Article

Survey on Simulation and Vulnerability Testing in Smart Grid

Shampa Banik * and Trapa Banik

Posted Date: 12 February 2024

doi: 10.20944/preprints202402.0047.v2

Keywords: Smart grid; vulnerability; cyber-attack; taxonomy; simulation

Article

Survey on Simulation and Vulnerability Testing in Smart Grid

Shampa Banik [1,*] and Trapa Banik [2]

[1] Dept. of Computer Science, Tennessee Technological University, 1 William L Jones Dr, Cookeville, TN 38505, USA

[2] Dept. of Electrical and Computer Engineering, Tennessee Technological University, 1 William L Jones Dr, Cookeville, TN 38505, USA; tbanik42@tntech.edu

* Correspondence: sbanik42@tntech.edu

Abstract: The rapid integration of Information and Communication Technology (ICT) is transforming the traditional electrical grid into a *Smart Grid*. Smart grids enable two-way communication and improved monitoring and control between utilities and customers. However, due to its heterogeneous nature, public exposure, and weak security at low-powered devices, the Smart Grid has vulnerabilities to various malicious threats, adversaries, and cyber attacks, which may affect cost and service availability. Additionally, when the systems' confidentiality, integrity, or availability are compromised, the resulting fallout can threaten national security and have cascading effects on human lives. Given the extreme consequences of an attack, smart-grid technology must be thoroughly tested for correct operation and security *before* it is deployed. As a result, vulnerability testing of smart grids, not only for correctness but for security purposes, has been the subject of numerous studies by academics, government agencies, and private companies. This paper reviews the vulnerabilities associated with the smart grid and spotlights simulation as the vulnerability testing methodology conducted in recent pertinent research works. It also presents various security aspects of the smart grid, including grid applications, system and network infrastructure and components, cyber threats and attacks, simulation, and different mitigation techniques. Finally, we analyze the gaps in the current research works, focusing on simulation. We briefly present a real-time simulation testbed that mimics customer behaviour and integrates hardware in the loop to apply attack methods, analyze vulnerabilities and risk mitigation associated with the smart grid system, and propose future work to improve the current framework.

Keywords: Smart grid; vulnerability; cyber-attack; taxonomy; simulation

1. Introduction

The *Smart Grid* refers to the next-generation grid that integrates the infrastructure of traditional electricity grids with information and communication technology. Figure 1 shows the multidisciplinary fields of the SG. The Department of Energy definition defines a smart grid as follows: "An SG uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to electricity consumers, and a growing number of distributed generation and storage resources." [1]. With the ability to self-heal and adapt, SGs must be sustainable, comply with regulations, be environmentally friendly, cost-effective, and economically viable and also integrate renewable energy sources [2].

According to the National Institute of Standards and Technology (NIST), an SG comprises seven logical domains: bulk production, transmission, distribution, customers, markets, service providers, and operations [3]. An SG's energy generation, transmission, and distribution network is automated and widely distributed [4]. In addition, the SG is a cutting-edge digital two-way communication system between the consumer and supplier.

