

## Review

# Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures

Mariem Bouslimani <sup>1,2</sup> , Fatima Benbouzid-Si Tayeb <sup>1</sup> , Yassine Amirat <sup>2</sup>  and Mohamed Benbouzid <sup>3,\*</sup> 

<sup>1</sup> Laboratoire des Méthodes de Conception de Systèmes (LMCS), École Nationale Supérieure d'Informatique (ESI), BP68M, Oued Smar, Algiers 16270, Algeria; gm\_bouslimani@esi.dz (M.B.); f\_sitayeb@esi.dz (F.B.-S.T.)

<sup>2</sup> LabISEN, ISEN Yncréa Ouest, 29200 Brest, France; yassine.amirat@isen-ouest.yncrea.fr

<sup>3</sup> Institut de Recherche Dupuy de Lôme (UMR CNRS 6027), University of Brest, 29238 Brest, France

\* Correspondence: mohamed.benbouzid@univ-brest.fr; Tel.: +86-332-9801-8007

## Abstract

Recent technological advances in communication networks, intelligent devices, power electronics, and phasor measurement units have significantly transformed the operation of modern power systems. This evolution gave rise to smart grids, which enable the flow of real-time information on the operational state of the grid and of control commands across multiple communication infrastructures, using a variety of protocols and standards, between control centers and devices deployed throughout the grid's physical structure. At the same time, it has exposed power systems to new challenges and threats, due to the vulnerabilities inherited from the different components they integrate. Attackers have a variety of attacks at their disposal, by which they can disturb the availability of electricity as well as cause damage to the smart grid's physical structure. Therefore, cybersecurity has become an important aspect of the smart grid concept. This field of research has attracted the attention of many researchers, and in the last decade or so, the number of studies on the cyber-physical security of smart grids has surged significantly. Proportionally, an important number of survey papers were published as well. It has therefore become more difficult to navigate literature on the topic of smart grid cyber-physical security due to the large number of papers, the complexity of the grid's structure, and the variety of attacks, resolution methods, and techniques. To address this issue, in this work, we present a comprehensive review of existing literature reviews on the topic of smart grid cyber-physical security. We reviewed 100 survey papers, which were categorized into general surveys, attack-specific surveys, method-specific surveys, and component-specific surveys. We discussed and highlighted research tendencies in terms of attacks and methods used to protect smart grids. Additionally, we presented an overview of the different research challenges and possible future directions.

**Keywords:** smart grid; microgrid; cyber-physical security; cyber-physical attack; survey of surveys



Received: 21 October 2025

Revised: 18 November 2025

Accepted: 19 November 2025

Published: 21 November 2025

**Citation:** Bouslimani, M.; Benbouzid-Si Tayeb, F.; Amirat, Y.; Benbouzid, M. Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures. *Appl. Sci.* **2025**, *15*, 12367. <https://doi.org/10.3390/app152312367>

**Copyright:** © 2025 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

Over the years, power systems have witnessed major changes with the integration of information and communication technology, smart inverters, smart sensors, distributed energy resources (DERs), and smart meters, leading to the emergence of the smart grid (SG) concept. SGs aim to revolutionize power systems by introducing efficient energy production, optimizing energy demand and supply, lowering electricity prices, and reducing CO<sub>2</sub>

emissions. The technological advancements in renewable energy sources (RESs), power electronics, and energy storage systems (ESSs) have encouraged the deployment of DERs at the distribution level, and resulted in microgrids rapidly evolving as well. Supervisory Control and Data Acquisition (SCADA) encompasses sensors, intelligent electronic devices (IEDs), programmable logic controllers, and remote terminal units (RTUs). It collects and analyzes the power system's data for monitoring and control purposes. At the transmission level, phasor measurement units (PMUs) enhance power system observability by timestamping measurements using the Global Positioning System (GPS). At the customer level, smart meters provide advanced measurement capabilities such as consumption data reporting, outage detection, and energy efficiency [1]. They also provide two-way communication capabilities, allowing utilities to emit commands and control messages [1].

The evolution of power systems has exposed them to new types of threats and challenges. SGs integrate a multitude of components issued by different vendors and manufacturers, and each component exhibits several vulnerabilities. The SG, therefore, inherits the vulnerabilities of its different components. Particularly, the integration of communication networks in power systems provides an attractive surface for attackers to initiate and propagate their attacks. Indeed, numerous historical incidents demonstrate that power systems have been targeted by cyberattacks. Although the attack on the Ukrainian power infrastructure in 2015 remains the most prominent and well-known, numerous cybersecurity incidents involving power systems and other critical infrastructures have taken place recently (Table 1). A variety of cyber-physical attacks targeting the communication layer, the cyber layer, and the physical layer of the grid have emerged [2], such as False Data Injection (FDI), Man-in-the-Middle (MitM), message replay, and Denial-of-Service (DoS). These attacks aim to disrupt the stability of the grid's functioning and the availability of electricity. Cyber-physical security has become an integral part of the SG concept.

**Table 1.** Recently reported cybersecurity incidents in ICSs.

| Year | Attack                 | Target                                                | Description                                                                                                                                                                           | Ref. |
|------|------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| 2022 | Industroyer2 (malware) | Power plant, Ukraine                                  | Operators discovered a second version of the Industroyer malware that was used in the 2015 attack. The malware targets circuit breakers with the aim of causing blackouts.            | [3]  |
| 2022 | Ransomware             | DESFA (Natural gas distributor), Greece               | System outage and data exposure.                                                                                                                                                      | [4]  |
| 2022 | DoS                    | Gestore dei Servizi Energetici (Energy agency), Italy | Hackers compromised servers, blocked access to systems, and suspended access to the agency's website for a week.                                                                      | [5]  |
| 2022 | DDoS                   | Energy provider, Lithuania                            | Hackers targeted Lithuania's state-owned energy provider in a DDoS attack.                                                                                                            | [5]  |
| 2021 | Ransomware             | Colonial pipeline (oil/fuel pipeline), US             | The company shut down its pipeline system for a few days in response to the attack. Although the company paid the ransom, the data encrypted by the ransomware could not be restored. | [6]  |

The field of SG cyber-physical security has gained attention over the past decade, and many research areas have emerged (Figure 1). Vulnerability assessment, or vulnerability analysis, consists of identifying potential weaknesses in the system and determining the extent of the resulting damage to system operation [7]. Attackers typically exploit vulnerabilities that remain undiscovered or insufficiently secured, underscoring the critical importance of this research domain. Research on attacks focuses on designing and evaluating effective attack strategies, as well as modeling systems under adversarial conditions. In

contrast, research on attack countermeasures is the most active area in SG cyber-physical security, encompassing the design of methods for attack detection, mitigation, and prevention. Some countermeasures are designed specifically for a particular attack, whereas others secure SGs against multiple attacks. Researchers' interest in testbeds and simulators has increased with the need to study and evaluate new methods, protocols, technologies, and vulnerabilities in SGs. Testbeds allow the modeling of SGs for testing purposes without posing any risk to the structure's physical components, systems, and electricity availability. Researchers have also taken an interest in studying existing protocols, standards, and security frameworks, their limitations, and possible enhancements and alternatives to increase the grid's cyber-physical security against attacks.

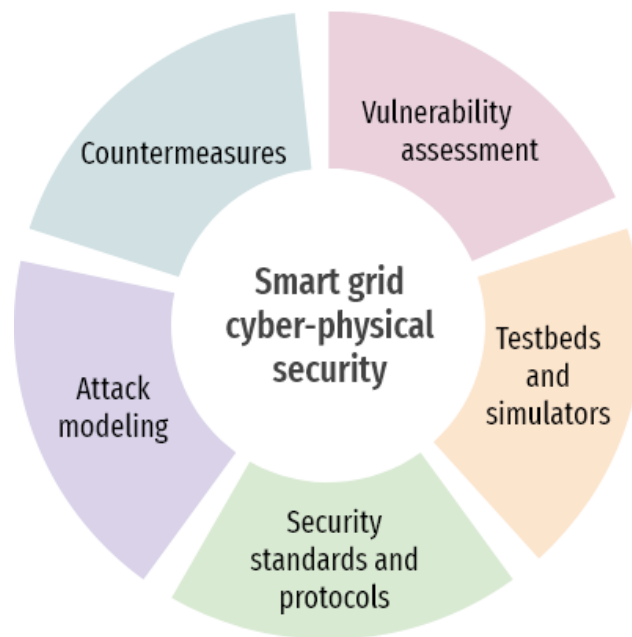


**Figure 1.** SG cyber-physical security research areas.

The SG is a complex structure as it generally extends over a large geographical area and integrates various components. The complexity of the grid's structure, the variety of attacks, the multiple research areas, and the growing interest of researchers in this field have resulted in a plethora of research works on the cyber-physical security of SGs, notably works proposing different attack scenarios exploiting vulnerabilities within the grid's structure, and works designing countermeasures against these attacks. This surge in the literature on SG cybersecurity, in turn, has led to the emergence of review papers proposing different taxonomies for attacks and countermeasures, as well as papers that provide an overview of the topic and its different research areas and key concepts. Although a significant number of these review papers provide a general overview of the field of SG cybersecurity, most papers tend to focus on a particular attack, technique, and/or component. This is due to the complex structure of the grid, the variety of attacks targeting it, and the diversity of techniques that can be adapted to countering attacks. While this is a beneficial outcome, the increased number of papers and surveys may be challenging when approaching the subject for the first time, especially when researchers are yet to become familiar with the grid's architecture, attacks, and countermeasure techniques. Additionally, navigating proper literature can become a time-consuming process, even for researchers who are already familiar with the field of SG cybersecurity, since search results must be filtered thoroughly. Consequently, there is a growing need for a systematic guide to help navigate the existing literature, both for readers already familiar with the field and for newcomers exploring the topic of SG cyber-physical security for the first time. Following a

systematic research methodology, we retrieved 100 literature reviews on the topic, which reflects the considerable interest in this research area. Motivated by this, we present in this work a comprehensive guide that systematically reviews existing literature reviews on SG cyber-physical security, highlights the key research areas and concepts of the field, and facilitates the process of navigating relevant literature. Moreover, it can offer a starting point for new researchers. The present manuscript seeks to review existing surveys on the cyber-physical security of SGs and reveal important findings, including research trends and future directions. Figures 2 and 3 depict the distribution of surveys per year and category, respectively.

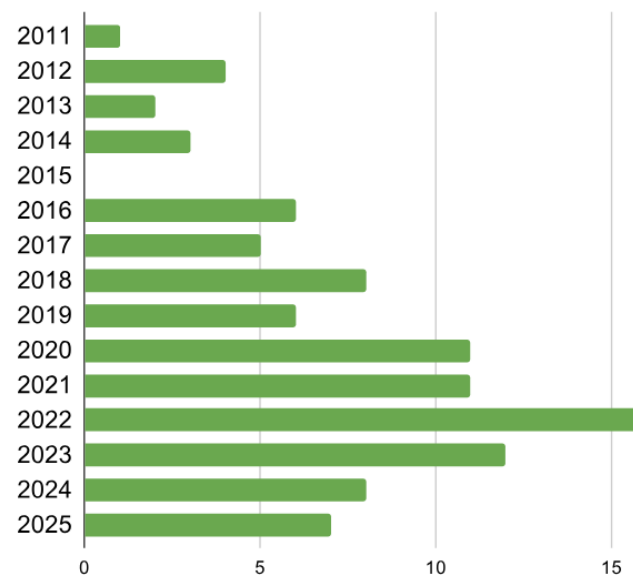


**Figure 2.** Distribution of survey papers per year.

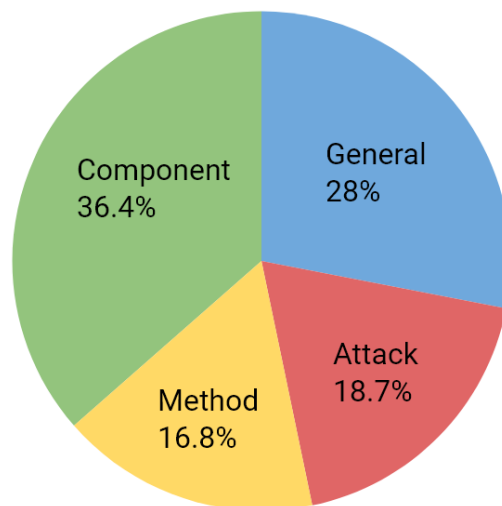


**Figure 3.** Percentage of survey papers per category (general, attack-specific, method-specific, component-specific).

This paper is organized as follows: in Section 2 we describe the research methodology and paper selection process that we followed to retrieve relevant literature for our survey. Section 3 provides a background on SG cybersecurity. Our review of reviews is conducted in Section 4, and discussed in Section 5. Section 6 summarizes the different research challenges faced by research on SG cyber-physical security. Finally, the limitations of this work and the conclusions are presented in Sections 7 and 8, respectively.

## 2. Research Methodology

A Systematic Literature Review (SLR) is a literature review in which the authors follow a well-defined process to analyze and interpret existing research relevant to a research question or phenomenon [8]. A literature review is referred to as a secondary study, where primary studies refer to empirical studies contributing to a secondary study [8].

The growing interest in SG cyber-physical security, combined with the complexity of the grid's structure and the diversity of attacks targeting it, has led to a surge in research, including numerous literature reviews. Consequently, there is a pressing need to track and organize these reviews. This SLR aims to serve as a practical guide, providing a comprehensive overview of the topic to help researchers navigate the extensive body of literature and identify the most relevant reviews for their work. It also aims to support new researchers in the field by offering a clear starting point, helping them avoid becoming overwhelmed by the vast amount of available literature.

In this review, we conducted an SLR on secondary studies, i.e., existing literature reviews on the cyber-physical security of electric grids. This type of work is referred to as a tertiary study [9]. The first step consists of identifying the need for a literature review by finding research gaps in existing literature. Several research questions were then identified, which we attempt to answer in our work. We define inclusion and exclusion criteria to select relevant literature. A number of quality assessment criteria were then defined to filter selected literature and obtain the final set of literature to be reviewed in our study. Finally, a search process was established and conducted on several databases using a set of keywords.

### 2.1. Paper Selection Criteria

Research questions are the foundation of an SLR, guiding the entire process. To address the issues outlined earlier, we formulated specific research questions that will be the central focus of this SLR:

- Q1: How is the research focus on SG cyber-physical security evolving over the years in existing literature reviews?
- Q2: How can we classify the existing reviews?
- Q3: Which cyberattacks on SGs have been the focus of researchers?
- Q4: What methods are used in securing grids against attacks?
- Q5: Which challenges are being faced by research on SG cybersecurity?

These questions help define the scope of this review and its key objectives. To be able to only select survey papers that are relevant to our research amid the large number of search results, we defined our inclusion and exclusion criteria. Surveys that fall into one or more of the following categories were included in our research:

- I1: Works that review the cyber-physical security of SGs in general.
- I2: Works that review existing countermeasures for attacks on SGs.
- I3: Works that review attacks, vulnerabilities, and attack vectors on SGs.
- I4: Works that review the cyber-physical security of a particular component in the SG.
- I5: Works that review countermeasures against a particular attack on SGs.

The inclusion criteria help us determine which survey papers fall within the scope of SG cybersecurity to keep during the selection process. They are applied by reading both the title and abstract of the paper, and in some cases, by reading through the rest of the paper. The selected papers must revolve around the topic of SG cybersecurity. Due to the variety of attacks and complex architecture of SGs, these criteria aim to include both papers that are general and papers that are particular to a certain attack, method, or component. On the other hand, surveys that fall into one or more of the following categories were deemed irrelevant for our research:

- E1: Works that do not focus on electric grid cyber-physical security.
- E2: Works on the security and resilience of electric grids that focus on aspect other than cyber-physical security and attacks.
- E3: Works on the security of cyber-physical systems (CPSs) or industrial control systems (ICSs) in general.

These exclusion criteria ensure that we stay within the boundaries of the scope of this research. Although the inclusion criteria are enough to select only papers that are relevant to our topic, some papers on the cybersecurity of CPSs and ICSs have also ended up in our search results due to the *smart grid* keyword, as well as keywords related to attacks. These papers do not provide a comprehensive review of SG cybersecurity, as SGs are only considered an example of CPSs under the threat of attacks. Moreover, we noticed that an important amount of work on the protection and resilience of power systems to various events also made it into our search results. Although these works are relevant to the field of SG cybersecurity, attacks are only considered as a case study at most, and therefore, they do not provide an extensive review on the topic of SG cybersecurity, attack implementation, and attack detection. By combining the inclusion and exclusion criteria defined above, we ensure that only relevant papers have been selected for our review. Finally, surveys that do not comply with the following quality assessment criteria were eliminated:

QA1: The survey must provide a comprehensive review of existing literature.

QA2: The survey must introduce a novelty compared to previous works.

These criteria ensure that the selected papers offer a sufficiently comprehensive and systematic review of the literature. Moreover, the paper must not introduce redundancy with existing literature. To maintain objectivity and consistency in literature selection, all retrieved papers were systematically reviewed by the authors. The first author conducted the initial literature search and applied the predefined inclusion and exclusion criteria. Subsequently, each author independently screened the papers and decided whether to include or exclude each paper based on the quality assessment criteria. Any paper for which the authors disagreed was resolved through discussion.

## 2.2. Search Process

We used a set of keywords to form search strings to find literature reviews relevant to our research. These keywords can be grouped into two categories: structure-related keywords (microgrid, smart grid, power system) and cybersecurity-related keywords (cybersecurity, security, attack, FDI, false data injection, DoS, denial of service, MitM, man-in-the-middle, replay). We also used keywords *review*, *survey*, and *state-of-the-art* to retrieve literature reviews from databases that do not have a filter. Boolean operators (AND, OR), double quotation marks (""), and parentheses were used to form search strings containing the previously mentioned keywords. The search strings used to retrieve relevant papers are listed in Appendix A.

Figure 4 visualizes the search process and the result of each step in terms of articles. The search for relevant literature reviews was conducted on five databases: IEEEXplore, Science Direct, Springer Link, MDPI, and Google Scholar. We did not specify a date range for the results. By referring to the title and abstract of each article, we applied the previously defined inclusion and exclusion criteria on the initially obtained search results, selecting 270 articles. After reading the content of each survey and applying the quality assessment criteria, the number of articles was narrowed down to 100, where 50.5% were selected from IEEEXplore, 22.77% from ScienceDirect, 13.86% from Springer, and 5.94% from MDPI. The remaining 6.93% include articles from other databases including ACM, IET, and ArXiv (Figure 5). Of the selected papers, 63% appeared in Q1 journals, 15% in Q2 journals, and 19% in conference proceedings. The remaining 3% consisted of a book chapter, an ArXiv

preprint, and a paper in a Q1 journal that had not yet been indexed at the time of its publication (Figure 6).

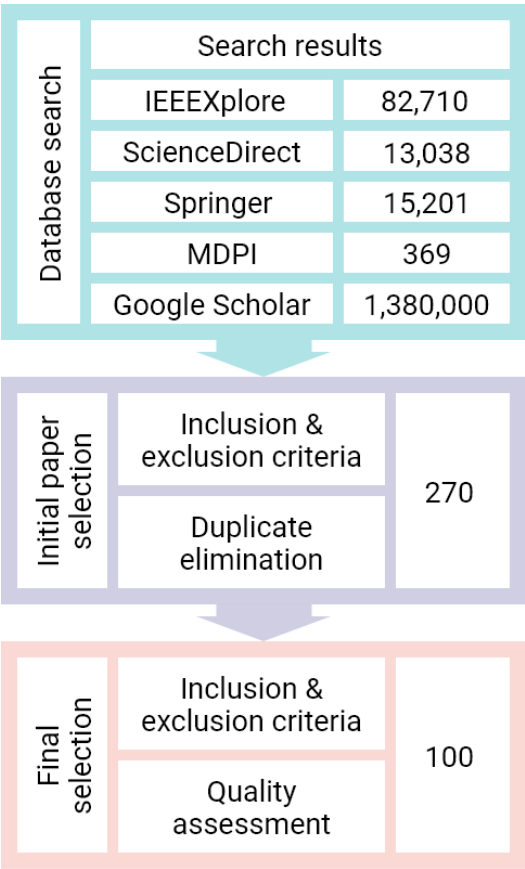


Figure 4. Paper search process and results.

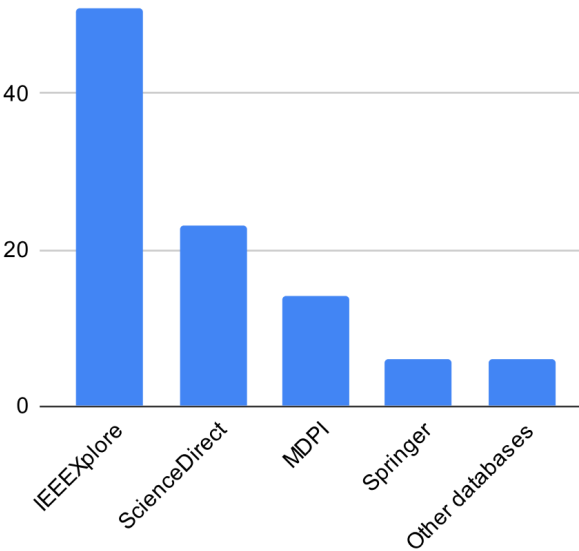


Figure 5. Number of papers per database.

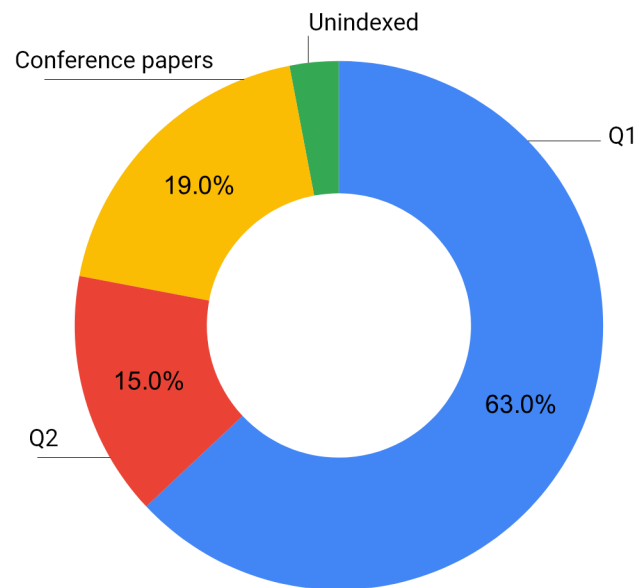


**Figure 6.** Distribution of selected papers per journal quartile.

### 3. Key Concepts and Definitions

The integration of smart devices and communication networks within the traditional power grid's structure, in addition to the decentralization of generation with the emergence of distributed generation (DG), has enabled the implementation of the SG concept. Furthermore, customers can now participate in the production of energy. Being part of the electric grid, microgrids have also changed, resulting in more intelligent control schemes and more reliable energy production through DG units. The capabilities of the SG rely on the ability of components and applications to communicate and exchange information through the communication infrastructure. Therefore, SGs combine various communication technologies to ensure reliable information exchange between their components and applications. The SG integrates diverse components from different vendors. As a result, multiple standards and protocols have been developed to enable secure communication and seamless integration among these components.

The integration of different technologies and communication networks in SGs has led to the emergence of numerous security challenges. SGs inherit vulnerabilities and security issues associated with their components and communication infrastructure, making them attractive targets for malicious attackers. As a result, cyber-physical security has become a critical aspect of the SG. Thus, to fully understand the intricacies of the topic, it is essential to first grasp several key concepts that form its foundation. This section provides an overview of these concepts, beginning with smart grid architecture, communication systems, relevant standards and protocols, cyber-physical attacks, and lastly, testbeds.

#### 3.1. Architecture

Formerly, the electric power grid could be represented by a hierarchical model consisting of generation, transmission, and distribution. The electricity is first generated in power plants before being transmitted over transmission lines to be distributed to customers over distribution lines [10,11]. Power grid energy resources generally include hydro and nuclear energy, fossil fuels, RESs such as solar and wind energy, and green energy resources such as fuel cells, combined heat and power, and microturbines [11]. Transformers are used to step up and step down electric power voltage in transmission and distribution substations [10,11]. Power grids are designed according to long-term forecasts developed in power grid control centers based on the anticipated needs of consumers [11].

The SG introduces some improvements to the traditional power grid, such as the reliable integration of RESs, microgrids, and communication technologies, as well as the implementation of full digital control using information technology [12,13]. SGs aim to reduce peak demand and enable the active participation of consumers [12]. On the distribution side, SGs integrate different types of generation and storage systems [12]. Smart sensing, smart metering, two-way communication infrastructure, and advanced control methods are some of the main components of an SG [12]. Table 2 summarizes some of the important differences between traditional power systems and the SG.

**Table 2.** Comparison between the traditional power grid and the SG.

| Aspect     | Traditional Power Grid        | SG                   | Ref. |
|------------|-------------------------------|----------------------|------|
| Customer   | Simple consumer               | Active participation | [12] |
| Generation | Centralized in power plants   | DERs                 | [14] |
| Power Flow | Unidirectional (hierarchical) | Bidirectional        | [15] |
| Control    | Limited                       | Widespread           | [16] |

To ensure a safe operation of the SG, real-time grid management is required [17]. The SCADA system acquires and monitors real-time data on the grid through sensors, IEDs and RTUs before sending it back to the control center through a communication network, where operators use the data for decision making to remotely control the grid [11,17]. PMUs are used to complement RTU measurements with more precise observations [17]. Aside from voltage transformation, substations set up a connection point for the transmission and distribution of power lines, provide a monitoring point for control centers, and ensure communication with other substations and regional control centers [12]. The operation of power grids requires that a balance is maintained between generation and demand by ensuring that voltage and frequency parameters remain within predetermined ranges [18]. This is ensured by system changes made through generation stations and transmission and distribution substations [18]. SCADA systems employ RTUs, and more recently, IEDs in substations. RTUs are microprocessor-based devices used to transmit data and issue commands to connected devices [12]. IEDs have emerged as more sophisticated microprocessor-based devices for protection, monitoring, control, and data acquisition in substations, and are capable of complementing RTU functionalities [12,19]. PMUs emerged in SGs with the need to transmit time-synchronized measurements over wide area networks (WANs) [18] and are considered one of the most promising measurement devices in transmission systems [17]. A PMU calculates the magnitude and phase of a voltage or current waveform and synchronizes them using an integrated GPS receiver [20]. Distributed Network Protocol 3 (DNP3), MODBUS, and more recently, IEC 61850 are some of the commonly employed protocols by SCADA in substations [19].

The concept of generation in traditional power systems has morphed into DERs, allowing the integration of RESs [14]. The DER concept encompasses DG and ESSs [12]. DERs are distribution-side energy sources of smaller generation capacities compared to utility generation resources, such as reciprocating diesel engines, natural gas-powered microturbines, and RESs such as solar photovoltaic and wind turbines [21]. The connection and protection of DERs are enabled by transformers, switches, relays, power electronics, and communications devices [12]. Since RESs are characterized by unpredictability, intermittency, and proneness to fluctuations, the integration of ESSs, such as battery energy storage systems (BESSs), allows the storage of energy when generation exceeds consumption so that the stored power can be used when demand exceeds the amount of generated power [21–23].

The advanced metering infrastructure (AMI) integrates smart meters, communication networks, a meter data management system (MDMS), sensors, and monitoring sys-

tems [13,24]. The AMI establishes two-way communication between smart meters and utility companies [1,14,24]. Smart meters are considered the foundation of the SG concept [1]. A smart meter is a developed version of traditional meters, offering both measurement and communication functionalities [14,24]. Smart meters measure energy, demand, consumption data, and power quality before communicating them to both utility and consumers [1]. Furthermore, the AMI enables utilities to issue commands through smart meters and load-controlling devices [1,24]. Metered consumption data is sent to the MDMS for data analysis and storage [24].

A microgrid is a distribution-side power network that integrates DERs, i.e., DG units and ESSs, as well as controllable loads, acting as a single entity from the main grid's view [23,25–27]. It is connected to the main grid through a point of common coupling (PCC) and has two modes of operation, grid-connected mode and islanded mode. In the grid-connected mode, the microgrid and the main grid trade power, while in the islanded mode, the microgrid operates autonomously, and the local loads are supplied with power generated inside the microgrid, including power from storage units.

Figure 7 presents a global representation of the SG's architecture. Figure 8 shows the different components and systems in each part of the grid.

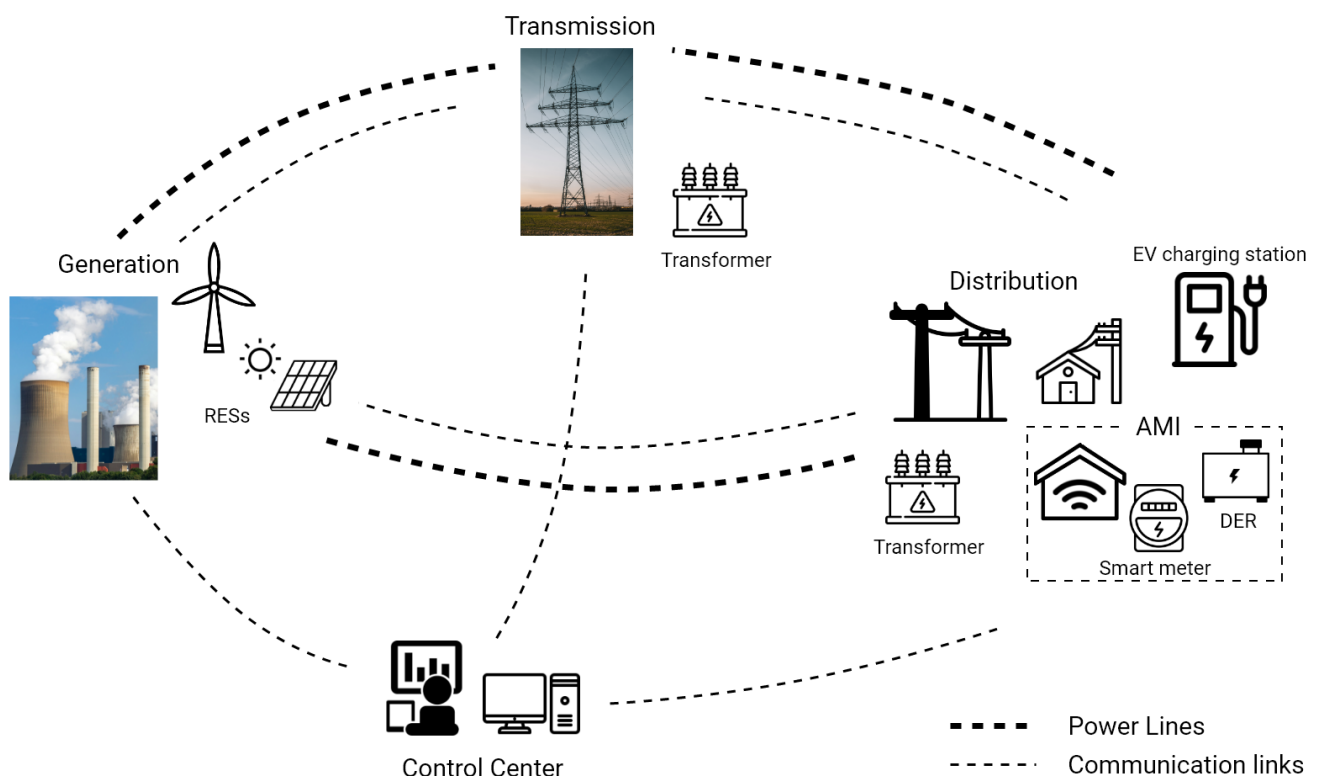


**Figure 7.** SG architecture.

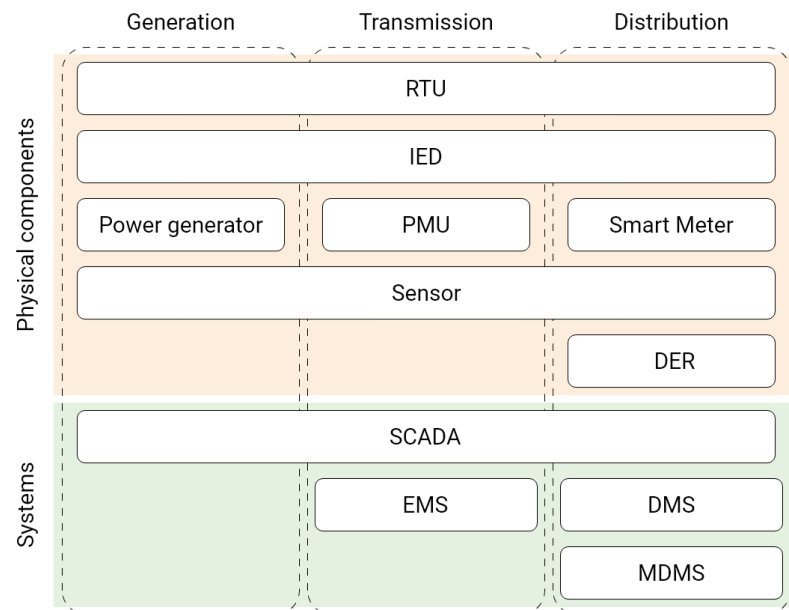


**Figure 8.** SG components and systems.

### 3.2. Smart Grid Communications

A power grid with its generation, transmission, and distribution generally extends over a large geographic area, thus requiring the usage of multiple types of networks to ensure reliable communication between its components. The communication infrastructure of the SG consists of home area networks (HANs), neighborhood area networks (NANs), field area networks (FANs), and a WAN [14,20,28]. The HAN covers a customer's home environment, connecting components such as smart meters, smart appliances, and electric vehicle (EV) chargers, allowing applications such as demand-response, energy efficiency, billing, and power consumption optimization to communicate with each other and with the control center through a gateway or a smart meter [20,28]. The NAN connects smart meters of a neighborhood with data concentrators or substations [29]. NANs transmit data related to smart metering, demand-response, energy consumption, pricing, and power outages [20,28]. FANs connect field devices and substations for the monitoring, control, and protection of the grid [20]. A FAN generally covers the communication between the control center, transmission and distribution substations, microgrids, DERs that are managed by the utility, and public EV charging stations [20,29]. It allows the connectivity of field devices such as RTUs, IEDs, and PMUs [20,28]. Transmission and distribution applications communicating through FANs include SG monitoring, control, and protection, energy management system (EMS), distribution management system (DMS), SCADA, and distribution automation such as controlling field devices remotely [20,28]. FAN and NAN are sometimes combined in the term FAN by considering that a FAN refers to a NAN that integrates field devices as well [28]. The SG's WAN connects energy control centers and data concentrators of NANs, providing a communication medium between utility control centers, substations, and power plants [20,29]. WANs transmit data related to the grid's state and support control and protection applications for outage prevention [28]. Figure 9 provides a visual representation of the different communication networks in an SG. Wireless technologies used in SGs include ZigBee, wireless mesh networks, WiFi, cellular networks, Bluetooth, and WiMAX, whereas wired technologies include power line communication (PLC), digital subscriber line (DSL), and optical fiber (Figure 10).



- The IEC 61850 standard defines the exchange of data between IEDs for substation automation [32]. The standard was initially designed for communication within a substation, but later evolved to enable substations to communicate with each other [32];
- IEC 62056 was defined for the transmission of smart metering data, including protocols for communication over power lines [32]. In the context of AMI, it specifies how information is transmitted between metering equipment and data collection systems [1];
- The ANSI C12 protocol suite was also defined for AMI applications [32];
- IEC 60870-6 provides a communication profile for SCADA that enables the exchange of telecontrol data between applications [31];
- DNP3 is mostly used for the communication between SCADA master stations, RTUs, and IEDs for substation automation [31];
- Modbus is also used for SCADA communications architecture [31];
- The AMI System Security Requirements (AMI-SEC) defines a set of security requirements covering AMI modules, including communication and networking devices, meters, and MDMS [31,33];
- IEC 62351 is a set of standards defining cybersecurity requirements to secure power system communications, offering security enhancements to different communication protocols [31–33];
- The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) defines a number of standards that aim to maintain a secure operation of bulk energy systems, which generally cover both generation and transmission [31,34]. The standard is applicable in multiple areas such as security control management, personnel training, and cybersecurity incident reporting [31,33];
- The National Institute of Standards and Technology Interagency Report 7628 (NISTIR 7628) provides a framework to guide organizations in developing effective cybersecurity strategies and assessing risks related to SGs [34].

SG communication protocols are vulnerable to attacks. They were designed decades ago in the absence of today's cybersecurity concerns. Moreover, they were adapted to the resource-constrained nature of most power system devices. Incorporating security measures into communication protocols often proves challenging. For instance, C37.118, IEC 61850, DNP3, and Modbus transmit messages in plaintext due to the absence of an encryption mechanism [35–37]. This allows attackers to intercept the communication between devices and to eavesdrop on sensitive information to initiate different attacks. Although the IEC 61850-90-5 protocol introduces a strong encryption feature, it is not always applicable due to the added communication overhead and the higher bandwidth requirements [35,38,39]. Moreover, these protocols lack authentication, and by performing a MitM attack, an attacker may replay data packets or inject false data. When built over the TCP/IP stack, the SG communication protocols inherit their vulnerabilities to DoS attacks [40]. Some protocols have design flaws, such as the buffer overflow vulnerability in IEC 61850 and DNP3, which can be exploited by sending data exceeding the buffer's capacity, resulting in a DoS [41,42]. Table 3 provides a summary of key standards and protocols used for SG communications and security purposes.

**Table 3.** Communication and security standards and protocols for SGs.

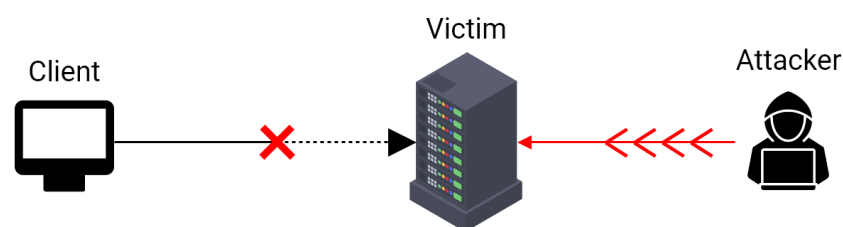
| Standard       | Purpose                                            | Refs.         |
|----------------|----------------------------------------------------|---------------|
| AMI-SEC 7628   | Security requirements for AMI                      | [31,33]       |
| ANSI C12.18    | Communication between smart meters                 | [13]          |
| ANSI C12.19    | Data structures for meter communication            | [1]           |
| C37.118.2-2011 | Communication for PMU and phasor data concentrator | [20,30,31]    |
| DNP3           | Automation system devices communications           | [31]          |
| IEC 60870-6    | Communication profile for SCADA                    | [31]          |
| IEC 61850      | Communication for substation automation            | [13,20,31,32] |
| IEC 62056      | Electricity metering data exchange                 | [1,32]        |
| IEC 62351      | Cybersecurity of protocols                         | [31–33]       |
| Modbus         | Communication protocol                             | [31]          |
| NERC-CIP       | Security standards for bulk energy systems         | [31,33,34]    |
| NISTIR 7628    | Security framework for organizations               | [34]          |

### 3.4. Cyber-Physical Attacks on Smart Grids

The connection of SG devices through communication networks has provided attackers with a broader attack surface. Consequently, various forms of cyber-physical attacks have emerged both in real-life incidents and in the literature on CPSs in general and on SGs in particular. These attacks can have devastating impacts on the availability of electricity and on the grid's physical components. Possible outcomes of an attack include power outages, damaged energy resources, and economic losses. In the following section, we will present the different cyber-physical attacks targeting SGs.