doi:10.20944/preprints202402.0047.v2

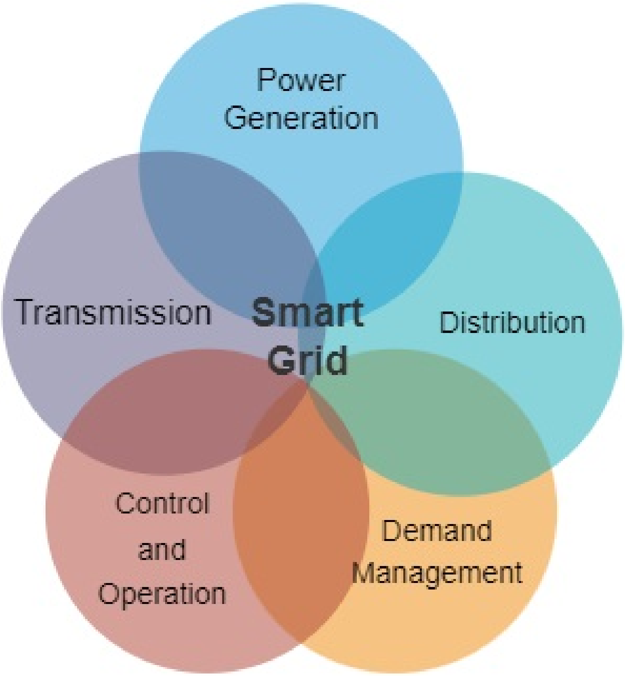

Figure 1. The multi-disciplinary fields of SG

Although the SG offers numerous advantages, its heterogeneous and complex nature significantly compromises its privacy and security, which have increasingly become targeted by cyber assaults or threats worldwide in recent years. For example, the Advanced Persistent Attack (APT), which security professionals coordinate over a prolonged period to pursue a specific goal, is a dangerous cyberattack targeting the SG. The intrusion on a Ukrainian electric substation that caused a power outage for more than 225,000 people was a typical APT [5]. While researching the August 2009 Stuxnet cyber-attack, Assante et al. in [6] demonstrated the ability to use vulnerabilities in control systems, which can also be found in the SG, to access hotel rooms and computerized passenger vehicle systems controlling throttle, braking, and steering to control operating functions remotely.

Vulnerability can be defined as the potential consequences of the system as a result of any incident, event, malicious action, intrusion, occurrence of malfunctioning, and associated activities. The SG vulnerabilities can be classified under security, operational, nontechnical, technical, and governance or regulatory parameters domains [7]. The attackers may investigate the system vulnerabilities to cause theft, vandalism, system failures, terrorism, and probable transmission sequence problems. The SG system is particularly susceptible to attacks because of the widespread availability of communication nodes. Secure real-time operational information of all the interconnected components is necessary for better security, load forecasting, and demand-side management (DSM) [8]. As vulnerabilities are inevitable in such large, complex cyber-physical systems, utilities must keep the vulnerability at a minimum level to ensure the system's resilience. Hence, a vulnerability testing method, mitigation plans and countermeasures must be employed.

Much research is underway to discover policies and mechanisms to protect or mitigate the vulnerabilities of SG systems. As the SG is regarded as a highly critical infrastructure that must provide consistent and continuous service, vulnerability testing in a live system is not viable. Hence, discovering practical solutions to enhance the resilience of SGs in risk assessment or vulnerability testing is crucial. Therefore, we compiled a study on vulnerability testing and challenges of SG security in this paper. Particular works have investigated vulnerability testing *before* integrating or implementing SG technologies or programs into a system. However, as of this study, we found little work on simulating Demand Response (DR) and Distributed Energy Resource (DER), which enabled SG models to determine network vulnerabilities. Therefore, more work in the area needs to be done.

The main focus of the study is to discover the gaps in current research for testing and evaluating the performance of SG infrastructure and its security before deployment. Therefore, we review the recent research works to assist us in investigating the system's vulnerabilities in-depth and, most importantly, examining what techniques could efficiently test the SG system's vulnerabilities and determining mitigation techniques to thwart adversaries. From the review, we identify gaps and present the directions for future SG cybersecurity research.

Following is a summary of this study's major contributions:

- Provide a thorough background of cyber-physical system components of smart grid (SG-CPS).
- Explore wide ranges of vulnerabilities associated with the cyber-physical components of SG systems and the various load management applications related to various operations and functionalities of the SG paradigm.
- Overview of the security background related to the SG's security goals, range of vulnerabilities, types of attacks and vulnerability mitigation techniques.
- Analysis of the scope of the simulation in SG paradigm in studying vulnerabilities found in the literature and methods to lessen these threats by strengthening the security of the smart energy system.
- Identify the research gaps from the current literature.
- Present directions in future research that address gaps and that will result in solutions for testing vulnerability to the SG system setup by measuring performance, correctness, and security before deployment.

The following sections serve as a structure for our review's findings: Section 2 presents the overview of the categories of the survey methodology. Section 3 discusses the SG security background along with the mapping of vulnerabilities associated with various components, technologies, and applications of the SG system. Next, Section 4 presents the categorical discussion on the role and types of simulation practised in SG research and study based on various aspects of the SG. The research gaps are outlined in detail throughout Section 5. Finally, Section 6 presents the conclusions and describes our approach to future work.

2. Survey Methodology

The survey methodology in this paper has been accomplished in two phases, as shown in Figure 2. In the first phase, we screened the literature and selected candidate publications based on relevant keywords, recency via year of publication, and impact via number of citations. In the second phase, we critically analyzed the pertinent selected papers to identify what research was being done and, where possible, what gaps existed.

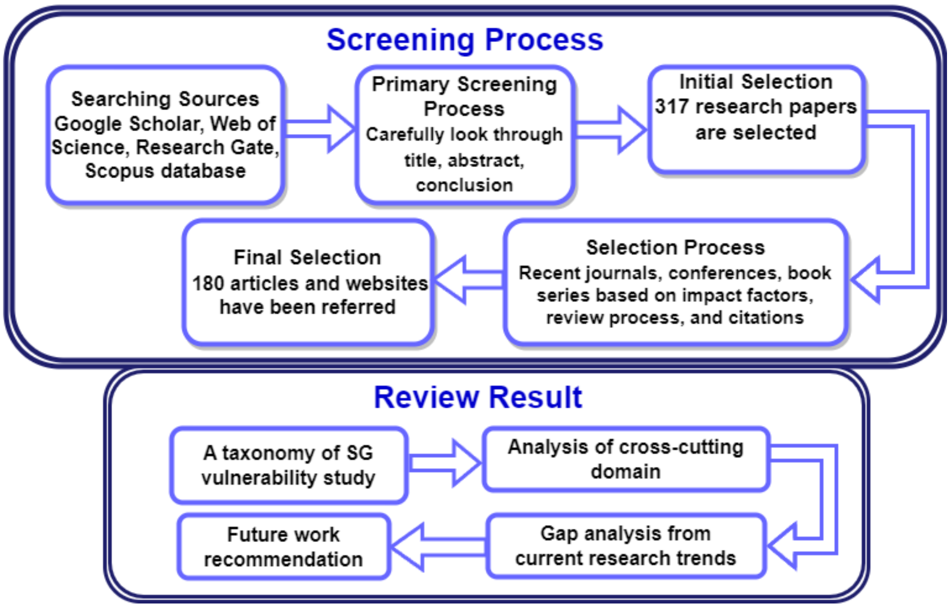
Screening Process
Searching Sources Google Scholar, Web of Science, Research Gate, Scopus database
Primary Screening Process Carefully look through title, abstract, conclusion
Initial Selection 317 research papers are selected
Selection Process Recent journals, conferences, book series based on impact factors, review process, and citations
Final Selection 180 articles and websites have been referred
Review Result
A taxonomy of SG vulnerability study
Analysis of cross-cutting domain
Gap analysis from current research trends
Future work recommendation

Figure 2. Survey Methodology

In particular, this study surveyed pertinent publications on vulnerability testing, smart grids, and SG simulation. Several sources were used to choose the relevant articles. The publications were initially searched in the Scopus Database, Web of Science, Research Gate, and Google Scholar databases. We preferred well-cited papers from reputable journals for impact and, for relevancy, conferences and works published in the last ten years. As search terms, we used *smart grid*, *Cyber-physical SG components*, *smart grid vulnerabilities*, *smart grid standards and protocols*, *SG simulation*, *smart grid simulation*, and others. Following a search, 140 pertinent articles were chosen for examination based on their pertinence to several key domains of interest, including *smart grid vulnerabilities testing and mitigation*, *SG cyber security*, and *smart grid simulation*. After determining the papers by the major and minor research topics, we then organized and classified those papers according to our main context. Finally, we used the works and our taxonomy to identify the amount of research according to the number of research works done on those topics. Additionally, using the major and minor themes of the papers, we investigated which papers cross-cut with themes from other papers. This methodology helped us identify what research is being done and where research gaps exist.

As a result of the survey methodology described, we constructed a conceptual taxonomy. The taxonomy itself is broken into two major categories: *SG Security background* that presents the necessary information to understand fundamental SG security issues in Section 3 and *Simulation for SG Security*, which describes issues of SG simulation and its role in security testing and evaluation in Section 4. In each section, we describe the further sub-categories and give a general overview of the works in each sub-category and the pertinent literature findings.

3. SG Security Background

The main topics in our overview of the background of Smart Grid Security are shown in Figure 3. The identified concepts are the goals of SG security, SG target vulnerabilities, threats and attacks against the SG, and vulnerability mitigation techniques.