#### 3.4.1. Denial-of-Service

A DoS attack targets availability by overloading a system so that it will no longer be able to respond to genuine requests from its legitimate users, or becomes relatively slow at doing so [43]. A DoS attack generally targets network devices, network segments, servers, and applications hosting a targeted service [43]. Attacking one of these elements will disrupt the transfer of information between communicating nodes (Figure 11).

**Figure 11.** DoS attack.

DoS attacks are often achieved through a technique called flooding. An attacker floods a network device with traffic, or a server with requests, to prevent authentic requests from reaching their destination [43,44]. SYN flood, UDP flood, the ping of death, and DNS flood are widely used flooding techniques. In wireless networks, jamming attacks can disrupt communications and cause a DoS [44]. A jamming attack is a physical attack that involves introducing noise into a wireless medium using electromagnetic signals [45,46]. An attacker may also exploit vulnerabilities in protocols and devices to cause a DoS [40].

Distributed Denial-of-Service (DDoS) is a powerful form of DoS where an attacker uses multiple distributed machines to deliver the attack (Figure 12). The machines attack in a coordinated and simultaneous manner, overwhelming the victim with traffic [43,47]. DDoS amplifies the impact of an attack and is harder to counter [48].

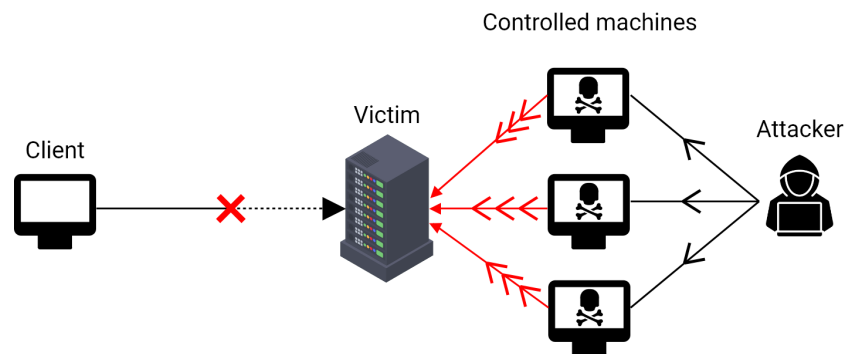


Figure 12. DDoS attack.

In the context of SGs, DoS attacks target the communication infrastructure and exploit vulnerabilities within protocols, software, and applications. Various DoS attack vectors exist within the SG. For instance, the IEC 61850 standard and Modbus protocol are both built over the TCP/IP protocol stack and are therefore vulnerable to flooding attacks [49,50]. A vulnerability within IEC 61850's Generic Object Oriented Substation Event (GOOSE) messages can be exploited by a GOOSE poisoning attack, where an attacker sends a GOOSE message containing a higher status number to an IED, rendering the IED unresponsive to legitimate GOOSE messages because of their lower status numbers [51]. Other protocols such as C12.22, C37.118, and DNP3 are vulnerable to DoS attacks, such as the buffer overflow vulnerability [41,52,53]. Although IEC 62351 was developed to enhance protocols' vulnerabilities, including IEC 61850, it does not protect against DoS attacks [54]. Wireless networks used in SG communications are vulnerable to jamming attacks.

DoS prevents sensor readings and measurements from reaching the control center, affecting its situational awareness of the grid and preventing it from taking adequate actions [50]. This could lead to instability and, eventually, blackouts [48,50]. Delays introduced by DoS attacks may delay time-critical messages, such as smart meter messages [50]. In the context of microgrids, DoS attacks preventing shedding and reconnection commands from being delivered may impact frequency stability [55]. Jamming can prevent sensors and smart meters from communicating with the utility [45,45].

### 3.4.2. False Data Injection

FDI is a stealthy attack that consists of injecting malicious data and manipulating information to disturb the SG's operational reliability [56]. State estimation is one of the main targets of FDI attacks. State estimation infers the operating conditions of the grid based on measurements collected by sensors and meters, and the control center relies on its output to monitor and control the grid [57–59]. FDI alters measurements destined for state estimation to mislead the control center into making wrong decisions, which can have catastrophic impacts, including power outages (Figure 13).

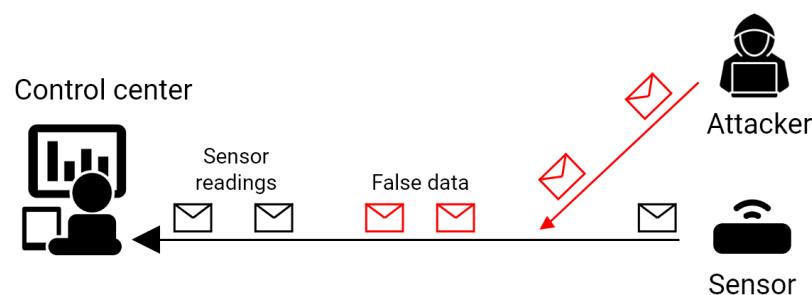


Figure 13. FDI attack.

Other FDI scenarios and targets were investigated in the literature. For instance, an attacker may inject false data into a DER's smart inverter, triggering inaccurate control actions from the EMS [60]. Sending falsified synchronization control messages to a microgrid's generator may result in unnecessary tripping, instability, and blackout [61]. An attacker may also inject false data between the AMI and the utility, either by compromising a smart meter or an aggregation point of multiple meters [24]. This allows them to perform energy theft and cause financial losses to the utility. An attacker may inject false control commands to cause, for instance, the opening of circuit breakers [62]. Resonance attacks can also be considered a form of FDI. A resonance attack involves altering system inputs, such as power frequency, using a resonance source such as the output of a function [56,63].

### 3.4.3. Replay Attack

A replay attack strategy involves an attacker first intercepting the transmission between two entities and recording a sufficient number of messages before replaying them [64–66] (Figure 14). The replayed messages, having been correct at the time of their recording, are less likely to be correct when replayed, which can lead to control centers responding with inaccurate actions, potentially damaging the grid. A replay attack can be very effective as it can give the illusion of the system being in a normal state [64]. Replay attacks are easier to implement compared to other attacks, such as FDI, since they do not require as much information on the target [67]. An attacker may intercept a wireless communication network to collect transmitted data packets, or break through the protection of sensors or smart meters to gain control over them [64,65].

Various possible scenarios exist for an attacker to use replay attacks to damage SGs. For instance, in the context of consensus-based control, an attacker may replay a high load demand message to trick a DER into responding with unnecessary actions, such as increasing its output, resulting in a disturbance of the power distribution's balance [64]. An attacker may also replay voltage regulation commands, leading to a destabilization of voltage levels [64]. The two previous scenarios can eventually lead to power outages. If an attacker gains access to the communication network of an IEC 61850-based power system, they can intercept GOOSE messages containing trip commands during a fault correction [66]. Once the fault is cleared, the attacker can replay the message, and the breaker IED receiving the replayed packet will interpret it as a new trip command, unnecessarily executing it [66]. This strategy can be exploited to cause blackouts or to induce physical damage to both centralized generators and DERs. By hijacking smart meters or the communication network of an AMI, an attacker can replay consumption data to perform energy theft, causing financial losses to the utility company. Replay attacks can also be used to open the circuit breaker at the PCC of a microgrid to cause unintentional islanding, resulting in a power outage, and possibly damaging the microgrid's DERs. Replay attacks can also be used to mask failures by maintaining the semblance of a normal system operation, resulting in necessary actions not being taken.

### 3.4.4. GPS Spoofing

In SGs, a PMU is the primary target of a GPS spoofing attack. PMUs time-stamp measurements such as current and voltage amplitudes and phases using GPS signals, and GPS spoofing aims to alter these time-stamps [68,69]. In the literature, GPS spoofing is also referred to as time synchronization attack, as it desynchronizes phasors. To perform a GPS spoofing attack, the attacker first uses a spoofer to cause interference between the PMU's GPS receiver and the authentic GPS signals [68]. Afterward, the spoofer is used to launch fake GPS signals, which the receiver will track and acquire, since the spoofer's signals have a higher signal-to-noise ratio than that of the authentic signals [68]. Figure 15 illustrates a GPS spoofing attack.

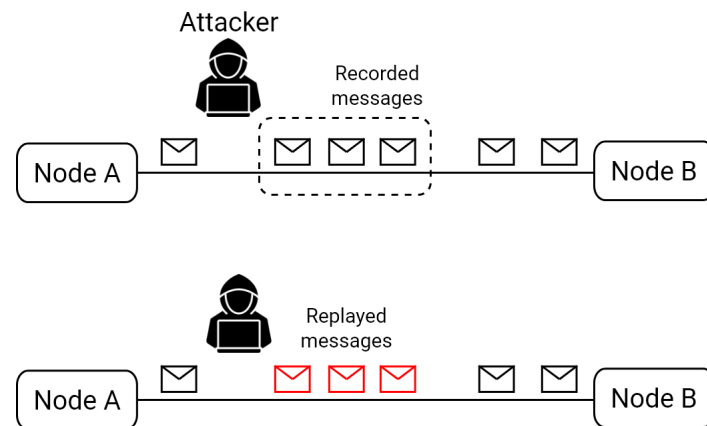


Figure 14. Replay attack.

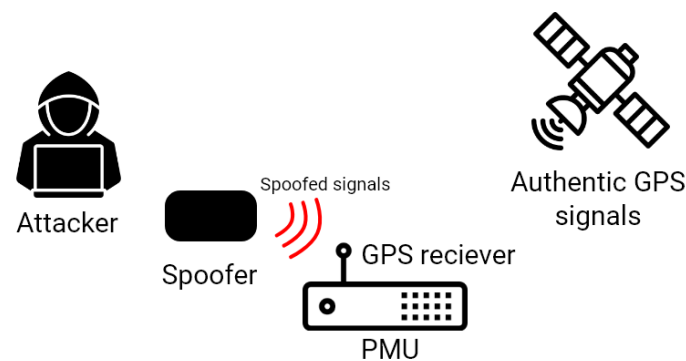


Figure 15. GPS spoofing attack.

GPS spoofing can impact the SG's transmission line fault detection, which relies on PMUs [68]. The fault detector in the presence of a GPS spoofing attack will possibly set off a false alarm at the control center level, affecting the grid's reliability and triggering cascading failures [68]. This type of attack also impacts grid voltage stability monitoring, which relies heavily on PMUs to provide stability indicators [68]. A GPS spoofing attack can desynchronize voltage indicators, resulting in inadequate actions during voltage regulation [68].

#### 3.4.5. Man-in-the-Middle

MitM refers to an attacker intercepting messages between two communicating ends, to eavesdrop and even impersonate one of the victims [43,70] (Figure 16). The attacker can modify and replace the exchanged messages [71]. MitM compromises confidentiality, as it allows an unauthorized entity to eavesdrop on information, and integrity, as the attacker can modify the content of messages. MitM can act as a precedent for other forms of attacks, such as FDI and replay. ARP-spoofing and DNS-spoofing are some of the techniques used to perform an MitM attack.

In the context of SGs, MitM may be used to intercept IEC 61850, DNP3, and Modbus messages [70]. An attacker can perform ARP-spoofing to intercept a substation's communication and alter DNP3 commands [70], which can disrupt the grid's operation and even cause physical damage and power outages. Power measurements transmitted through the communication network may also be intercepted and altered, causing abnormal conditions that will eventually lead to a regional blackout, as was demonstrated in [72].

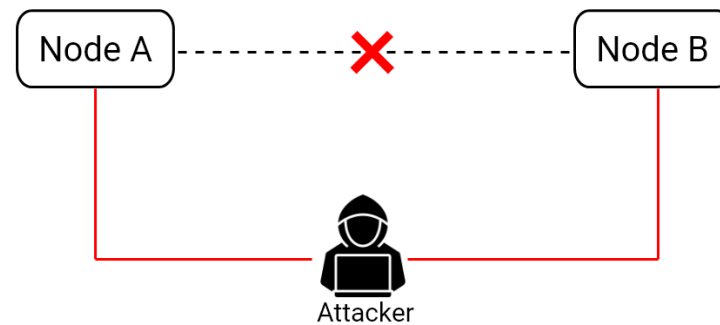


**Figure 16.** MitM attack.

### 3.5. Cyber-Physical Testbeds for Cybersecurity Testing

Power systems are a critical infrastructure. Their correct operation is crucial, as countless sectors depend upon the availability of electricity. When it comes to implementing cyberattacks and their countermeasures, it is impossible to test them on the actual power grid, as it risks disrupting its operation. Moreover, SGs consist of a cyber part and a physical part, necessitating tools that can reflect the grid's operation through the interactions between its different components. Testbeds have emerged as a solution that allows the experimental verification of applications in critical fields and infrastructures such as hydraulic systems, healthcare, transportation systems, aviation, robotics, and SGs [73]. In the field of SG cybersecurity, testbeds are essential for assessing vulnerabilities, as they enable the implementation and testing of attacks, the design of countermeasures, and the evaluation of their robustness.

To reflect the interaction between the cyber and physical components of a power system, testbeds implement power system devices (the physical part) and the communication infrastructure (the cyber part) using simulators, emulators, and physical devices. Testbeds can either be fully virtual, where the power system is implemented through simulators and emulators only, or they can incorporate physical devices such as PMUs, IEDs, and energy resources, in which case they are often referred to as hardware-in-the-loop [39]. Testbeds can be categorized into simulation-based, hardware-based, and hybrid testbeds [73,74]. Simulation-based testbeds use software-based simulators to implement power system components and simulate data and communication networks [73]. Various power system simulators exist, such as DigSilent Powerfactory, MATLAB/Simulink, PowerWorld, Power System Simulation and Modeling Software (PSS), HYPERSIM, and Transient Security Assessment Tool (TSAT) [39,73,75,76]. Moreover, real-time simulation platforms such as the Real-Time Digital Simulator (RTDS) and OPAL-RT, which allow real-time simulation and testing of power systems by providing interfacing capabilities with physical devices and real-time data acquisition [75,77]. Furthermore, communication networks are generally simulated using OPNET, Network Simulator-3 (NS-3), OMNeT++, and EXata network emulator [39,73,78]. For instance, ref. [79] used RTDS to simulate the power grid, while an independent simulator was used to simulate power resources. They also developed a data interface to ensure the connection between the two simulation platforms. Furthermore, they implemented virtual RTUs separately from the RTDS to reflect the process of data transmission in a practical situation. For the communication network, a wide area network emulator was used. Ref. [78] used both OPAL-RT and RTDS to simulate the power grid components and emulated the communication network through the EXata network emulator. Simulation-based testbeds are becoming less common with the emergence of hardware-in-the-loop systems, as the integration of hardware in testbeds allows for a more realistic representation of power grids.

Hardware-based testbeds rely exclusively on physical devices and power resource emulators to represent SGs. Ref. [80] proposed a hardware-based microgrid testbed consisting of both conventional energy resources (motor generators) and DER emulators for fuel cells, wind, and photovoltaic sources. Although the testbed was used to test microgrid islanding capabilities, it can also be used in the field of SG cybersecurity to test the physical impact of attacks on energy resources and electricity availability by launching them through the communication network or from one of its components, as well as to evaluate the response of countermeasures to these attacks. In contrast to software-based and hybrid testbeds, fully hardware-based testbeds are less prevalent in the literature due to the difficulty of putting together a testbed consisting exclusively of physical devices. Moreover, they can only reflect a portion of the grid, or a small-scale microgrid, as it is impossible to put into place a large-scale SG or microgrid that covers an entire city or country.

Hybrid testbeds have become an attractive alternative to both hardware-based and simulation-based testbeds, since they combine physical power system devices and simulators, bringing testbeds closer to reality, while replacing elements that are difficult to implement using hardware through simulations. In [81], the authors proposed a testbed using RTDS to implement the power system, including grid topology, generators, and loads. They integrated RTUs and PMUs for real-time monitoring and measurement in the testbed, with the data being transmitted to the simulator. The testbed is used to test the impact of FDI attacks on PMUs and RTUs. Ref. [82] proposed a transmission network testbed for SG cybersecurity testing, consisting of physical devices including RTUs, IEDs, and merging units, as well as signal emulators that output current and voltage measurements. A digital-twin model was used to represent a city's energy and data infrastructures, while the testbed acted as its transmission and distribution network. Various parts of the SCADA system were emulated using Raspberry Pi devices, including RTUs and Master Terminal Units. Ref. [83] combined OPAL-RT with two physical IEDs used as protective relays for transmission lines. Table 4 lists existing testbeds designed for SG cybersecurity, including the ones reviewed in this section.

**Table 4.** SG cyber-physical testbeds for cybersecurity applications.

| Ref. | Target                     | Year | Type       | Power System                                                                   | Communication                                            |
|------|----------------------------|------|------------|--------------------------------------------------------------------------------|----------------------------------------------------------|
| [82] | Transmission network       | 2025 | Hybrid     | Digital-twin city model, RTUs, IEDs, SCADA, Raspberry Pi                       | Real network                                             |
| [81] | Synchrophasor network      | 2024 | Hybrid     | RTDS, PMUs, RTUs                                                               | -                                                        |
| [78] | Large-scale power systems  | 2024 | Simulation | OPAL-RT, RTDS                                                                  | EXata network emulator                                   |
| [80] | Microgrid                  | 2021 | Hardware   | Motor generators, RES emulators, inverters, transmission lines, electric loads | Wired and wireless communication networks (real network) |
| [76] | AC microgrid               | 2021 | Simulation | OP5700, HYPERSIM, OPAL-RT                                                      | -                                                        |
| [79] | SG                         | 2017 | Simulation | RTDS, energy resource simulators                                               | Wide area network emulator                               |
| [83] | SG                         | 2017 | Hybrid     | OPAL-RT, IEDs                                                                  | Serial communication (real network)                      |
| [84] | SG                         | 2015 | Hybrid     | RTDS, PMUs                                                                     | NS-3                                                     |
| [42] | IEC 61850-based substation | 2015 | Hybrid     | RTDS, IEDs, RTU                                                                | Ethernet switch, fiber-optic network                     |

## 4. Synthesis of Existing Surveys: A Deep Dive into SG Cybersecurity Literature

In Section 2, we defined the process by which we selected the surveys to be reviewed in this study. These surveys generally include definitions of the key components and systems of an SG concerned with cybersecurity and cyber-physical security, in addition to security objectives and requirements. They also discuss vulnerabilities, attack vectors, and attack taxonomies. Moreover, they review existing literature on attack strategies and countermeasures. To provide a structured and meaningful analysis of the reviewed literature, we organized the surveyed works into four main thematic categories of surveys: (1) surveys that cover the topic of the SG cybersecurity in a general manner; (2) surveys that focus on a specific attack such as FDI attacks; (3) surveys that focus on a particular method, machine learning (ML) for instance; (4) and finally surveys that focus on a specific component or part of the SG. This categorization serves two key purposes: first, to identify recurring research patterns and gaps within the existing body of literature; and second, to assist readers in efficiently locating reviews that align with their specific research interests within the domain of SG cybersecurity. In what follows, we present the structure of our analysis through four thematic sections, each addressing a specific dimension of the surveyed literature. First, Section 4.1 outlines the core concepts commonly addressed in the literature, including cybersecurity objectives, attack types, communication protocols, and smart grid architecture. Then, Section 4.2 examines the most critical attacks discussed in the reviews, their points of entry, propagation vectors, and their potential impact on grid operation. Next, Section 4.3 analyzes the main research trends in detection, mitigation, and prevention, highlighting the transition from traditional approaches to the adoption of emerging technologies. Finally, Section 4.4 focuses on the key components and systems that are frequently studied in the context of SG cybersecurity, emphasizing the areas considered most vital for protection efforts.