Smart Grid-Background

The term *Smart grid* has been widely used, with different definitions and meanings. An SG is a cyber-physical system (CPS), sometimes called a smart grid CPS (SG-CPS), which is an amalgamation of physical components for energy generation, control devices, and communication networks. The cyber-physical components of SG are depicted in Figure 4. The cyber system performs a large computational operation on the data acquired from physical devices, reading them and initiating

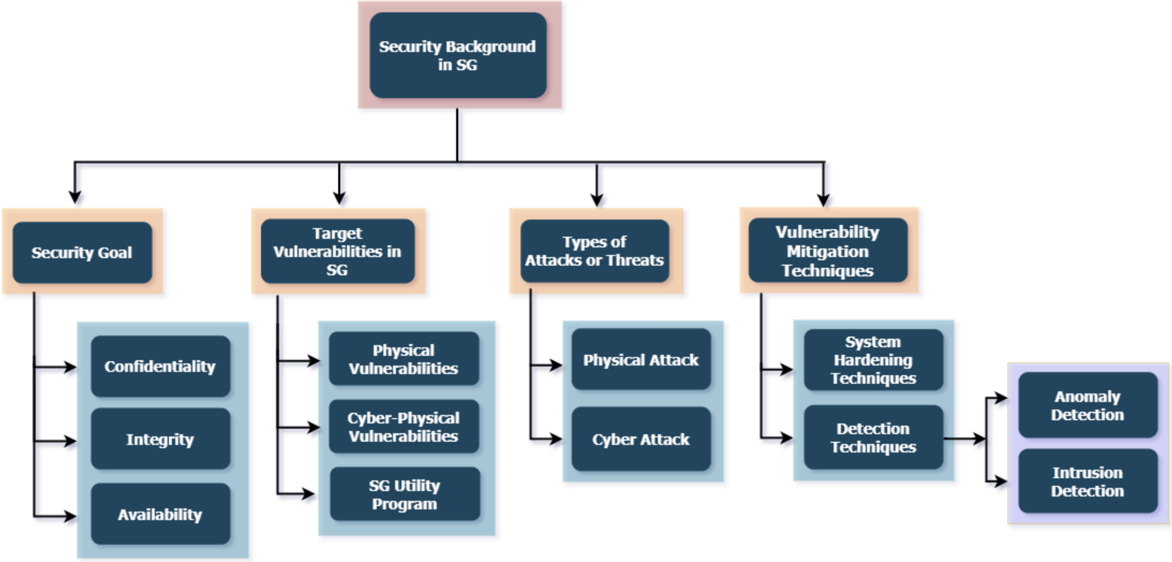

Figure 3. Security perspectives in SG

effective real-time control activities. Adopting CPS technologies in SG results in advanced operational efficiency, more customer responsiveness, increased economic viability, and greater environmental sustainability[9]. The United States Department of Homeland Security (DHS) [10] has classified it as a "critical" essential infrastructure.

The SG is heterogeneous. Various technologies connect power systems with network communications, sensors, and automation processes to improve the modern power system's adaptability, security, dependability, efficiency, and safety. In the SG, a large amount of data is gathered from the physical system, processed, and then used to direct actions in the cyber world. Various security threats exist due to the interactions between the SG's cyber and physical components, as the SG relies on both to perform essential functions. Furthermore, cyber attacks can cascade and significantly affect the physical system and society at large [11]. For instance, false data injection could cause infrastructure failure or set off a chain reaction. Essential CPS features rely on data and measurements that must be reliable to work. Therefore, malfunctioning sensors, control devices, or communication lines can delay or prevent the delivery of critical data, instructions, or both. Consequently, the physical system can be compromised, which would have devastating effects.

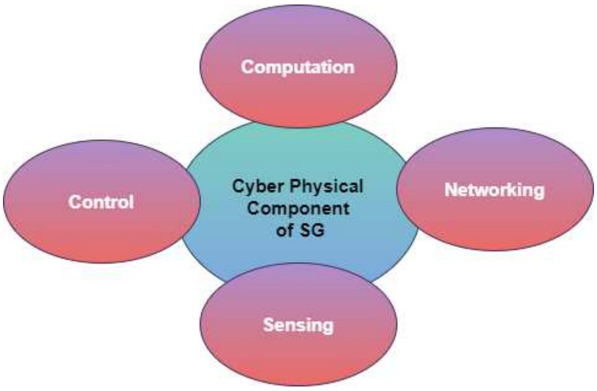

Figure 4. Cyber physical component of SG

3.1. Security Goal in SG

The conventional power network became more complex and vulnerable to several attacks due to the SG network's introduction of improvements and expanded capabilities. The CIA properties

doi:10.20944/preprints202402.0047.v2

indicate High-level security goals (Confidentiality, integrity, and availability). The *CIA triad* is a model that guides information security policies within an organization and is crucial to the dependable operation of smart energy systems [12,13]. Each policy in the CIA triad and its application to the SG is as follows:

- **Confidentiality:** Confidentiality is roughly equivalent to privacy. It prevents an enemy's unwanted access to highly secured information, such as power usage, price data, and control instructions. Such unwanted access can invade customers' privacy and divulge sensitive information about utilities.
- **Integrity:** Integrity refers to the ability to prevent the alteration of crucial data from sensors, electronic devices, such as smart meters (SM), software, and control commands that can impair decision-making and taint the data exchange of the SG. According to the authors in [14], improper data injection can alter state estimation, impair the SG's integrity and lead to improper power management.
- **Availability:** Availability refers to the ability to stop an enemy from denying authorized people access to, or control over, a system. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks can obstruct, delay, or corrupt information, resulting in an SG's inability to share information or provide power. Control-command and price information must be available in this situation because a loss of revenue could result.

3.2. Target Vulnerabilities in SG

A vulnerability in SG-CPS is a security weakness or flaw. Figure 5 illustrates the categorical SG vulnerability taxonomy. Any component of SG-CPS might have security vulnerabilities that malicious actors can use or even accidentally access by unsuspecting employees. Therefore, the primary action of enhancing security in the SG is to assess the vulnerabilities of each component, which encompasses the process of detecting and analyzing the existing flaws. Additionally, it involves implementing suitable corrective and preventive measures to minimize, mitigate, or potentially eradicate any vulnerabilities present.

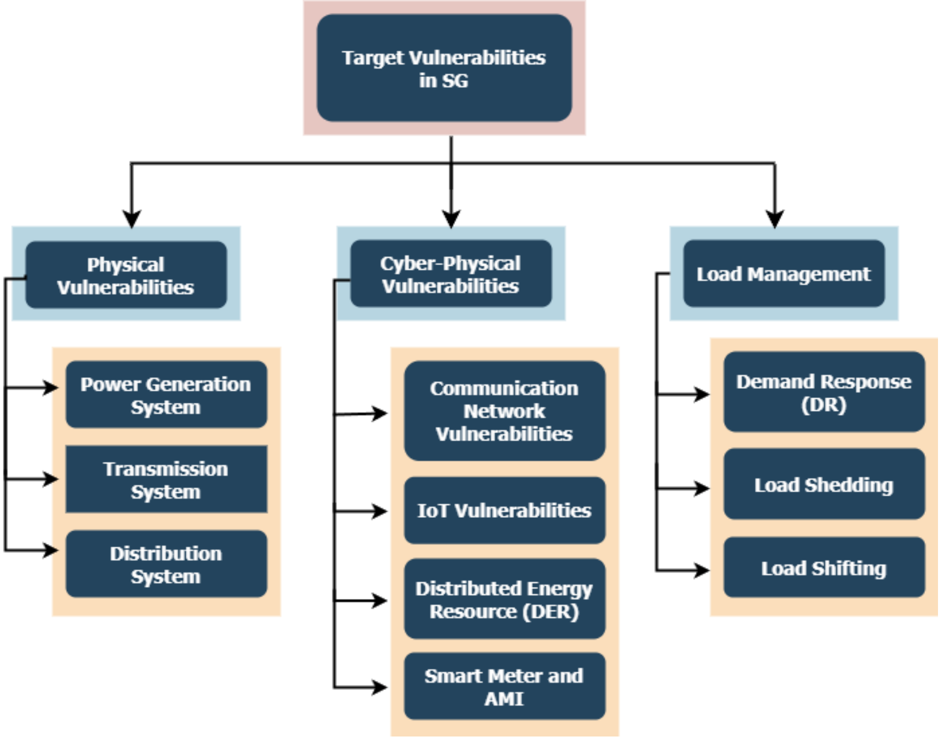

Figure 5. A map of the vulnerability study of the SG-CPS system taxonomies used in the literature

The SG-CPS typically encompasses a multitude of interconnected systems that possess the capability to observe and manipulate tangible entities and ongoing operations. Like many networking systems, backdoors or loopholes in software or hardware may be accessed through the network to exploit the vulnerabilities of the entire system and launch cyber-attacks. Moreover, many technologies and applications of the SG that allow consumers and utilities to manage electricity consumption in response to supply conditions and electricity demands may increase the attack surface, i.e., more device and network technologies means that more vulnerabilities may exist. The trending research topics, applications, and technologies of the SG that increase complexity and heterogeneity are distributed energy resources (DER), smart meters, AMI, load shedding, load shifting, and demand response (DR).