### 4.1. Focused Analysis of General Surveys in SG Cybersecurity

Many researchers have covered the topic of the electric grid's cyber-physical security from a bird's-eye view, presenting vulnerabilities that exist in the grid structure and possible attack vectors, security objectives, the different types of cyberattacks targeting the grid stability, and existing types of intrusion detection systems (IDSs). To the best of our knowledge, the seminal works of [85,86] were among the first to explore the topic of power grid cyber-physical security. Ref. [85] introduced vulnerabilities that exist in the power grid's control loops in generation, transmission, and distribution, as well as the cyberattacks targeting them. They also presented security concerns related to some of the power grid's components and aspects, including communication, devices, and security management and awareness. They reviewed research efforts to enhance the grid's security as well. Ref. [86] summarized security-related challenges in SGs and introduced the different attacks threatening them. Security fundamentals, such as IDSs, access control, and authentication, were also discussed. Ref. [87] discussed cyber-physical security objectives in the context of SGs, as well as a number of cybersecurity requirements such as authentication and authenticity. They also provided a detailed review of cyberattacks classified according to the targeted security objective and according to the targeted network layer. Some of the techniques and frameworks used in SG cyber-physical security analysis are briefly discussed, and an overview of future research directions is given. Ref. [39] provided an overview of the cyber-physical security of SGs in terms of IDSs and communication standards and protocols. They presented the SG's vulnerabilities to cyberattacks with a focus on standards and protocols and introduced the different types of IDSs as well as some of the existing testbeds for SG cyber-physical security testing purposes. They also reviewed some of the threats

exploiting the vulnerabilities of SGs. A demonstration is given at the end of the paper where attacks and defense methods were simulated on a testbed. Ref. [88] introduced the types and metrics of both vulnerabilities and resilience in cyber-physical power systems, and reviewed analytical approaches in the literature for assessing each of the two. They also identified and discussed research gaps and future research opportunities. Ref. [89] introduce the cybersecurity challenges arising from the SG's structure and its different components. They discuss various possible attack scenarios and vectors and review possible defense strategies to protect the SG against intrusions and attacks. Ref. [90] introduced threat models and detailed attack characteristics, types, and impacts. They reviewed IDS, monitoring and visualization techniques, and co-simulation tools, while also discussing cyber-physical situational awareness, research challenges, and future directions.

With the rising need for defense methods against cyber-physical attacks on SGs, a significant number of research works have been published on attack detection, prevention, and mitigation methods. Many surveys have taken an interest in reviewing these works. Ref. [91] reviewed cyberattacks on SGs, highlighting the targeted component of each attack and the compromised security objective. They also reviewed detection techniques and possible countermeasures to such attacks. They also discussed research challenges and future directions. Ref. [92] reviewed vulnerabilities and security issues related to SGs and their possible outcome and impact. They introduced cyberattacks on SGs and presented a modeling of these attacks on the system to demonstrate their impact. A detailed review of works on detecting these attacks and protecting against them was also provided. Ref. [56] presented the different types of attacks on SGs in detail, reviewing attack scenarios from the literature and possible targets. A review of the existing detection mechanisms in the literature for each type of attack was then provided. New strategies using machine learning (ML), signal processing, blockchain, quantum computing, and big data analysis were also reviewed with their possible applications in securing SGs against cyberattacks. The role of cybersecurity in the future of SGs was also discussed. Ref. [93] examined the different cyber-physical attacks targeting SGs, their implementation and modeling, their impact, and their targets, reviewing relevant works in the literature. They also reviewed works on cyber-physical defense methods against these attacks. They discussed existing research challenges and opportunities. Ref. [94] reviewed cyberattacks, possible attack surfaces, and their impact and consequences in the literature. The concept of SG resilience to cyberattacks was discussed. The paper reviewed various works from the literature on the protection of SG from cyberattacks and the mitigation of their impact to achieve resiliency. Ref. [95] introduced different cyberattacks on SGs. They reviewed both attack scenarios and detection and protection schemes from the literature. They also reviewed works on the physical security of power systems and addressed current research limitations, challenges, and possible directions. Ref. [96] introduced cyberattacks threatening SGs, highlighting the causes that make SGs vulnerable to such attacks, and reviewed works in the literature on the vulnerabilities that exist in EV charging stations. They conducted a review of existing countermeasures in the literature and discussed challenges and future research directions. Ref. [97] reviewed some of the security challenges related to SGs. They reviewed the use of recent technologies, including blockchain, ML, and 5G in securing SGs. Ref. [98] took interest in the cybersecurity of the inverter-based SG, taking into account the integration of DERs, RESs, BESSs, and EV charging stations. First, the authors discussed vulnerabilities associated with various components of inverter-based SG, including DER; communication networks; Wide-Area Monitoring, Protection, and Control (WAMPAC); Internet-of-Things (IoT); AMI; renewable energy facilities; and EMS, along with the cyberattacks targeting them. They outlined potential attack scenarios and highlighted relevant studies from the literature. The review then focused on defense strategies, particularly

against FDI and DoS attacks, covering prevention, detection, and mitigation approaches. Additionally, they proposed a step-by-step framework for validating and assessing defense strategies, supported by relevant research. The authors also addressed research challenges and suggested future directions in the field. Ref. [99] focused on the security of WAMPAC systems in SGs. Authors reviewed vulnerabilities in the different components and standards within a WAMPAC system and presented the attacks threatening the system and its applications. Countermeasures were reviewed and categorized according to the WAMPAC system's security lifecycle, consisting of prevention, detection, mitigation and resilience, forensics, and deterrence. A security assessment of the different WAMPAC applications was provided, and testbeds used in WAMPAC security-related research were introduced, in addition to different security initiatives around the world. Moreover, they proposed recommendations for future research and discussed future directions. Ref. [100] reviewed the different cyberattacks on SGs and classified them according to the Open Systems Interconnection (OSI) model, extracting the targeted layers for each attack. They also reviewed attack detection techniques and countermeasures from the literature. Ref. [101] focused on both security and privacy aspects in SSGs. For each aspect, the authors described various attacks and examined the existing countermeasures reported in the literature. Ref. [102] introduced cyberattacks on SGs and reviewed attack scenarios on different parts of the SG. They reviewed countermeasures and classified them according to the NIST framework, i.e., identification, protection, detection, response, and recovery. Ref. [103] presented various attacks targeting SGs and examined existing countermeasures for each, along with potential research directions. Ref. [104] introduced SG architecture and its key components. The need for SG cybersecurity was highlighted through several vulnerabilities within its components and by reviewing the major cyber-physical attacks that occurred in the past. The authors also introduced cyberattacks on SGs, classifying them according to the CIA triad. Future directions included technologies requiring further research, such as blockchain, ML, cryptography, standards and protocols, digital Twins, and new cyberthreats. Ref. [105] provided an overview of the architecture of SGs and of the integration of IoT. Security challenges faced by SGs, as well as security objectives and requirements, were introduced. Cyberattacks were presented and classified according to the CIA triad. Moreover, more sophisticated attacks, such as the Stuxnet worm and Flame, were introduced. Countermeasures and solutions were also classified according to the CIA triad, solutions aiming to secure protocols and standards, and emerging technologies, such as blockchain and software-defined networks, where research challenges were discussed for each category. Lastly, the authors presented the possible future directions. In [106], an overview of SG components, communication protocols, and wireless sensor networks (WSNs) was given, followed by a list of cybersecurity incidents on CPSs. Attacks and countermeasures on SGs were reviewed and classified according to their target: the AMI, operational technology, and information technology. A framework for testing attacks on SGs was defined, with suggestions of different tools that can be used for simulating different grid components, and a case study was presented with flooding, jamming, and FDI attacks. Finally, challenges and future directions were presented. Ref. [107] presented the different layers in a SG architecture: business, application, communication, and power, its different systems including the AMI and SCADA, and the cybersecurity objectives. They introduced the different attacks threatening SGs, and eventually their countermeasures, grouping them according to the targeted cybersecurity objective. Countermeasures included encryption, blockchain, access management, and firewalls, in addition to diverse anomaly detection techniques.

Microgrids, as part of the main electric grid, have also evolved as smart microgrids and have become vulnerable to cyber-physical attacks as well. Although most security solutions designed for SGs are applicable to microgrids, researchers have also given particular

attention to the security of microgrids. Ref. [108] investigated research efforts on microgrid cybersecurity from multiple perspectives: microgrid communication, microgrid control, smart meters, testbeds, and impact analysis. Ref. [109] highlighted vulnerabilities related to microgrids and discussed the application of IEC 62351, Software-Defined Networking (SDN), IDSs, and resilient control strategies to enhance microgrid cybersecurity. Ref. [110] introduced the different cyberattacks targeting microgrids and reviewed the various cybersecurity schemes in the literature. They also reviewed resilient control schemes to protect microgrids against cyberattacks and discussed future research directions.

Standards and protocols represent a main factor in the cyber-physical security of SGs, as they offer many vulnerabilities for attackers to exploit on the one hand, and they can be improved to enhance the security of SGs on the other hand. Ref. [33] provided a review on the cyber-physical security of SGs in regard to standards and protocols. A review on the communication technologies, standards, and protocols used in SGs was provided. Cybersecurity objectives, requirements, and key components were discussed. Cybersecurity standards and protocols were reviewed, and the scope, type, and applicability of each were provided. A detailed discussion on challenges and opportunities in research on SG cybersecurity was provided, as well as recommendations for future trends. Ref. [111] reviewed standards addressing security issues in SGs. The reviewed standards were categorized according to their application area, followed by a discussion on privacy.

#### *4.2. Focused Analysis of Attack-Specific Surveys in SG Cybersecurity*

Many researchers have focused on a particular attack in their reviews. FDI is by far the most covered attack by research on the cybersecurity of SGs. Analogously, many literature reviews have focused on FDI attacks, their implementation, impact, and countermeasures. As the first review on the topic, ref. [59] introduced four scenarios for constructing an FDI vector under different circumstances. This review examined literature on the impact of FDI on power systems and discussed various countermeasures. Ref. [58] focused on FDI attacks targeting state estimation in power systems, reviewing the construction of the attack and the requirements to do so. Works on the impact of FDI attacks on the electricity market's operations were reviewed. The paper also reviewed existing defense methods against the attack. Ref. [2] reviewed works depicting how vulnerabilities can be exploited on the different levels of the SG's cyber-physical structure to deliver FDI attacks, as well as works analyzing their impact. The paper also reviewed existing algorithms in the literature for the detection of FDI attacks. Ref. [112] focused on FDI attacks on microgrids, reviewing their economic and physical impact, as well as the different methods for constructing the attack. Ref. [113] reviewed advances in FDI attacks. They proposed different classifications for FDI attacks based on the attack model, target, and impact. They discussed vulnerabilities related to the SG's cyber-physical elements and reviewed the impact of different FDI attack types on the SG structure. Research gaps and future research directions were also discussed. Ref. [114] focused on profit-oriented FDI attacks on the electricity market. Works on both FDI attacks and countermeasures were reviewed and categorized. Ref. [115] categorizes FDI attacks according to their target (end users, field devices, control center, energy trading). For each target, works presenting advances in FDI attacks were reviewed. Ref. [116] focused on countermeasures that perform the joint detection and localization of FDI attacks. The reviewed papers are separated into those using data-driven modeling and those using mathematical modeling. The paper discussed localization techniques used in each of the reviewed works, evaluation methodologies, the adversary's knowledge, and metrics used for the evaluation of ML techniques. Open issues and research directions were also introduced. Ref. [117] conducted a literature review of works handling the impact of FDI attacks on the energy market. Ref. [118] introduced FDI attacks on WSN

and their applications in SGs. The attack scenarios are compared to previous studies on wired systems. Ref. [119] introduced FDI attacks, which were categorized into FDI, replay, and zero-dynamic attacks. They reviewed ML-based detection methods, which were grouped according to the attack scenario: abnormal energy consumption, attacks on state estimation, and attacks on load forecasting. Research challenges and future directions were also discussed. Ref. [120] introduced the different types of FDI attacks and classified them according to the targeted subsystem and according to the impact of the attack. Countermeasures against FDI in the literature were reviewed and categorized into detective, reactive, and preventive methods. The review also discussed research challenges and future directions. Ref. [121] reviewed research focused on improving FDI detection accuracy and computational efficiency. Detection methods from the literature were also examined, including ML-based, state estimation, and game theory approaches.

Researchers have paid attention to other attacks as well. As the only review focusing on replay attacks, ref. [122] examined countermeasures against these attacks on SGs. The reviewed works were categorized based on their methods, including ML, watermarking, cryptography, and game-theory. Ref. [40] reviewed DoS attacks on SGs and classified them based on the targeted part of the grid (generation, transmission, etc.), the affected communication protocol, and the targeted SG application (AMI, DMS, etc.). The review also examined countermeasures and solutions from the literature, categorizing them according to the techniques they employ. Future directions were also presented. Ref. [123] reviewed DoS attacks on the LTE infrastructure used in SGs and examined possible countermeasures. Ref. [50] also reviewed DoS attacks against SGs, focusing on detection and mitigation techniques using reinforcement learning (RL). Ref. [124] introduced different attack models for data-driven energy theft and reviewed different attack strategies for implementing such attacks. Additionally, data-driven detection methods from the literature were analyzed. Ref. [125] introduced the types of energy theft and reviewed different detection techniques. They also provided a comparative analysis of countermeasures and discussed research challenges and future directions. Ref. [126] presented electricity theft methods and scenarios on different types of meters, including smart meters. An extensive review of both existing ML-based detection techniques and measurement mismatch-based detection methods was provided, followed by a comparative discussion of the two types of methods. The paper also included a discussion of future research directions.

#### *4.3. Focused Analysis of Method-Specific Surveys in SG Cybersecurity*

Other review papers on countermeasures and solutions for the SG's cyber-physical security have concentrated on specific methods, such as ML, blockchain, and cryptography. Research that delves into ML encompasses the works of [127–130]. Ref. [127] provided a set of guidelines for the selection of an ML model for threat detection in the context of SGs. ML-based countermeasures in the literature were reviewed and classified according to the CIA triad, and for each objective, works were divided into conventional ML and deep learning (DL) models. The paper also discussed future research directions. Ref. [128] reviewed ML techniques from the literature aiming to secure SGs against attacks, such as RL, recurrent neural networks, generative adversarial networks, and deep belief networks. Ref. [129] reviewed works using ML techniques to conduct cyber-physical attacks on SGs. They also reviewed ML-based countermeasures from the literature. Ref. [130] reviewed ML-based countermeasures in the literature. The authors then focused on ensemble learning, DL, and RL methods, categorizing them into detection, localization, and mitigation techniques. Ref. [119] focused on ML-based countermeasures against FDI attacks. Ref. [131] introduced cyberattacks threatening microgrids and reviewed AI-based and ML-based attack detection and mitigation techniques from the literature. The authors then focused on

learning-based attack detection and mitigation techniques. Refs. [50,132,133] specifically focused on DL algorithms. Ref. [132] summarized literature on using DL models to secure SGs against attacks, while ref. [50], mentioned previously in Section 4.2, reviewed DL algorithms for detecting DoS attacks on SGs. Ref. [133] examined research on employing DL to develop IDSs for the protection of SCADA systems. The authors also presented research challenges and open issues. Ref. [134] provided an overview of SG communication networks, the AMI, SCADA, security requirements for SG cybersecurity, and vulnerabilities. They presented attacks and classified threats according to the targeted layer (device, data, privacy, network). The paper extensively reviewed literature on countermeasures using ML and DL, such as RNNs, Autoencoders, Random Forest, and Ensemble Learning, dividing them into centralized learning and federated learning-based approaches. Reviewed works were compared in terms of algorithm, attack, dataset, limitations, real-world applications, and potential biases. The paper also discussed opportunities for future work. Ref. [135] focused on large language models for SG cybersecurity. They introduced three layers in the SG architecture: the physical layer, comprising generation, transmission, distribution, and consumption; the cyber-physical layer, including control and measurement components; and the cyber layer, encompassing the network, management, and application levels. Additionally, the paper introduced communication protocols, as well as cybersecurity requirements and challenges. Cyberattacks were presented and classified according to the targeted level (network-based, data-based, and user-based attacks), the attack knowledge level (low, moderate, high), the CIA triad, the attack layer (cyber and cyber-physical), and according to the NIST SG domains defined in [136]. Protection and detection techniques, such as encryption, ML and DL algorithms, and the usage of PMUs were reviewed. The paper discussed the challenges and limitations of these techniques before introducing large language models and exploring their application to SG cybersecurity, as well as an enabler of cyberattacks. Research challenges and future directions were also discussed. Ref. [137] focused on physics-based anomaly detection for attack detection in SGs. The paper reviewed various ML and DL-based solutions from the literature. The paper compared works in terms of the targeted component, validation process (dataset vs. simulation), proposed algorithm, and performance according to the most significant metric.

Cryptography and key management schemes have been widely used for the protection of SG communications. Ref. [138] evaluated existing public key infrastructure (PKI) trust models and their applicability for SG cybersecurity. Ref. [139] reviewed key management schemes proposed in the literature for the SG. Ref. [140] reviewed and compared works proposing key algorithms relevant to SGs, and discussed some related research issues. Ref. [141] focused on key management approaches in the SG's AMI. The surveyed works were classified according to the technique they used, followed by a comparative discussion. Future research directions were discussed as well. As to blockchain, ref. [142] provided an overview of blockchain for SG cybersecurity and introduced its architecture and development platforms in the context of SGs. They reviewed research on the integration of blockchain for the SG's cybersecurity in field measurement and communications, power generation and transmission, as well as power distribution and utilization. Future research directions for blockchain in SG cybersecurity were also discussed. Ref. [143] reviewed blockchain solutions in the literature for privacy protection, identity authentication, and data aggregation in the context of SGs.

Surveys concentrating on other methods are also available; for instance, ref. [144] examined quantum key distribution protocols applicable to SG communications. The reviewed works were categorized based on the specific challenges they address, such as the extended coverage area of SGs and the high number of control devices.

#### 4.4. Focused Analysis of Component-Specific Surveys in SG Cybersecurity

Some surveys are dedicated to exploring specific grid components in depth, with the AMI—a key pillar of the SG concept—being a prominent focus. For instance, ref. [145] reviewed privacy protection schemes for smart meter data under the trusted operator model and discussed issues related to these solutions. Then, privacy protection schemes under the non-trusted operator model were reviewed. Challenges and future directions were also discussed. Ref. [146] identified different vulnerabilities in the AMI's embedded systems, applications and networks, as well as threat targets. The authors reviewed different threats to system-level security, metering services, and privacy in the SG's AMI. An extensive review of countermeasures for each category of threats was then provided, and the pros and cons of each countermeasure were evaluated. Research challenges and future directions were also discussed. Ref. [147] reviewed some of the existing defense mechanisms for protecting smart meters in the literature and compared them. Some future research directions were proposed as well. Ref. [148] discussed vulnerabilities present in AMI components and possible attack vectors on the hardware, data, and communication layers, as well as their impact on the infrastructure. Different countermeasures from the literature were reviewed and discussed. Research challenges and future directions were presented as well. Ref. [149] focused on privacy-preserving schemes for SG metering in their literature review. Works were classified into studies based on attributable measurements and those on non-attributable measurements. The reviewed works were further categorized according to other criteria, such as the usage of aggregation and cryptography. Some future research directions were also presented. Ref. [141] reviewed some of the security issues related to the AMI and existing key management approaches used in the AMI from the literature. Ref. [150] presented different attack vectors and techniques on the AMI, as well as their impact. They reviewed IDSs against attacks on the AMI from the literature. The reviewed works were categorized according to the type of the proposed IDS. The authors also provided a set of recommendations on the deployment of IDSs for the AMI and discussed research challenges. Ref. [126]'s work focused on energy-theft attacks targeting energy meters.