3.2.1. SG Physical Vulnerabilities

Power-generating stations, such as power plants, base stations, power grids, and other facility types, use varying degrees of security. They may implement access restrictions, authorization, and authentication methods such as usernames and passwords, access cards, biometrics, and video surveillance. In some instances, physical security is insured by well-manned and well-guarded stations. However, transmission cables are susceptible to interruption and sabotage attacks, so power-generating substations are less physically secure. In addition, misleading information can be generated by physically tampering with the SG components. Due to inadequate physical security measures, the exposure of ICS components is categorized as a vulnerability [15]. Therefore, they can be easily physically manipulated, altered, modified, or even sabotaged. Because many exposed components can be destroyed physically, SG field devices (such as smart grids, power grids, supply chains, etc.) are vulnerable to the same ICS vulnerabilities. Examples of vulnerabilities to SG physical devices are as follows:

Power Generation Plant:

- Power generation components are monitored through SCADA systems, but traditional systems may have vulnerabilities that make them vulnerable to cyberattacks. Attackers can exploit these vulnerabilities to manipulate frequency measurements and affect the facility's stability [16].
- Generation plant numerical relays use Ethernet-based IEC 61850. Attackers can cause malfunction or trip protection to damage power equipment [17].
- Local control loops are connected to the plant control center through Ethernet. Attackers can access the LAN, install a Trojan horse, or compromise digital control modules.

Transmission System:

- Transmission of significant volumes of energy using HVDC wires is becoming prevalent. HVDC lines need improved cyber security; therefore, their SCADA network incorporates permission and access control. When an opponent sends control signals to modify the commutation angle or block power flow, the targeted region loses power.
- RTUs and PLCs in the transmission system share generating system weaknesses. An opponent can build a URL and send it to any control center member. A networked HMI accesses the URL and tricks the web browser into running a malicious JavaScript code. After that, the network's PLCs are automatically detected, compromising the system. These are CSRF attacks.

Distribution System:

- A key distributive mechanism in a smart grid is the smart meter. A conventional meter can be changed by reversing the internal consumption counter or influencing the electric current calculation. IEDs like SMs can be remotely controlled to perform preprogrammed tasks. This lets an attacker remotely connect or disconnect devices, change system operator data, or steal critical user data. An attacker sending false data packets to cause negative pricing and power shortages in the targeted region would cost the utility provider income. Protecting every node is difficult, with millions of conventional and SMs coupled to the system, increasing susceptibility.

- Anderson and Fuloria found that a remote attacker could disable millions of SMs [18]. SMs also violate OWASP, or Open Web Application Security Project, rules. These standards address function-level access control inadequacy, injection, authentication, XSS, unsafe direct object references, security misconfiguration, exposed sensitive data, and XSS.
- Consumers who have a net metering system implemented at their location can tamper with the data on their net energy consumption transmitted to the utility's control center by breaking into the communication network of the AMI [19].
- Even if the customer is not sending power back to the grid, the attacker can cut costs or gain credits. Distribution companies lose more, yet the system doesn't stop instantly.

3.2.2. SG Cyber-Physical Vulnerabilities: Communication Network

The network architecture of SG has been depicted in Figure 6. To communicate, SGs employ both the HAN and the WAN. Each smart appliance in a home communicates with the SM across a home area network (HAN). Zigbee, Ethernet (wired or wireless), and Bluetooth are all methods of communication that the HAN can use to interact with other devices [20]. Information interchange between heterogeneous devices in smart energy systems is enabled via a variety of communication topologies such as the home area network (HAN), neighbourhood area network (NAN), and wide area network (WAN). WLANs (wireless local area networks) such as Zigbee are important technologies for constructing a HAN network. Unfortunately, WLANs are susceptible to energy demand analysis and subsequent fraudulent message injection by unauthorized users. ZigBee is vulnerable to signal interference [21]. WiMAX and LTE are implemented in NANs. WiMAX technologies are susceptible to radio-frequency link signal interference. LTE technology is also vulnerable to compromise if the evolved Node B (eNB) base stations are compromised, which allows access to all connected devices, including user equipment. The message exchange in a WAN may be susceptible to jamming that renders a particular PMU inaccessible and contributes to anomalous energy depletion at compromised nodes [22]. In addition, the communication path between the PMU and the PDC is susceptible to replay and false injection assaults. The smart grid is subject to network-layer attacks. Ethernet-based communication in substation LANs, which is crucial for safety and control in digital substations, is susceptible to attacks that manipulate the operation of devices. Weak security rules in network device configurations can jeopardize smart grids at entrances and egresses where SCADA devices connect to the main network [23]. IP packet tampering (source/destination address spoofing, fragmented message interruption, packet flag manipulation, and outstation data resetting) at network-layer devices such as routers and layer three switches also threatens the smart grid.