Other surveys have provided an in-depth focus on DERs and their various components, including electronics [151,152], BESSs [153,154], and RESs [155]. For instance, ref. [151] explored multiple attack scenarios and vulnerabilities specifically related to smart inverters. Countermeasures to these attacks from the literature were reviewed, encompassing both system-level and device-level solutions. Ref. [152] examined vulnerabilities and attack vectors associated with grid-connected power electronic converters. The review then covered countermeasures, categorizing them into mitigation techniques for the cyber and physical layers, along with their alignment with security standards and protocols. Additionally, the review addressed relevant testbeds for cybersecurity testing and provided recommendations for future research. Ref. [153] introduced different battery technologies and subsystems, as well as their vulnerabilities and cyberattacks targeting them. An extensive literature review on countermeasures against attacks on BESSs was then provided, and research gaps and future directions were discussed. Security standards were also reviewed and discussed. Ref. [154] introduced attacks targeting BESSs as well as existing detection and prevention techniques. Reviews on both residual-based and long-term pattern-based approaches for attack detection were then provided. Ref. [156] identified vulnerabilities in DER interfaces and attacks targeting DERs. The paper also reviewed works on security measures, mechanisms aiming to secure protocols and security standards. A discussion of research challenges and future directions was also included. Ref. [155] reviewed vulnerabilities in IoT-based microgrid RES and attacks threatening them. Ref. [157] presented a multilayer architecture of DER systems, highlighting the different stakeholders, management platforms, communication interfaces and protocols, and cybersecurity risks. The

authors also presented the different cybersecurity requirements for DERs, consisting of authentication and integrity, criticality rating, communication partitioning, boundary protection, security management, and security compliance. Security guidelines and standards were also reviewed. The paper presented the vulnerabilities corresponding to each level of the multilayer architecture, and the impact of attacks on DER systems was discussed through different possible scenarios. The authors also reviewed countermeasures from the literature, classifying them into prevention, detection, and mitigation techniques, and according to the level that they aim to protect. Finally, research challenges and opportunities in terms of emerging technologies were discussed.

Numerous surveys have examined the security of SCADA systems. Ref. [158] provided an in-depth review of risk assessment methods applicable to SCADA systems. Meanwhile, ref. [159] explored security issues and vulnerabilities, discussed attacks targeting SCADA systems, and reviewed existing security testbeds. This survey also included a comprehensive review of efforts to secure SCADA systems, with a focus on protocols used by these systems.

A review of the literature on the survivability and resilience of SCADA systems was also conducted. Ref. [160] explored advanced solutions for securing fog-based SG SCADA systems, encompassing authentication mechanisms, privacy-preserving techniques, key management frameworks, and IDSs. Additionally, the review highlighted pertinent research challenges in this domain. Existing surveys offer a comprehensive overview of these solutions and challenges. Ref. [74] introduced vulnerabilities within SCADA systems. Attacks on SCADA systems were presented and categorized according to various criteria, including the type of attack, the target, and the impact of the attack. A review on IDSs was provided, and classifications of IDSs, ML techniques, and feature extraction techniques were included as well. Existing testbeds, as well as some cybersecurity controls and mitigation mechanisms, were discussed. The paper also presented related research challenges. Ref. [161] highlighted attacks on SCADA systems and reviewed cryptography-based and formal verification-based solutions. Ref. [162] reviewed research works on attacks threatening RTUs and discussed vulnerabilities. Ref. [133], presented in Section 4.3, reviewed works using DL algorithms in the development of IDSs for SCADA systems.

Researchers have also focused on other parts of the SG, such as communications networks [163–165], PMUs [166], SG data [167], and vehicle-to-grid (V2G) networks [168,169]. Ref. [163] highlighted challenges related to the cybersecurity of SG communications and reviewed solutions for each cybersecurity requirement (privacy, integrity, authentication, trusted computing). Ref. [164] focused on cognitive radio-based SG communications. They reviewed cognitive radio standards used in SGs along with their associated security issues and vulnerabilities to attacks. The survey also examined security technologies and standards and discussed relevant research challenges. Ref. [165] discussed security issues related to the usage of WSNs in SGs and reviewed possible attacks. Countermeasures, including IDSs and topology control methods, were also reviewed. Ref. [170] discussed attacks on cognitive WSNs and countermeasures. Ref. [171] reviewed security issues and attack scenarios threatening PLCs, as well as protection schemes in the literature and security recommendations. Ref. [166] reviewed research works on vulnerabilities and attacks targeting synchrophasor networks. Ref. [172] presented the different applications of WSNs within the SG architecture and the communication protocols used by each SG network. The authors reviewed existing works in the literature focused on securing WSNs in the context of SGs, including access control, secure routing, secure clustering, and encryption. Attacks and countermeasures are also reviewed, including blockchain and SDN.

Surveys focusing on SGs data address aspects including data management, analysis, and security. Ref. [167] focused on the security of SG data throughout its life cycle (genera-

tion, acquisition, storage and processing). For each stage, related vulnerabilities and attacks on different components and processes of the SG were reviewed from existing literature. The paper then reviewed research on potential data sources for security analytics in SG, as well as data analysis and visualization methods. Future research directions were also discussed.

Surveys focusing on V2G systems address aspects including communication protocols, security challenges, and integration strategies. Ref. [168] examined threats associated with both physical and communication-related V2G connections and explored potential mitigation strategies. Ref. [169] introduced privacy issues and challenges in V2G networks and identified potential attacks. Privacy preservation techniques from the literature were then reviewed and categorized based on the methods they employ. Both the advantages and limitations of existing solutions were discussed. In [173], potential attack vectors and scenarios threatening power systems IEDs were reviewed and categorized based on their target and the type of attack scenario. The review also examined existing countermeasures, classifying them according to the level of protection they offer.

Surveys related to IoT in SGs explore aspects like connectivity, data interoperability, and security challenges. For instance, ref. [174] discussed security and privacy implications and challenges related to the integration of IoT in SGs. Ref. [175] discussed security challenges related to the IoT-based SG, presenting common attacks, possible mitigation techniques, and prospects. Ref. [176] focused on the energy-aware smart home environment and its interaction with the SG environment. They discussed attack scenarios arising from the interactions between smart homes and SGs, as well as their impact. Countermeasures outlined in the existing literature were thoroughly reviewed, alongside cybersecurity standards for SGs. The paper also discussed future directions. Ref. [177] provided a comprehensive review of the security of smart substations, covering attacks, vulnerabilities, and associated security issues. The survey also examined attack detection methods and protection schemes from the literature, along with datasets, testbeds, and pertinent security standards. The authors also proposed a multilayered protection scheme and discussed open challenges and future directions. Ref. [178] reviewed cyberattacks on the load frequency control system of the SG. Attack detection techniques were reviewed and categorized into model-based and data-based approaches, along with additional methods such as watermarking and game theory. Mitigation techniques were also reviewed. The authors discussed testbeds, as well as the major steps in vulnerability assessment. Research gaps were also identified and discussed.

## 5. Overview of Key Research Aspects in Smart Grid Cybersecurity

In the previous section, we reviewed existing surveys on the cyber-physical security of SGs. Each paper presented concepts related to the topic, attack and/or countermeasure classifications, research challenges, and future directions. In the following subsections, we will discuss the different aspects related to research on SG cybersecurity, derived from the previously reviewed papers.

### 5.1. Taxonomies

In Section 3, we discussed various cyber-physical attacks targeting SGs, such as FDI, DoS, MitM, GPS spoofing, and replay attacks. Nevertheless, the literature also reveals additional threats, including reconnaissance [91,92], sniffing [179], delay [90,95,99,102], and covert [56,110]. Reconnaissance normally precedes other attacks, allowing an attacker to gather information on their target, usually through traffic analysis. An attacker performs sniffing to monitor and capture data traffic. An MitM attack involves an attacker intercepting information circulating in a network; hence, reconnaissance and traffic analysis may be considered as MitM attacks. Message delay attacks include introducing a delay in the transmission of data packets, possibly destabilizing the grid's operation since SG

applications are time-critical. In Section 3, we defined DoS as an attack that either delays or completely prevents the transmission of data or the delivery of services. Therefore, we consider any attack aiming to delay the transmission of data, including message delay attacks, as DoS attacks. Ref. [90] also considered delay attacks as DoS attacks. A covert attack refers to an attack that aims to alter measurements, with a remarkable capability of evading detection [180,181]. Following the definition of FDI, a covert attack can be considered a stealthy FDI attack.

Our analysis of the surveyed literature also highlights additional attacks, including aurora attacks [90,93], load redistribution attacks [90,93,102], topology attacks [93,128], automatic generation control (AGC) attacks [90,93], and switching attacks [102,129], all of which have been addressed in the reviewed surveys. These are more sophisticated attacks that typically involve a combination of several previously discussed attacks, making them more complex and challenging to address, and have a specific target. The aurora attack involves opening a generator's circuit breaker to disrupt synchronization and then reclosing it before the system can respond [93]. This results in mechanical and electrical stress on the generator, and repeating the process will eventually damage the generator [182]. A load redistribution attack is delivered through an FDI attack by manipulating measurements of load buses and line power flow measurements [93], possibly leading to unnecessary load shedding or to an insecure operating state where the power flow on a transmission line may exceed its capacity, eventually leading to outages [183]. A topology attack aims to alter both network data and meter measurements [128]. Attacks targeting the AGC modify power flow measurements to destabilize the system [90,93].

Various classifications for cyber-physical attacks on SGs were proposed by researchers in the previously reviewed surveys. The most common classification criteria are the CIA triad, the attack layer, and the attack target (Table 5). In classifications based on the CIA triad, DoS, including jamming, falls within the class of attacks targeting availability [33,87,91]. Integrity attacks are FDI, replay and GPS spoofing [33,56,87,99]. Although MitM is generally considered to violate confidentiality, since it allows an attacker to intercept data, it can also violate integrity since it can be used to alter data as well [33,87,91]. Attack layers include network layers from the OSI and TCP/IP models [87,100], in addition to the cyber and physical layers [2,56].

**Table 5.** Attack classifications in reviewed surveys.

| Classification Criteria | Refs.                      |
|-------------------------|----------------------------|
| CIA triad               | [33,87,104,105,135]        |
| Target                  | [86,93,98,102,105,106,135] |
| Layer                   | [2,56,87,100,105,134,135]  |

A variety of classifications categorize countermeasures based on the method or technique they use, such as cryptography, ML, blockchain, signal processing, filtering techniques, moving target defense, game theory, and watermarking. More general classifications may divide methods into data-driven and model-based, or according to the countermeasure's role (prevention, detection, mitigation, localization). Countermeasures are also commonly classified according to the attack they address, or, more generally, the attack type. Ref. [92]'s attack types included periodic, stochastic, and arbitrary attacks, whereas [95]'s consisted of direct and indirect attacks. Refs. [91,97] considered attack phases when classifying countermeasures (pre-attack, under attack, and post-attack). The targeted device, system, security requirement, or layer is also a common criterion for classifying countermeasures. Table 6 summarizes the different classification criteria used in the reviewed papers.

**Table 6.** Classification criteria used for countermeasures in reviewed surveys.

| Ref.  | Method | Role | Target | M vs. D | Attack | Att. Type | Att. Phases |
|-------|--------|------|--------|---------|--------|-----------|-------------|
| [91]  | -      | -    | ✓      | -       | -      | -         | ✓           |
| [92]  | -      | -    | -      | -       | -      | ✓         | -           |
| [56]  | -      | -    | -      | -       | ✓      | -         | -           |
| [93]  | ✓      | -    | -      | -       | -      | -         | -           |
| [95]  | -      | -    | -      | -       | ✓      | ✓         | -           |
| [96]  | ✓      | -    | -      | -       | -      | -         | -           |
| [97]  | ✓      | -    | -      | -       | -      | -         | ✓           |
| [98]  | ✓      | -    | -      | -       | ✓      | -         | -           |
| [100] | ✓      | ✓    | -      | -       | -      | -         | -           |
| [101] | ✓      | -    | -      | -       | ✓      | -         | -           |
| [89]  | -      | -    | ✓      | -       | -      | -         | -           |
| [99]  | -      | ✓    | -      | -       | -      | -         | -           |
| [90]  | ✓      | -    | -      | -       | -      | -         | -           |
| [103] | -      | -    | -      | -       | ✓      | -         | -           |
| [2]   | -      | -    | -      | ✓       | -      | -         | -           |
| [116] | -      | -    | -      | ✓       | -      | -         | -           |
| [120] | -      | -    | -      | -       | -      | -         | -           |
| [122] | -      | ✓    | -      | -       | -      | -         | -           |
| [40]  | ✓      | -    | ✓      | -       | -      | -         | -           |
| [123] | ✓      | -    | -      | -       | -      | -         | -           |
| [124] | -      | -    | -      | -       | -      | ✓         | -           |
| [125] | ✓      | -    | -      | -       | -      | -         | -           |
| [126] | ✓      | -    | -      | -       | -      | -         | -           |
| [146] | ✓      | -    | -      | -       | -      | -         | -           |
| [147] | -      | -    | ✓      | -       | -      | -         | -           |
| [148] | ✓      | -    | -      | -       | -      | -         | -           |
| [153] | ✓      | -    | -      | -       | -      | -         | -           |
| [160] | ✓      | -    | -      | -       | -      | -         | -           |
| [74]  | ✓      | ✓    | -      | -       | -      | -         | -           |
| [161] | ✓      | -    | -      | -       | -      | -         | -           |
| [163] | ✓      | -    | ✓      | -       | -      | -         | -           |
| [173] | -      | -    | ✓      | -       | -      | -         | -           |
| [175] | -      | -    | -      | -       | -      | -         | -           |
| [176] | ✓      | -    | ✓      | -       | -      | -         | -           |
| [178] | -      | ✓    | -      | ✓       | -      | ✓         | -           |
| [105] | ✓      | ✓    | -      | -       | -      | -         | -           |
| [157] | ✓      | ✓    | ✓      | -       | -      | -         | -           |
| [106] | -      | -    | ✓      | -       | -      | -         | -           |
| [107] | -      | -    | ✓      | -       | -      | -         | -           |
| [134] | ✓      | -    | -      | -       | -      | -         | -           |
| [135] | ✓      | -    | -      | -       | -      | -         | -           |

M vs. D: model-based vs. data-driven; Att.: Attack.

## 5.2. Discussion

Countermeasures against cyber-physical attacks on SGs can be divided into three categories: attack detection, attack mitigation, and attack prevention. These countermeasures contribute to achieving grid resilience (Figure 17). Attack detection refers to identifying and recognizing the presence of an attack or unauthorized access to one or multiple components or systems in the SG. Detection techniques should be able to differentiate between arbitrary system faults and malicious attacks. In addition to detection, some research works provide attack localization, which involves identifying which component or part of the grid was compromised. The detection of an attack is often followed by mitigation. Attack mitigation is a set of corrective actions aiming to reduce the attack's impact on the system's stability

and performance. The efficiency of a mitigation approach is highly dependent on the reliability of the detection approach that precedes it [93]. Attack prevention, as the name suggests, completely prevents the occurrence of an attack and is, therefore, a more secure approach. However, it generally necessitates securing each component individually, which tends to be computationally expensive, possibly unfeasible [98]. Finally, the resilience of an SG against cyber-physical attacks and threats refers to its capability of maintaining a normal operational state, even when under attack [98]. Thus, grid resilience reduces the possibility of power outages caused by attacks [94].

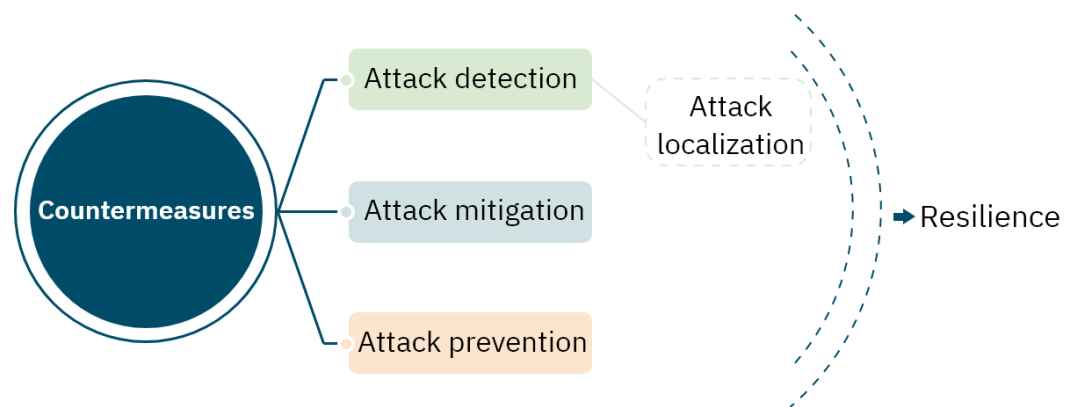


**Figure 17.** Classification of countermeasures.

Numerous survey papers have focused on particular techniques in research on attack countermeasures for SGs, both classical and recent. Classical techniques include cryptography, watermarking, moving target defense, signal processing, and game theory. Cryptography and key management schemes are perhaps the most prevalent classical techniques found in the literature, and they have been the central focus of many survey papers [40,91,98,101,122,138–141,148,161,175]. Cryptography is mostly used for preventing attacks on SGs [98,100], although it can also be used for attack detection, such as in [66]. Watermarking is used for attack detection, and it involves embedding an authenticating signal into data packets so that their authenticity and integrity can later be verified [122]. Moving target defense prevents attacks through constantly changing system configuration to reduce the attack surface, making it harder for attackers to deliver attacks by increasing uncertainty [93]. In game theory, a game is played between players, in either a cooperative or a competitive manner to defend against attacks, as well as determining malicious nodes [147].

Analysis shows that component-specific surveys were prevalent from 2012 to 2019. This results from the model-dependent nature of countermeasures, such as conventional IDSs, firewalls, watermarking, and Kalman filters. These countermeasures are tailored specifically to secure a particular component or system. With the rise of data-driven (i.e., model-independent) countermeasures, the number of component-specific surveys has visibly decreased (Figure 18). From 2020 onward, a clear decline in component-specific surveys can be observed, paralleled by a steady increase in method-specific ones. Method-specific surveys before 2020 focused on encryption-based techniques, since authentication, encryption, and PKI were the main strategies for attack prevention. Since 2020, a notable shift toward ML-focused surveys has been observed, along with the emergence of surveys addressing Blockchain and Quantum Computing (Figure 19). Furthermore, the number of surveys in the field of SG cybersecurity has steadily increased since the first publication in 2011, with a particularly sharp rise after 2020 (Figure 20). Figure 21 illustrates the different shifts in research trends and number of publications survey papers between 2011 and 2025.