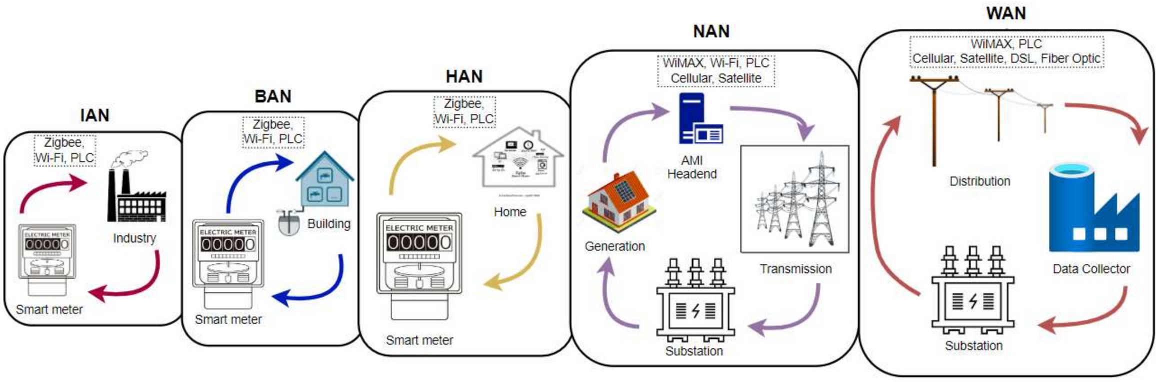

Figure 6. The network architecture of SG

HANs use wireless communication through IoT technologies and protocols, allowing more devices, appliances, and protocols to be connected. Unfortunately, the security implemented in these devices is often incompatible. Additionally, the usage of external cloud providers to manage data volume and end-users prioritizing convenience over security are concerning developments in HANs [24]. These variables increase the smart meter system's attack surface, making HAN communications, including forecasting data, easier to intercept and change.

Wireless sensor networks (WSNs) and micro-electrical and mechanical technologies used in SG's HANs and NANs gather and transmit data from the environment. WSN attacks, vulnerabilities, and security needs differ from wired network security because of sensor node limitations [4]. Further, SG Cyber-physical vulnerabilities are found at the *protocol level*, in the *IoT system*, in *distributed energy resources*, and in *advance metering infrastructures*.

SG Cyber Vulnerabilities: Protocol Level Integrating Information and Communications Technology (ICT) in a smart grid is extensive and closely connected to the power infrastructure. When combined with a power system, a cyber system creates a full Cyber-Physical System (CPS). Various cyber vulnerabilities, accessed via vulnerable access points shown in Figure 7, can pose security threats to the power system, leading to instability and unreliability of the CPS.