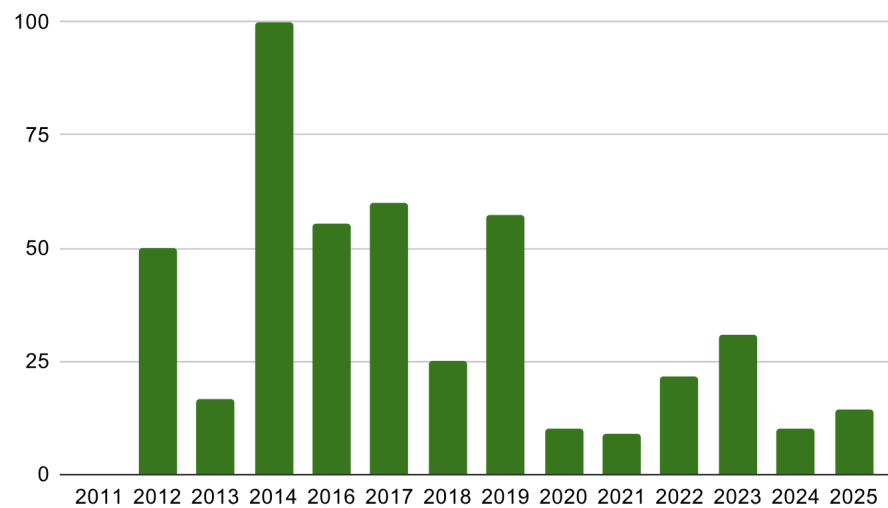


**Figure 18.** Percentage of component-specific surveys relative to the total number of surveys per year.

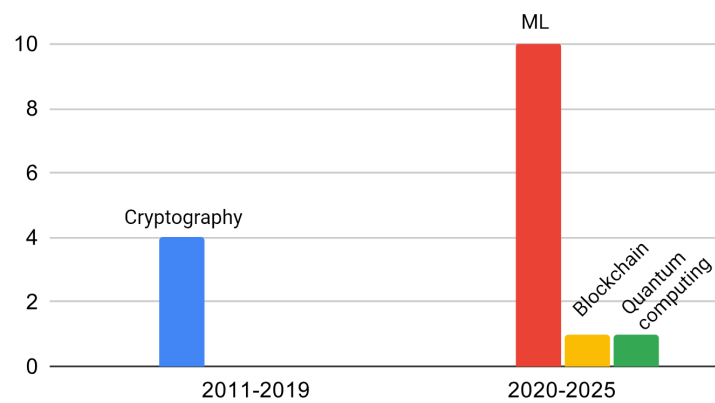


**Figure 19.** Distribution of method-specific surveys.

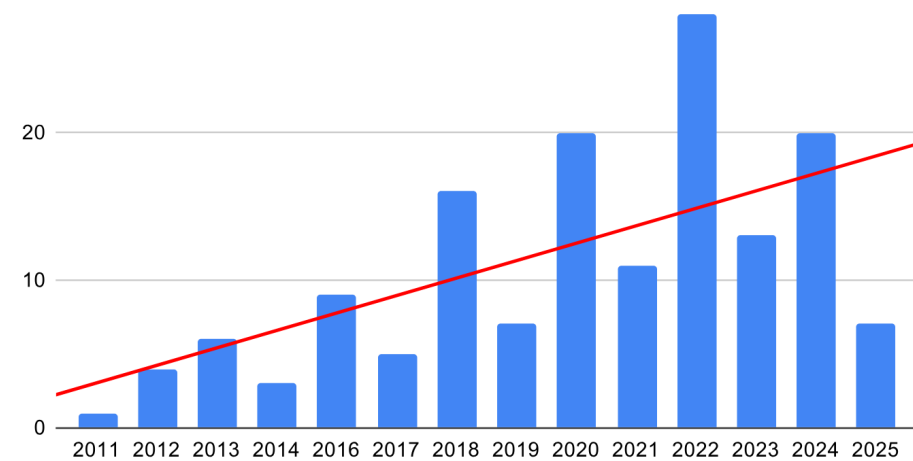


**Figure 20.** Distribution of surveys per year.

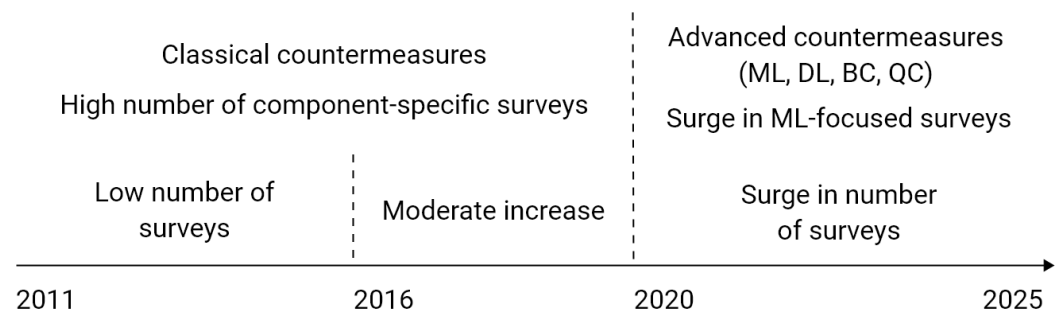


**Figure 21.** Trends in survey papers from 2011 to 2025.

Emerging technologies, such as ML, blockchain, cloud computing, and quantum computing, have attracted growing interest from researchers in the context of SG cyber-physical security, with ML being the most widely studied (Figure 22). This is encouraged by the fact that ML algorithms are model-independent, allowing their generalization over various components and systems in the SG. With the rising complexity of the SG's cyber-physical structure, it has become difficult to model the system and design countermeasures accordingly. Moreover, any changes in the structure will affect the applicability of model-based countermeasures. ML algorithms offer a robust solution for attack detection, as they can uncover hidden and complex patterns within data. Consequently, ML-based solutions are rapidly growing compared to those using other techniques, as ML algorithms enable not only attack detection but also localization. Figure 23 shows the different surveys that focused on ML-based countermeasures. Blockchain also emerged as a promising solution for secure SG communications [143]. Its decentralized nature offers lower costs, complementing conventional encryption, authentication, network IDSs, and firewalls [142]. Moreover, blockchain minimizes the risk of a single point of failure through the usage of distributed ledgers, ensuring that the SG maintains its operations even if one of its nodes is compromised [104]. With the proliferation of IoT devices in SGs, cloud computing offers attractive features for SGs. For instance, aggregated smart meter data can be processed by powerful online servers running robust attack detection modules [184]. The literature also views quantum computing as a promising technology for ensuring SG cybersecurity. In theory, quantum keys are unbreakable. Therefore, systems implementing quantum key exhibit a high level of security, preventing even the stealthiest intrusions such as eavesdropping [144].

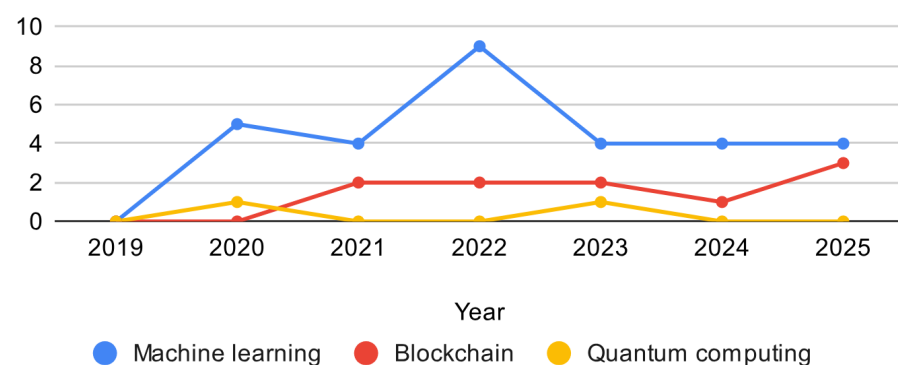


**Figure 22.** Number of surveys with a partial/full focus on recent technologies.

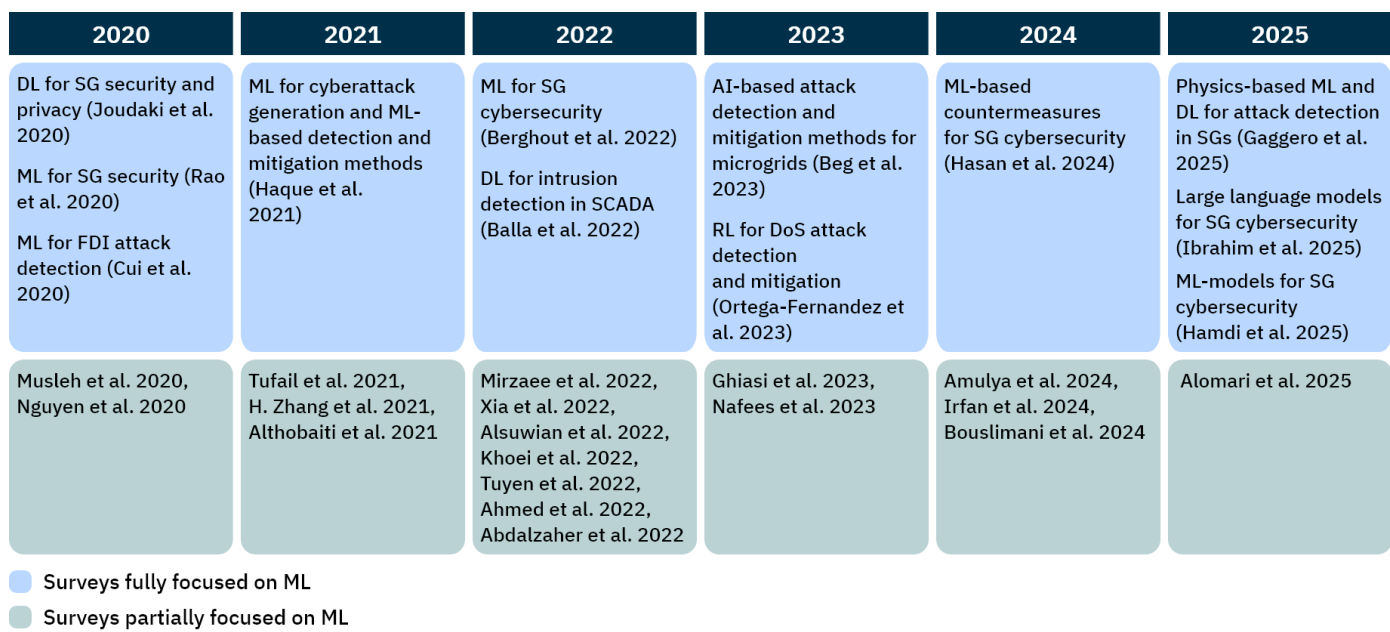


**Figure 23.** Surveys reviewing ML-based countermeasures [2,50,56,90,93,94,96–98,100,101,104,116,119,122,124–135,137,147,178].

FDI is arguably the most researched attack in the context of SG cyber-physical security (Figure 24). This is because an FDI attack involves inserting malicious information, such as altered measurements, which, undetected, may lead to wrong decisions and, eventually, devastating consequences. A well-structured FDI vector has the ability to evade detection and compromise the grid’s stability and availability. Moreover, FDI can be delivered through multiple layers (communication network, cyber layer, physical layer) [2].

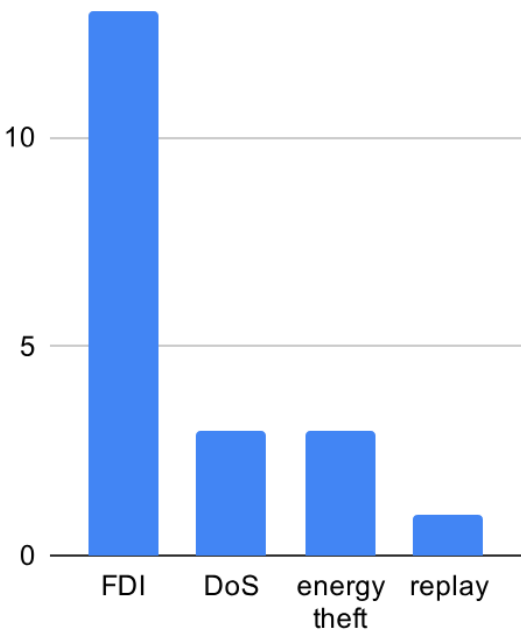


**Figure 24.** Number of survey papers focused on a specific attack.

6. Emerging Research Challenges and Future Directions in Smart Grid Cybersecurity

This section highlights some of the common research challenges and future directions proposed in literature reviews on SG cyber-physical security. We only selected recent papers for this discussion, i.e., papers published in the past 5 years.

## 6.1. Smart Grid Cyber-Physical Structure

### 6.1.1. Current Research Challenges

Compared to transmission systems, distribution systems have not received enough focus in terms of research on cyber-physical security [33,93,103]. The complexity of the distribution grid has increased with the integration of DERs, EV charging stations, and IoT devices in the AMI [93,116]. Consequently, the distribution grid has ended up with a larger attack surface and an increased number of vulnerabilities. Furthermore, many emerging areas of the SG are underresearched in terms of security, such as DERs [113], power electronics [152], and the AMI [93]. On the microgrid level, most existing works have focused on either DC microgrids or AC microgrids. However, there hasn't been enough research on hybrid AC/DC microgrids in terms of attack detection, mitigation, and resilient control [98,110]. Hybrid microgrids present a higher number of vulnerabilities, and the presence of both DC-based and AC-based devices increases the difficulty of modeling the system and of designing countermeasures [98].

For simplification purposes, many research works have tended to approximate the non-linearity of AC-based models into linear DC models, notably in modeling the SG for research on FDI attacks, which could result in inapplicable and inefficient solutions [99,113].

The interdependence between the cyber and physical layers of an SG can be exploited by attackers to cause physical damage by leveraging vulnerabilities in the cyber layer [93]. However, it has been underinvestigated, as most research works focus exclusively on either the cyber layer or the physical layer [33,40,88].

### 6.1.2. Proposed Future Directions

Further research on the distribution grid is required, by identifying its different stakeholders and the vulnerabilities of each, before attempting to implement protective measures against attacks. Adopting model-independent solutions that can generalize across emerging components is recommended, ensuring their reproducibility and durability. Thanks to their data-driven nature, ML algorithms can adapt to both the AC and hybrid microgrid models, eliminating the need to resort to the simplified, DC model. Hardware-in-the-loop can be exploited to identify all possible attack vectors and scenarios that leverage the interdependence between the cyber and physical layers, identifying the weakest links before implementing protection measures for both layers.

## 6.2. Advancements in Countermeasure Development

### 6.2.1. Current Research Challenges

One of the most persistent challenges in developing security solutions for CPSs, particularly SGs, is related to datasets [74,116,133,160]. Ground-truth datasets are essential for implementing and evaluating security solutions for SGs and are crucial for training data-driven models. The quality of a dataset is an important factor that determines the robustness of learning-based methods and can reduce the resulting number of false positives and false negatives [116]. Moreover, data-driven solutions require datasets to be up-to-date [116,133]. However, datasets are often either too general to be used in securing a particular component or system of the SG, or outdated [74,160]. Data imbalance is another drawback in existing datasets, where the percentage of abnormal (or malicious) records is generally low [126,133].

Another challenge is ensuring countermeasures' reproducibility. This is because most, if not all countermeasures are implemented under less realistic conditions, such as simulations, affecting their applicability in real-life situations [125,146]. For instance, communication delays and resource-constrained conditions are often not considered in the design of countermeasures and secure control schemes [99,110,177]. Simulators and testbeds are crucial elements in evaluating the performance of proposed security measures.

Existing simulations provide small-scale representations of the system, which could affect the robustness and efficiency of tested solutions [116]. Furthermore, with the increasing complexity in the SG's structure, notably on the distribution side, most existing simulations have become outdated and no longer represent the structure [33]. Therefore, there is a need for simulation tools with hardware-in-the-loop (HIL) capabilities that represent both the cyber and physical aspects of the SG [93].

The robustness of mitigation solutions is highly dependent on the reliability of the detection process [93]. Although a plethora of research works have developed and adapted IDSs to detect attacks on SGs, there hasn't been as much research on intrusion prevention [74,125,177]. The reliability of attack detection methods and IDSs can also be highly impacted by the presence of false positives and false negatives, even though they may seem promising when using other metrics such as accuracy [99,125,177]. Vulnerability assessment and risk analysis are an important step in developing mitigation schemes. Due to the complex structure of the grid, current research lacks a comprehensive understanding of all vulnerabilities and attack vectors [178]. It also faces challenges due to the lack of adequate datasets [33].

Privacy preservation has become an important aspect in the development of countermeasures and security schemes for SGs. For instance, consumption data can be used to deduce sensitive information such as customers' lifestyles [146]. ML-based attack detection requires the detection models to be trained on consumer data. Most existing works focus more on the detection/prevention aspect and less on privacy-preserving, which could pose a risk to customers' safety [125,126]. Moreover, ML-based approaches raise ethical concerns, including biases in training datasets and the black-box nature of most ML models.

Data-driven methods present a promising solution to the increasing complexity of the distribution grid as they are model-independent. However, data imbalance, inadequate datasets, and false positives and negatives are challenges faced by multiple data-driven methods, particularly ML algorithms.

#### 6.2.2. Proposed Future Directions

Further research efforts are required where SG cybersecurity datasets are concerned. Digital twins are an emerging potential solution to countermeasure development and testing. They can be exploited for generating realistic datasets that reflect SG operation under different attack scenarios. They can also be exploited for handling the challenge of ensuring countermeasure reproducibility, as they can provide a virtual replica of power systems through a combination of numerical models and simulation hardware [185]. They offer real representations of cyber interactions and can therefore be used in testing and validating countermeasures effectively. Moreover, further in-depth studies on handling persistent issues in ML-based approaches are necessary. Data-imbalance, for instance, can be handled through producing synthetic data using oversampling techniques [186,187]. Furthermore, solutions that aim to ensure consumer data privacy should be further explored, such as federated learning and learning over encrypted data. Countermeasures should also consider ethical concerns, including generating fair datasets and exploring solutions to the black-box nature of ML algorithms such as explainable artificial intelligence.

### 6.3. Cyber-Physical Attacks

#### 6.3.1. Current Research Challenges

Coordinated and complex attacks present a major challenge to the cyber-physical security of SGs as they often do not correspond to the assumptions on which the design of solutions was based, such as attack ordering, timing, duration, and distribution [90,93,103]. Attackers, for instance, may launch a series of intermittent energy theft attacks to evade

being detected [126]. A well-planned attack may be leveraged to not only evade detection, but to amplify its physical impact as well [93]. Other forms of attacks are emerging and need to be investigated, such as adversarial ML, which allows attackers to evade ML-based detectors [116,119]. It is also worth noting that current literature predominantly focuses on FDI attacks, leaving other attacks underinvestigated in the context of SGs.

### 6.3.2. Proposed Future Directions

Extensive research on attack vectors is required. Hardware-in-the-loop technologies can be exploited to explore a wide range of possible scenario, as they are capable of better reflecting the SG's operation than conventional simulators. This represents a major step in developing adequate and robust countermeasures, particularly against coordinated attacks. Furthermore, research should consider protecting SGs against various types of attacks at different stages, rather than focusing on each attack separately when designing countermeasures.

Table 7 summarizes the aforementioned research challenges and presents opportunities for future work.

**Table 7.** Research challenges in SG cybersecurity and proposed directions.

| Research Challenge                                                                                                | Proposed Directions                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lack of research on the distribution grid. Predominance of the simplified DC model over the AC and hybrid models. | Adopting data-driven solutions (ML) for their model-independence nature, allowing their reproducibility and generalization over different models and components. |
| Interdependence between the cyber and physical layers. Coordinated and complex attacks.                           | Hardware-in-the-loop for a realistic representation of SG operation to identify complex attack scenarios and design robust countermeasures.                      |
| Literature focuses on countering a single attack (notably FDI).                                                   | Focusing on developing countermeasures against multiple attacks and for various attack stages.                                                                   |
| ML-related issues, including data privacy and data imbalance.                                                     | Adapting and improving existing solutions for the context of SG cybersecurity, such as oversampling, federated learning, and learning over encrypted data.       |
| Countermeasure testing for reproducibility in real-life conditions. Lack of SG cybersecurity datasets.            | Digital twins for their ability to reproduce realistic SG operation.                                                                                             |

## 7. Limitations and Outlook

Although this work is the first to provide an in-depth review of survey papers in the field of SGs, several limitations should be noted. First, this paper focuses exclusively on survey papers and literature reviews, which inherently do not cover the most recent primary studies at the time of their publication. Consequently, some of the latest advancements in SG research may not be reflected in the insights presented here. Second, given the large number of literature reviews on SG cybersecurity, the scope of this study was limited to papers specifically addressing this topic. Complementary work could expand the scope to include surveys on the cybersecurity of related cyber-physical systems to derive additional insights relevant to SG cybersecurity.

## 8. Conclusions

The evolution of power systems into SGs has introduced new features that benefit both customers and utility companies. However, it has also exposed power systems to new threats and challenges. SGs integrate smart devices and communication networks, which provide entry points for attackers to insert and propagate attacks. Thus, cybersecurity has become an essential aspect of the SG concept.

The increasing interest of researchers in the cyber-physical security of SGs combined with the complexity of the grid's structure, has resulted in an elevated number of papers, including literature reviews. It has become increasingly difficult to navigate the literature on the topic, which has prompted this work. In this study, we presented a systematic review of existing literature reviews on SG cyber-physical security. We reviewed 100 review papers, which we divided into general reviews, attack-specific reviews, method-specific reviews, and component-specific reviews. We noticed that most works have focused on FDI attacks, due to their stealthiness and ability to cause great damage. We also realized that data-driven methods, particularly ML, are becoming more prevalent. ML algorithms are model-independent, which is advantageous given the complexity of the grid's structure. Research on SG cyber-physical security faces a number of challenges, such as the interdependence between the cyber and physical layers, the lack of adequate and up-to-date datasets and testbeds, and the randomness of coordinated and complex attacks. Future works should consider privacy preservation, as SG data is becoming more sensitive. They should also focus more on the distribution system. This includes DERs, power electronics, the AMI, and hybrid microgrids.

**Author Contributions:** Conceptualization, M.B. (Mariem Bouslimani), F.B.-S.T., Y.A. and M.B. (Mohamed Benbouzid); methodology, M.B. (Mariem Bouslimani) and F.B.-S.T.; validation, M.B. (Mariem Bouslimani), F.B.-S.T. and Y.A.; resources, M.B. (Mariem Bouslimani) and Y.A.; writing—original draft preparation, M.B. (Mariem Bouslimani), F.B.-S.T. and Y.A.; writing—review and editing, M.B. (Mariem Bouslimani), F.B.-S.T., Y.A. and M.B. (Mohamed Benbouzid); visualization, M.B. (Mariem Bouslimani); supervision, F.B.-S.T., Y.A. and M.B. (Mohamed Benbouzid). All authors have read and agreed to the published version of the manuscript.

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

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

## Abbreviations

The following abbreviations are used in this manuscript:

|       |                                          |
|-------|------------------------------------------|
| AGC   | automatic generation control             |
| AMI   | advanced metering infrastructure         |
| BESS  | battery energy storage system            |
| CPS   | cyber-physical system                    |
| DDoS  | Distributed Denial-of-Service            |
| DER   | distributed energy resource              |
| DG    | distributed generation                   |
| DL    | deep learning                            |
| DMS   | distribution management system           |
| DNP3  | Distributed Network Protocol 3           |
| DoS   | Denial-of-Service                        |
| DSL   | digital subscriber line                  |
| EMS   | energy management system                 |
| ESS   | energy storage system                    |
| EV    | electric vehicle                         |
| FAN   | field area network                       |
| FDI   | False Data Injection                     |
| GOOSE | Generic Object Oriented Substation Event |
| GPS   | Global Positioning System                |
| HAN   | home area network                        |
| ICS   | industrial control system                |

|        |                                               |
|--------|-----------------------------------------------|
| IDS    | intrusion detection system                    |
| IED    | intelligent electronic device                 |
| IoT    | Internet-of-Things                            |
| MDMS   | meter data management system                  |
| MitM   | Man-in-the-Middle                             |
| ML     | machine learning                              |
| NAN    | neighborhood area network                     |
| NS-3   | Network Simulator-3                           |
| OSI    | Open Systems Interconnection                  |
| PCC    | point of common coupling                      |
| PKI    | public key infrastructure                     |
| PLC    | power line communication                      |
| PMU    | phasor measurement unit                       |
| RES    | renewable energy source                       |
| RL     | reinforcement learning                        |
| RTDS   | Real-Time Digital Simulator                   |
| RTU    | remote terminal unit                          |
| SCADA  | Supervisory Control and Data Acquisition      |
| SG     | smart grid                                    |
| V2G    | vehicle-to-grid                               |
| WAMPAC | Wide-Area Monitoring, Protection, and Control |
| WAN    | wide area network                             |
| WSN    | wireless sensor network                       |

## Appendix A

The following appendix lists the search strings employed to retrieve relevant survey papers from the aforementioned databases. We start by defining A, B, and C:

A = “smart grid” OR “microgrid” OR “power system”

B = “false data injection” OR “denial-of-service” OR “man-in-the-middle” OR “replay”

C = “review” OR “survey” OR “state-of-the-art”

The following search strings were used in retrieving relevant survey papers for our work:

A AND (“cybersecurity” OR “security” OR “attack”) AND C

A AND B AND C

When the search string is too long, we reduce the number of keywords, e.g.:

A AND “false data injection” AND “review”

## References

1. Snyder, A.; Kranzler, D.; Simpson, R. Smart Meters and Advanced Metering Infrastructure. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 13, pp. 445–462. [\[CrossRef\]](#)
2. 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* **2020**, *11*, 2218–2234. [\[CrossRef\]](#)
3. Salazar, L.; Castro, S.R.; Lozano, J.; Koneru, K.; Zambon, E.; Huang, B.; Baldick, R.; Krotofil, M.; Rojas, A.; Cardenas, A.A. A Tale of Two Industroymers: It was the Season of Darkness. In Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2024; pp. 312–330. [\[CrossRef\]](#)
4. Kaspersky ICS CERT. H2 2022–Brief Overview of Main Incidents in Industrial Cybersecurity. 2023. Available online: <https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-H2-2022-brief-overview-of-main-incidents-En.pdf?> (accessed on 11 November 2025).
5. Center for Strategic and International Studies. Significant Cyber Incidents Since 2006. 2023. Available online: [https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404\\_Significant\\_Cyber\\_Events.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf) (accessed on 11 November 2025).
6. Olorunlana, T.; Mohammed, H. Analysis of the Colonial Pipeline Cybersecurity Incident. *Int. J. Sci. Archit. Technol. Environ.* **2025**, *2*, 13. [\[CrossRef\]](#)

7. Zang, T.; Wang, Z.; Wei, X.; Zhou, Y.; Wu, J.; Zhou, B. Current Status and Perspective of Vulnerability Assessment of Cyber-Physical Power Systems Based on Complex Network Theory. *Energies* **2023**, *16*, 6509. [\[CrossRef\]](#)
8. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Technical Report TR/SE-0401; NICTA Technical Report 0400011T.1; Keele University: Keele, UK, 2004.
9. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report EBSE-2007-01; EBSE: Durham, UK, 2007.
10. Brandao, M.; Newton, C.W.; Wojszczyk, B. Overview of the Electric Utility Industry. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 1, pp. 1–16. [\[CrossRef\]](#)
11. Keyhani, A. *Design of Smart Power Grid Renewable Energy Systems*, 3rd ed.; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2019; p. 621. [\[CrossRef\]](#)
12. Borlase, S. (Ed.) Smart Grid Technologies. In *Smart Grids: Infrastructure, Technology, and Solutions*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2013; Chapter 3, pp. 61–496. [\[CrossRef\]](#)
13. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [\[CrossRef\]](#)
14. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 5–20. [\[CrossRef\]](#)
15. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [\[CrossRef\]](#)
16. Farhangi, H. The path of the smart grid. *IEEE Pow Energy Mag.* **2010**, *8*, 18–28. [\[CrossRef\]](#)
17. Borlase, S.; Fan, J.; Feng, X.; Giri, J.; Wilson, D.; Gray, G.R.; Huang, Z.H.; Sattinger, W.; Yang, B.; Zeng, B. Real-Time Grid Management. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 5, pp. 179–252. [\[CrossRef\]](#)
18. Padilla, E. *Substation Automation Systems: Design and Implementation*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2015. [\[CrossRef\]](#)
19. Schoene, J.; Humayun, M. Advanced Protection and Control for the Smart Grid. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 6, pp. 253–306. [\[CrossRef\]](#)
20. Mesbah, M.; Allan, S.S.; Hettich, D.D. Communications Systems. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 4, pp. 149–178. [\[CrossRef\]](#)
21. Borlase, S.; Behboodi, S.; Bradley, T.H.; Brandao, M.; Chassin, D.; Enslin, J.; McCarthy, C. Smart Energy Resources: Supply and Demand. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 3, pp. 67–148. [\[CrossRef\]](#)
22. Xu, G.; Yu, W.; Griffith, D.; Golmie, N.; Moulema, P. Toward Integrating Distributed Energy Resources and Storage Devices in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 192–204. [\[CrossRef\]](#)
23. Zia, M.F.; Elbouchikhi, E.; Benbouzid, M. Microgrids energy management systems: A critical review on methods, solutions, and prospects. *Appl. Energy* **2018**, *222*, 1033–1055. [\[CrossRef\]](#)
24. Mohassel, R.R.; Fung, A.; Mohammadi, F.; Raahemifar, K. A survey on Advanced Metering Infrastructure. *Int. J. Electr. Power Energy Syst.* **2014**, *63*, 473–484. [\[CrossRef\]](#)
25. Olivares, D.E.; Mehrizi-Sani, A.; Etemadi, A.H.; Cañizares, C.A.; Iravani, R.; Kazerani, M.; Hajimiragha, A.H.; Gomis-Bellmunt, O.; Saeedifard, M.; Palma-Behnke, R.; et al. Trends in Microgrid Control. *IEEE Trans. Smart Grid* **2014**, *5*, 1905–1919. [\[CrossRef\]](#)
26. Parhizi, S.; Lotfi, H.; Khodaei, A.; Bahramirad, S. State of the Art in Research on Microgrids: A Review. *IEEE Access* **2015**, *3*, 890–925. [\[CrossRef\]](#)
27. Borlase, S.; Ganji, M.; Shahidehpour, M.; Tian, W.; Burgess, P. Microgrids. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 19, pp. 591–604. [\[CrossRef\]](#)
28. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [\[CrossRef\]](#)
29. Kabalci, E.; Kabalci, Y. Introduction to Smart Grid Architecture. In *Smart Grids and Their Communication Systems*; Kabalci, E., Kabalci, Y., Eds.; Springer: Singapore, 2019; pp. 3–45. [\[CrossRef\]](#)
30. *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*; IEEE Standard for Synchrophasor Data Transfer for Power Systems. IEEE: Piscataway, NJ, USA, 2011; pp. 1–53. [\[CrossRef\]](#)
31. Cali, U.; Kuzlu, M.; Pipattanasomporn, M.; Kempf, J.; Bai, L. Smart Grid Standards and Protocols. In *Digitalization of Power Markets and Systems Using Energy Informatics*; Springer International Publishing: Cham, Switzerland, 2021; pp. 39–58. [\[CrossRef\]](#)
32. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613. [\[CrossRef\]](#)
33. Hasan, M.K.; Habib, A.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. [\[CrossRef\]](#)

34. Hahn, J. Cybersecurity for the Smart Grid. In *Smart Grids: Advanced Technologies and Solutions*, 2nd ed.; Borlase, S., Ed.; CRC Press: Boca Raton, FL, USA, 2017; Chapter 17, pp. 533–566. [\[CrossRef\]](#)
35. Morris, T.H.; Pan, S.; Adhikari, U. Cyber security recommendations for wide area monitoring, protection, and control systems. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; pp. 1–6. [\[CrossRef\]](#)
36. Katulić, F.; Sumina, D.; Erceg, I.; Groš, S. Enhancing Modbus/TCP-Based Industrial Automation and Control Systems Cybersecurity Using a Misuse-Based Intrusion Detection System. In Proceedings of the 2022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), Sorrento, Italy, 22–24 June 2022; pp. 964–969. [\[CrossRef\]](#)
37. Darwish, I.; Igbe, O.; Celebi, O.; Saadawi, T.; Soryal, J. Smart Grid DNP3 Vulnerability Analysis and Experimentation. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015; pp. 141–147. [\[CrossRef\]](#)
38. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5. [\[CrossRef\]](#)
39. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [\[CrossRef\]](#)
40. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access* **2020**, *8*, 177447–177470. [\[CrossRef\]](#)
41. Irvine, C.; Shekari, T.; Formby, D.; Beyah, R. If I Knew Then What I Know Now: On Reevaluating DNP3 Security Using Power Substation Traffic. In Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop, San Juan, PR, USA, 10 December 2019; ICSS: New York, NY, USA, 2019; pp. 48–59. [\[CrossRef\]](#)
42. Yang, Y.; Jiang, H.T.; McLaughlin, K.; Gao, L.; Yuan, Y.; Huang, W.; Sezer, S. Cybersecurity test-bed for IEC 61850 based smart substations. In Proceedings of the 2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5. [\[CrossRef\]](#)
43. Graham, J.; Olson, R.; Howard, R. *Cyber Security Essentials*, 1st ed.; CRC Press: New York, NY, USA, 2011; p. 342. [\[CrossRef\]](#)
44. Keromytis, A.D. Network Bandwidth Denial of Service (DoS). In *Encyclopedia of Cryptography and Security*, 2nd ed.; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; pp. 836–838. [\[CrossRef\]](#)
45. Baig, Z.A.; Amoudi, A.R. An analysis of smart grid attacks and countermeasures. *J. Commun.* **2013**, *8*, 473–479. [\[CrossRef\]](#)
46. Capkun, S., Jamming Resistance. In *Encyclopedia of Cryptography and Security*, 2nd ed.; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; pp. 661–662. [\[CrossRef\]](#)
47. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53. [\[CrossRef\]](#)
48. Asri, S.; Pranggono, B. Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wirel. Pers. Commun.* **2015**, *83*, 2211–2223. [\[CrossRef\]](#)
49. Ashraf, S.; Shawon, M.H.; Khalid, H.M.; Muyeen, S.M. Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat Towards Smart Substation Pathways. *Sensors* **2021**, *21*, 6415. [\[CrossRef\]](#)
50. Ortega-Fernandez, I.; Liberati, F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. [\[CrossRef\]](#)
51. Kush, N.S.; Ahmed, E.; Branagan, M.; Foo, E. Poisoned GOOSE: Exploiting the GOOSE protocol. In Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand, 20–23 January 2014; Australian Computer Society: Darlinghurst, NSW, Australia, 2014; Volume 149, pp. 17–22.
52. Rana, S.; Zhu, H.; Lee, C.W.; Nicol, D.M.; Shin, I. The Not-So-Smart Grid: Preliminary work on identifying vulnerabilities in ANSI C12.22. In Proceedings of the 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 3–7 December 2012; pp. 1514–1519. [\[CrossRef\]](#)
53. Farooq, S.M.; Nabirasool, S.; Kiran, S.; Suhail Hussain, S.; Ustun, T.S. MPTCP based mitigation of Denial of Service (DoS) Attack in PMU Communication Networks. In Proceedings of the 2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Chennai, India, 18–21 December 2018; pp. 1–5. [\[CrossRef\]](#)
54. Ibtissam, K.; Abdelrahman, M.S.; Alrashide, A.; Mohammed, O.A. Assessment of Protection Schemes and their Security Under Denial of Service Attacks. In Proceedings of the 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Prague, Czech Republic, 28 June–1 July 2022; pp. 1–6. [\[CrossRef\]](#)
55. Chlela, M.; Joos, G.; Kassouf, M. Impact of cyber-attacks on islanded microgrid operation. In Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems, RSES '16, Lisbon, Portugal, 26–30 June 2016; IEEE Press: New York, NY, USA, 2016; [\[CrossRef\]](#)

56. 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. [\[CrossRef\]](#)
57. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [\[CrossRef\]](#)
58. 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. Inform.* **2017**, *13*, 411–423. [\[CrossRef\]](#)
59. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [\[CrossRef\]](#)
60. Olowu, T.O.; Dharmasena, S.; Jafari, H.; Sarwat, A. Investigation of False Data Injection Attacks on Smart Inverter Settings. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6. [\[CrossRef\]](#)
61. Mohamed, A.S.; Arani, M.F.M.; Jahromi, A.A.; Kundur, D. False Data Injection Attacks Against Synchronization Systems in Microgrids. *IEEE Trans. Smart Grid* **2021**, *12*, 4471–4483. [\[CrossRef\]](#)
62. Gao, W.; Morris, T.; Reaves, B.; Richey, D. On SCADA control system command and response injection and intrusion detection. In Proceedings of the 2010 eCrime Researchers Summit, Dallas, TX, USA, 18–20 October 2010; pp. 1–9. [\[CrossRef\]](#)
63. Wu, Y.; Wei, Z.; Weng, J.; Li, X.; Deng, R.H. Resonance Attacks on Load Frequency Control of Smart Grids. *IEEE Trans. Smart Grid* **2018**, *9*, 4490–4502. [\[CrossRef\]](#)
64. Taher, M.A.; Tariq, M.; Behnamfar, M.; Sarwat, A.I. Analyzing Replay Attack Impact in DC Microgrid Consensus Control: Detection and Mitigation by Kalman-Filter-Based Observer. *IEEE Access* **2023**, *11*, 121368–121378. [\[CrossRef\]](#)
65. Mo, Y.; Sinopoli, B. Secure control against replay attacks. In Proceedings of the 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 30 September–2 October 2009; pp. 911–918. [\[CrossRef\]](#)
66. Ustun, T.S.; Farooq, S.M.; Hussain, S.M.S. A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard. *IEEE Access* **2019**, *7*, 156044–156053. [\[CrossRef\]](#)
67. Yu, Y.; Yang, W.; Ding, W.; Zhou, J. Reinforcement Learning Solution for Cyber-Physical Systems Security Against Replay Attacks. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2583–2595. [\[CrossRef\]](#)
68. Zhang, Z.; Gong, S.; Dimitrovski, A.D.; Li, H. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [\[CrossRef\]](#)
69. Shepard, D.P.; Humphreys, T.E.; Fansler, A.A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int. J. Crit. Infrastruct. Prot.* **2012**, *5*, 146–153. [\[CrossRef\]](#)
70. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Phys. Syst. Theory Appl.* **2021**, *6*, 164–177. [\[CrossRef\]](#)
71. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [\[CrossRef\]](#)
72. Hadjidemetriou, L.; Tertytchny, G.; Karbouj, H.; Charalambous, C.; Michael, M.K.; Sazos, M.; Maniatakis, M. Demonstration of Man in the Middle Attack on a Feeder Power Factor Correction Unit. In Proceedings of the 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, The Netherlands, 26–28 October 2020; pp. 126–130. [\[CrossRef\]](#)
73. Zhou, X.; Gou, X.; Huang, T.; Yang, S. Review on Testing of Cyber Physical Systems: Methods and Testbeds. *IEEE Access* **2018**, *6*, 52179–52194. [\[CrossRef\]](#)
74. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Comput. Secur.* **2023**, *125*, 103028. [\[CrossRef\]](#)
75. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 446–464. [\[CrossRef\]](#)
76. Gupta, K.; Sahoo, S.; Panigrahi, B.K.; Blaabjerg, F.; Popovski, P. On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids. *Energies* **2021**, *14*, 4941. [\[CrossRef\]](#)
77. Kuffel, R.; Giesbrecht, J.; Maguire, T.; Wierckx, R.; McLaren, P. RTDS—a fully digital power system simulator operating in real time. In Proceedings of the Proceedings 1995 International Conference on Energy Management and Power Delivery EMPD '95, Singapore, 21–23 November 1995; Volume 2, pp. 498–503. [\[CrossRef\]](#)
78. Nguyen, T.T.; Kadavil, R.; Hooshyar, H. A Real-Time Cyber-Physical Simulation Testbed for Cybersecurity Assessment of Large-Scale Power Systems. *IEEE Trans. Ind. Appl.* **2024**, *60*, 8329–8340. [\[CrossRef\]](#)
79. Zhang, H.; Ge, D.; Liu, J.; Zhang, Y. Multifunctional cyber-physical system testbed based on a source-grid combined scheduling control simulation system. *IET Gener. Transm. Distrib.* **2017**, *11*, 3144–3151. [\[CrossRef\]](#)
80. Idowu, P.B.; Suryadevara, R. Hardware-based microgrid testbed to facilitate development of Distributed Energy Resource (DER) systems for sustainable growth. In *IOP Conference Series: Earth and Environmental Science*; IOP Publishing: Bristol, UK, 2021; Volume 746, p. 012037.

81. Nie, Y.; Ye, T.; Zhou, B.; Xu, T.; Luo, H. A Testbed for Studying Security in Synchrophasor-Based State Estimation of Electric Power Transmission Grid. In Proceedings of the 2nd International Conference on Internet of Things, Communication and Intelligent Technology, Paris, France, 27–29 September 2024; Dong, J., Zhang, L., Cheng, D., Eds.; Springer: Singapore, 2024; pp. 240–248.
82. Blazek, P.; Bohacik, A.; Fudjak, R.; Jurak, V.; Ptacek, M. Smart Grids Transmission Network Testbed: Design, Deployment, and Beyond. *IEEE Open J. Commun. Soc.* **2025**, *6*, 51–76. [\[CrossRef\]](#)
83. 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. [\[CrossRef\]](#)
84. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [\[CrossRef\]](#)
85. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224. [\[CrossRef\]](#)
86. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45. [\[CrossRef\]](#)
87. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [\[CrossRef\]](#)
88. 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. [\[CrossRef\]](#)
89. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. [\[CrossRef\]](#) [\[PubMed\]](#)
90. Nafees, M.N.; Saxena, N.; Cardenas, A.; Grijalva, S.; Burnap, P. Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review. *ACM Comput. Surv.* **2023**, *55*, 1–36. [\[CrossRef\]](#)
91. Mrabet, Z.E.; Kaabouch, N.; Ghazi, H.E.; Ghazi, H.E. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [\[CrossRef\]](#)
92. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks. *IEEE Trans. Syst. Man, Cybern. Syst.* **2019**, *49*, 1554–1569. [\[CrossRef\]](#)
93. Zhang, H.; Liu, B.; Wu, H. Smart Grid Cyber-Physical Attack and Defense: A Review. *IEEE Access* **2021**, *9*, 29641–29659. [\[CrossRef\]](#)
94. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebarsari, A.; Dehghanian, P. Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access* **2020**, *8*, 87592–87608. [\[CrossRef\]](#)
95. Mehrdad, S.; Mousavian, S.; Madraki, G.; Dvorkin, Y. Cyber-physical resilience of electrical power systems against malicious attacks: A review. *Curr. Sustain. Energy Rep.* **2018**, *5*, 14–22. [\[CrossRef\]](#)
96. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*. [\[CrossRef\]](#)
97. Alsuwian, T.; Shahid Butt, A.; Amin, A.A. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. *Sustainability* **2022**, *14*, 4226. [\[CrossRef\]](#)
98. Tuyen, N.D.; Quan, N.S.; Linh, V.B.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [\[CrossRef\]](#)
99. Vahidi, S.; Ghafouri, M.; Au, M.; Kassouf, M.; Mohammadi, A.; Debbabi, M. Security of Wide-Area Monitoring, Protection, and Control (WAMPAC) Systems of the Smart Grid: A Survey on Challenges and Opportunities. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1294–1335. [\[CrossRef\]](#)
100. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. *arXiv* **2022**, arXiv:2207.07738. [\[CrossRef\]](#)
101. Haji Mirzaee, P.; Shojafar, M.; Cruickshank, H.; Tafazolli, R. Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). *IEEE Access* **2022**, *10*, 52922–52954. [\[CrossRef\]](#)
102. Achaal, B.; Adda, M.; Berger, M.; Ibrahim, H.; Awde, A. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity* **2024**, *7*, 10. [\[CrossRef\]](#)
103. Inayat, U.; Zia, M.F.; Mahmood, S.; Berghout, T.; Benbouzid, M. Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects. *Electronics* **2022**, *11*, 3854. [\[CrossRef\]](#)
104. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkaws, G.; Alsayaydeh, J.A.J.; Gaid, A.S.A. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies* **2025**, *18*, 141. [\[CrossRef\]](#)
105. Amanlou, S.; Hasan, M.K.; Asma' Mokhtar, U.; Mahmood Malik, K.; Islam, S.; Khan, S.; Attique Khan, M.; Asghar Khan, M. Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations. *IEEE Open J. Commun. Soc.* **2025**, *6*, 1965–1997. [\[CrossRef\]](#)
106. Swathika, O.V.G.; Karthikeyan, A.; Rout, K.; Hatkar, S. Cybersecurity Deployment in Smart Grids: Critical Review, Applications, Protection, and Challenges. *IEEE Access* **2024**, *12*, 113618–113641. [\[CrossRef\]](#)
107. Szczepaniuk, E.K.; Szczepaniuk, H. Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. *Energies* **2025**, *18*, 5017. [\[CrossRef\]](#)

108. Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid Cyber-Security: Review and Challenges toward Resilience. *Appl. Sci.* **2020**, *10*, 5649. [[CrossRef](#)]
109. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and Research Trends in Microgrids Cybersecurity. *Appl. Sci.* **2021**, *11*, 7363. [[CrossRef](#)]
110. Shafei, H.; Li, L.; Aguilera, R.P. A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems. In *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*; Haes Alhelou, H., Hatziaargyriou, N., Dong, Z.Y., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 1–45. [[CrossRef](#)]
111. Leszczyna, R. Cybersecurity and privacy in standards for smart grids—A comprehensive survey. *Comput. Stand. Interfaces* **2018**, *56*, 62–73. [[CrossRef](#)]
112. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [[CrossRef](#)]
113. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [[CrossRef](#)]
114. Zhang, Q.; Li, F.; Shi, Q.; Tomsovic, K.; Sun, J.; Ren, L. Profit-Oriented False Data Injection on Electricity Market: Reviews, Analyses, and Insights. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5876–5886. [[CrossRef](#)]
115. Husnoo, M.A.; Anwar, A.; Hosseinzadeh, N.; Islam, S.N.; Mahmood, A.N.; Doss, R. False data injection threats in active distribution systems: A comprehensive survey. *Future Gener. Comput. Syst.* **2023**, *140*, 344–364. [[CrossRef](#)]
116. Irfan, M.; Sadighian, A.; Tanveer, A.; Al-Naimi, S.J.; Oligeri, G. A survey on detection and localisation of false data injection attacks in smart grids. *IET Cyber-Phys. Syst. Theory Appl.* **2024**, *9*, 313–333. [[CrossRef](#)]
117. Rahman, M.A.; Venayagamoorthy, G.K. A Survey on the Effects of False Data Injection Attack on Energy Market. In Proceedings of the 2018 Clemson University Power Systems Conference (PSC), Charleston, SC, USA, 4–7 September 2018; pp. 1–6. [[CrossRef](#)]
118. Liu, J.; Labeau, F. From Wired to Wireless: Challenges of False Data Injection Attacks Against Smart Grid Sensor Networks. In Proceedings of the 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), Quebec, QC, Canada, 13–16 May 2018; pp. 1–6. [[CrossRef](#)]
119. Cui, L.; Qu, Y.; Gao, L.; Xie, G.; Yu, S. Detecting false data attacks using machine learning techniques in smart grid: A survey. *J. Netw. Comput. Appl.* **2020**, *170*, 102808. [[CrossRef](#)]
120. Aoufi, S.; Derhab, A.; Guerroumi, M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *J. Inf. Secur. Appl.* **2020**, *54*, 102518. [[CrossRef](#)]
121. Ullah, S.S.; Abianeh, A.J.; Ferdowsi, F.; Basulaiman, K.; Barati, M. Measurable Challenges in Smart Grid Cybersecurity Enhancement: A Brief Review. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 331–338. [[CrossRef](#)]
122. Bouslimani, M.; Tayeb, F.B.S.; Amirat, Y.; Benbouzid, M. Replay Attacks on Smart Grids: A Comprehensive Review on Countermeasures. In Proceedings of the IECON 2024-50th Annual Conference of the IEEE Industrial Electronics Society, Chicago, IL, USA, 3–6 November 2024; pp. 1–6. [[CrossRef](#)]
123. Pedramnia, K.; Rahmani, M. Survey of DoS Attacks on LTE Infrastructure Used in AMI System and Countermeasures. In Proceedings of the 2018 Smart Grid Conference (SGC), Sanandaj, Iran, 28–29 November 2018; pp. 1–6. [[CrossRef](#)]
124. Althobaiti, A.; Jindal, A.; Marnerides, A.K.; Roedig, U. Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods. *IEEE Access* **2021**, *9*, 159291–159312. [[CrossRef](#)]
125. Ahmed, M.; Khan, A.; Ahmed, M.; Tahir, M.; Jeon, G.; Fortino, G.; Piccialli, F. Energy Theft Detection in Smart Grids: Taxonomy, Comparative Analysis, Challenges, and Future Research Directions. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 578–600. [[CrossRef](#)]
126. Xia, X.; Xiao, Y.; Liang, W.; Cui, J. Detection Methods in Smart Meters for Electricity Thefts: A Survey. *Proc. IEEE* **2022**, *110*, 273–319. [[CrossRef](#)]
127. Berghout, T.; Benbouzid, M.; Muyeen, S. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100547. [[CrossRef](#)]
128. Rao, P.U.; Sodhi, B.; Sodhi, R. Cyber Security Enhancement of Smart Grids Via Machine Learning - A Review. In Proceedings of the 2020 21st National Power Systems Conference (NPSC), Gandhinagar, India, 17–19 December 2020; pp. 1–6. [[CrossRef](#)]
129. Haque, N.I.; Shahriar, M.H.; Dastgir, M.G.; Debnath, A.; Parvez, I.; Sarwat, A.; Rahman, M.A. A Survey of Machine Learning-Based Cyber-Physical Attack Generation, Detection, and Mitigation in Smart-Grid. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe, AZ, USA, 11–13 April 2021; pp. 1–6. [[CrossRef](#)]
130. Hasan, M.K.; Abdulkadir, R.A.; Islam, S.; Gadekallu, T.R.; Safie, N. A review on machine learning techniques for secured cyber-physical systems in smart grid networks. *Energy Rep.* **2024**, *11*, 1268–1290. [[CrossRef](#)]
131. Beg, O.A.; Khan, A.A.; Rehman, W.U.; Hassan, A. A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. *Energies* **2023**, *16*, 7644. [[CrossRef](#)]

132. Joudaki, M.; Zadeh, P.T.; Olfati, H.R.; Deris, S. A Survey on Deep Learning Methods for Security and Privacy in Smart Grid. In Proceedings of the 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS), Shiraz, Iran, 30–31 December 2020; pp. 153–159. [\[CrossRef\]](#)
133. Balla, A.; Habaebi, M.H.; Islam, M.R.; Mubarak, S. Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system. *Clean. Eng. Technol.* **2022**, *9*, 100532. [\[CrossRef\]](#)
134. Hamdi, N. Enhancing Cybersecurity in smart grid: A review of machine learning approaches. *Telecommun. Syst.* **2025**, *88*, 72. [\[CrossRef\]](#)
135. Ibrahim, N.; Kashef, R. Exploring the emerging role of large language models in smart grid cybersecurity: A survey of attacks, detection mechanisms, and mitigation strategies. *Front. Energy Res.* **2025**, *13*, 1531655. [\[CrossRef\]](#)
136. Gopstein, A.; Nguyen, C.; O'Fallon, C.; Hastings, N.; Wollman, D. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0*; Special Publication 1108r4; National Institute of Standards and Technology, Department of Commerce: Gaithersburg, MD, USA, 2021. [\[CrossRef\]](#)
137. Gaggero, G.B.; Girdinio, P.; Marchese, M. Artificial Intelligence and Physics-Based Anomaly Detection in the Smart Grid: A Survey. *IEEE Access* **2025**, *13*, 23597–23606. [\[CrossRef\]](#)
138. Baumeister, T. Adapting PKI for the smart grid. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 249–254. [\[CrossRef\]](#)
139. Badra, M.; Zeadally, S. Key management solutions in the smart grid environment. In Proceedings of the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, United Arab Emirates, 23–25 April 2013; pp. 1–7. [\[CrossRef\]](#)
140. Kumar, A.; Agarwal, A. Research issues related to cryptography algorithms and key generation for smart grid: A survey. In Proceedings of the 2016 7th India International Conference on Power Electronics (IICPE), Patiala, India, 17–19 November 2016; pp. 1–5. [\[CrossRef\]](#)
141. Ghosal, A.; Conti, M. Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2831–2848. [\[CrossRef\]](#)
142. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3–19. [\[CrossRef\]](#)
143. Cao, Y.N.; Wang, Y.; Ding, Y.; Guo, Z.; Wu, Q.; Liang, H. Blockchain-empowered security and privacy protection technologies for smart grid. *Comput. Stand. Interfaces* **2023**, *85*, 103708. [\[CrossRef\]](#)
144. Kong, P.Y. A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security. *IEEE Syst. J.* **2022**, *16*, 41–54. [\[CrossRef\]](#)
145. Asghar, M.R.; Dán, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [\[CrossRef\]](#)
146. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [\[CrossRef\]](#)
147. Abdalzaher, M.S.; Fouda, M.M.; Ibrahim, M.I. Data Privacy Preservation and Security in Smart Metering Systems. *Energies* **2022**, *15*, 7419. [\[CrossRef\]](#)
148. Shokry, M.; Awad, A.I.; Abd-Ellah, M.K.; Khalaf, A.A. Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Gener. Comput. Syst.* **2022**, *136*, 358–377. [\[CrossRef\]](#)
149. Sultan, S. Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Comput. Secur.* **2019**, *84*, 148–165. [\[CrossRef\]](#)
150. Tong, W.; Lu, L.; Li, Z.; Lin, J.; Jin, X. A Survey on Intrusion Detection System for Advanced Metering Infrastructure. In Proceedings of the 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 21–23 July 2016; pp. 33–37. [\[CrossRef\]](#)
151. Gursoy, M.; Mirafzal, B. On Self-Security of Grid-Interactive Smart Inverters. In Proceedings of the 2021 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA, 19–20 April 2021; pp. 1–6. [\[CrossRef\]](#)
152. Fu, R.; Lichtenwalner, M.E.; Johnson, T.J. A Review of Cybersecurity in Grid-Connected Power Electronics Converters: Vulnerabilities, Countermeasures, and Testbeds. *IEEE Access* **2023**, *11*, 113543–113559. [\[CrossRef\]](#)
153. Trevizan, R.D.; Obert, J.; De Angelis, V.; Nguyen, T.A.; Rao, V.S.; Chalamala, B.R. Cyberphysical Security of Grid Battery Energy Storage Systems. *IEEE Access* **2022**, *10*, 59675–59722. [\[CrossRef\]](#)
154. Kharlamova, N.; Træhold, C.; Hashemi, S. Cyberattack detection methods for battery energy storage systems. *J. Energy Storage* **2023**, *69*, 107795. [\[CrossRef\]](#)
155. Rekeraho, A.; Cotfas, D.T.; Cotfas, P.A.; Bălan, T.C.; Tuyishime, E.; Acheampong, R. Cybersecurity challenges in IoT-based smart renewable energy. *Int. J. Inf. Secur.* **2024**, *23*, 101–117. [\[CrossRef\]](#)
156. Vosughi, A.; Tamimi, A.; King, A.B.; Majumder, S.; Srivastava, A.K. Cyber-physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs. *Renew. Sustain. Energy Rev.* **2022**, *168*, 112794. [\[CrossRef\]](#)

157. Chen, J.; Yan, J.; Kemmeugne, A.; Kassouf, M.; Debbabi, M. Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Appl. Energy* **2025**, *383*, 125364. [\[CrossRef\]](#)
158. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [\[CrossRef\]](#)
159. Pliatsios, D.; Sarigiannidis, P.; Lagkas, T.; Sarigiannidis, A.G. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1942–1976. [\[CrossRef\]](#)
160. Ferrag, M.A.; Babaghayou, M.; Yazici, M.A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *J. Inf. Secur. Appl.* **2020**, *52*, 102500. [\[CrossRef\]](#)
161. Antonini, A.; Barengi, A.; Pelosi, G.; Zonouz, S. Security challenges in building automation and SCADA. In Proceedings of the 2014 International Carnahan Conference on Security Technology (ICCST), Rome, Italy, 13–16 October 2014; pp. 1–6. [\[CrossRef\]](#)
162. Cabus, J.E.U.; Bütün, İ.; Lagerström, R. Security Considerations for Remote Terminal Units. In Proceedings of the 2022 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC), Novi Sad, Serbia, 25–26 May 2022; pp. 47–52. [\[CrossRef\]](#)
163. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A Survey on Cyber Security for Smart Grid Communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [\[CrossRef\]](#)
164. Nghia Le, T.; Chin, W.L.; Chen, H.H. Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies—A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 423–445. [\[CrossRef\]](#)
165. Chhaya, L.; Sharma, P.; Bhagwatikar, G.; Kumar, A. Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control. *Electronics* **2017**, *6*, 5. [\[CrossRef\]](#)
166. Beasley, C.; Zhong, X.; Deng, J.; Brooks, R.; Venayagamoorthy, G.K. A survey of electric power synchrophasor network cyber security. In Proceedings of the IEEE PES Innovative Smart Grid Technologies, Europe, Istanbul, Turkey, 12–15 October 2014; pp. 1–5. [\[CrossRef\]](#)
167. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 397–422. [\[CrossRef\]](#)
168. Carryl, C.; Ilyas, M.; Mahgoub, I.; Rathod, M. The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 300–305. [\[CrossRef\]](#)
169. Han, W.; Xiao, Y. Privacy preservation for V2G networks in smart grid: A survey. *Comput. Commun.* **2016**, *91–92*, 17–28. [\[CrossRef\]](#)
170. Araujo, A.; Blesa, J.; Romero, E.; Villanueva, D. Security in cognitive wireless sensor networks. Challenges and open problems. *EURASIP J. Wirel. Commun. Netw.* **2012**, *2012*, 1–8. [\[CrossRef\]](#)
171. Yaacoub, J.P.A.; Fernandez, J.H.; Noura, H.N.; Chehab, A. Security of Power Line Communication systems: Issues, limitations and existing solutions. *Comput. Sci. Rev.* **2021**, *39*, 100331. [\[CrossRef\]](#)
172. Yilmaz, S.; Dener, M. Security with Wireless Sensor Networks in Smart Grids: A Review. *Symmetry* **2024**, *16*, 1295. [\[CrossRef\]](#)
173. Wang, J.; Shi, D. Cyber-Attacks Related to Intelligent Electronic Devices and Their Countermeasures: A Review. In Proceedings of the 2018 53rd International Universities Power Engineering Conference (UPEC), Glasgow, UK, 4–7 September 2018; pp. 1–6. [\[CrossRef\]](#)
174. Dalipi, F.; Yayilgan, S.Y. Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68. [\[CrossRef\]](#)
175. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [\[CrossRef\]](#)
176. Komninou, N.; Philippou, E.; Pitsillides, A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [\[CrossRef\]](#)
177. Gaspar, J.; Cruz, T.; Lam, C.T.; Simões, P. Smart Substation Communications and Cybersecurity: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2456–2493. [\[CrossRef\]](#)
178. Amulya, A.; Swarup, K.S.; Ramanathan, R. Cyber Security of Smart-Grid Frequency Control: A Review and Vulnerability Assessment Framework. *ACM Trans. Cyber-Phys. Syst.* **2024**, *8*, 1–27. [\[CrossRef\]](#)
179. Sanghavi, P.; Solanki, R.; Parmar, V.; Shah, K. Comprehensive Study of Cyber Security in AI Based Smart Grid. In Proceedings of the International Conference on Advances in Computing and Data Sciences, Kolkata, India, 27–28 April 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 189–202. [\[CrossRef\]](#)
180. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. *IEEE Access* **2018**, *6*, 27518–27529. [\[CrossRef\]](#)
181. Mohan, A.M.; Meskin, N.; Mehrjerdi, H. Covert Attack in Load Frequency Control of Power Systems. In Proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon), Tunis, Tunisia, 28 September–1 October 2020; pp. 802–807. [\[CrossRef\]](#)
182. Zeller, M. Myth or reality — Does the Aurora vulnerability pose a risk to my generator? In Proceedings of the 2011 64th Annual Conference for Protective Relay Engineers, College Station, TX, USA, 11–14 April 2011; pp. 130–136. [\[CrossRef\]](#)

183. Yuan, Y.; Li, Z.; Ren, K. Modeling Load Redistribution Attacks in Power Systems. *IEEE Trans. Smart Grid* **2011**, *2*, 382–390. [\[CrossRef\]](#)
184. Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet* **2023**, *15*, 83. [\[CrossRef\]](#)
185. Srivastava, A.; Liu, C.C.; Stefanov, A.; Basumallik, S.; Hussain, M.M.; Somda, B.; Rajkumar, V.S. Digital Twins Serving Cybersecurity: More Than a Model: Cybersecurity as a Future Benefit of Digital Twins 2. *IEEE Power Energy Mag.* **2024**, *22*, 61–71. [\[CrossRef\]](#)
186. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **2002**, *16*, 321–357. [\[CrossRef\]](#)
187. He, H.; Bai, Y.; Garcia, E.A.; Li, S. ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In Proceedings of the 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), Hong Kong, China, 1–6 June 2008; pp. 1322–1328. [\[CrossRef\]](#)

**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.