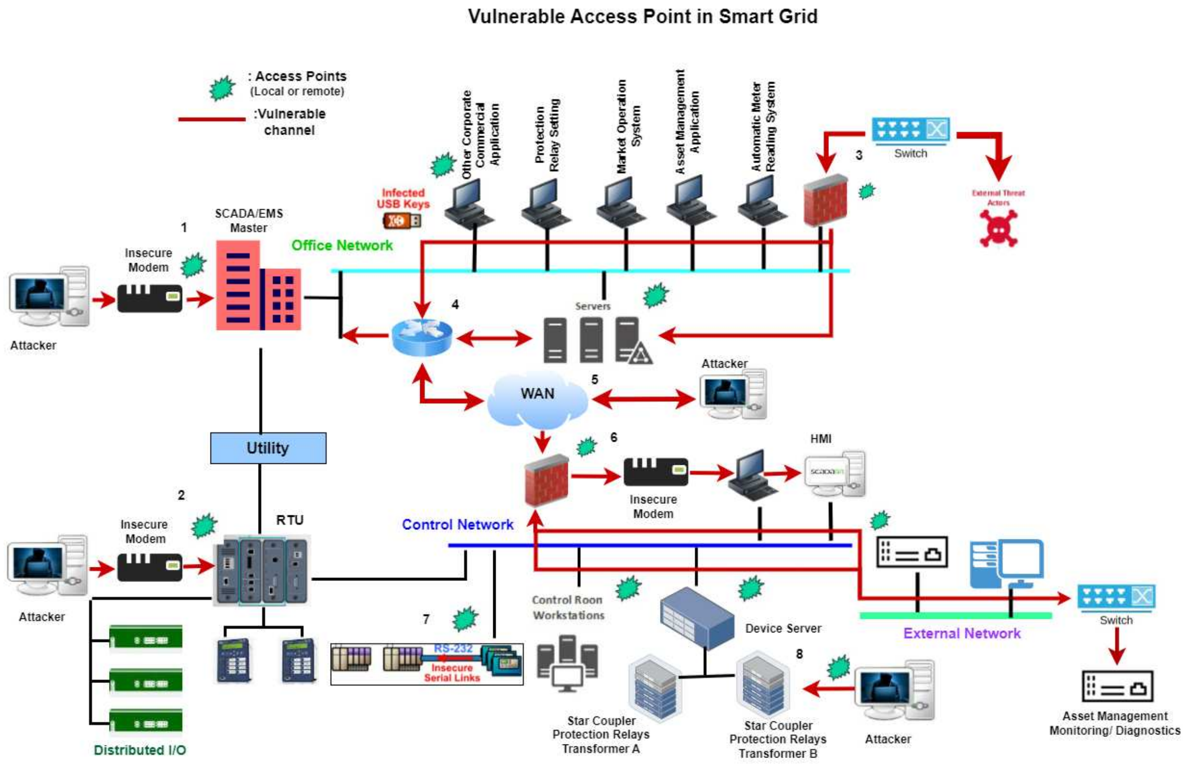

Figure 7. Vulnerable Access Points in Smart Grid cyber systems

Information flows from the application to the HAN, NAN, and WAN. A secure application can be exploited at an insecure network protocol layer. Each form of the network has interdependent protocols. The SG comprises protocols from all four communication networks: Home, Local, and Wide Area Networks. TCP/IP, Ethernet, Modbus, DNP3, MQTT, OpenADR, OPC, and Wi-Max are popular SG network protocols. The various protocols have different standards, implementations, applications, and security. For example, due to their absence of authentication and permission, Modbus, IEC-60870-5-104, Profinet, and DNP3 pose cybersecurity risks [25].

An SG inherits the cybersecurity weaknesses of its various technologies. Modbus is often used in industrial architectures because of its simplicity, e.g., it offers raw data transfer without authentication or encryption. However, these characteristics also make it vulnerable and easy to abuse [26]. Many studies examined and detected the impact of various potential cyber-attacks on Modbus of the SG [27–29]. Distributed network protocol version 3.0 (DNP3) is another critical infrastructure communication technology, especially in electrical installations. DNP3 was used in electrical stations to connect master stations (RTUs) and outstations (IEDs). An experiment was done to detect flaws and conduct penetration testing utilizing Man-in-the-middle (MITM) attacks on a simulated DNP3 system [30]. Direct or indirect access to routers, switches, or hubs is often enough to attack a protocol. For example, to attach MQTT, Internet connectivity, or access to an ISP router is sufficient. A physically connected device like an RTU or control network can also attack Modbus or DNP3.

SG Cyber-physical vulnerabilities: IoT-System

SG-CPS is similar to IoT systems, except CPS specifically stresses physical, networking, and computing activities. The Internet of Cyber-Physical Things (IoCPT) emerged from the use of IoT technologies in Cyber-Physical Systems (CPS) [15]. The SG uses IoT to collect, monitor, and analyze electrical grid data and deliver control signals. It also uses cutting-edge technologies like Wireless Sensor Networks (WSNs), which can cause sinkhole, sybil, and wormhole cyberattacks. IoT's reliance on the insecure internet creates major security issues. 2018 IEC 61850-8-2, an XMPP-based information mapping, was published to integrate SG and IoT, requiring WAN connectivity [31].

Many reasons exist that make security in the IoT complex. Due to its lack of security, an IoT device is often the SG's weakest link, allowing an enemy to enter the system and launch more attacks. Most IoT devices lack processing power or memory to encrypt data yet adhere to real-time constraints. Additionally, SG's IoT device connection path is vulnerable to data theft, manipulation, and change due to a lack of secure protocols, public exposure, and oversight. IoT devices may interact with each other and their environment without human supervision, raising security and privacy concerns. Due to their interaction with many IoT devices, DAUs and PDCs with IoT capabilities are particularly vulnerable to network-level attacks. IoT device-level authentication is at risk due to public key implementation complexity and resource constraints. APIs might provide fake data injection vulnerabilities in SG visualization systems like the human-machine interface (HMI) without proper auditing. IoT-enabled SGs connect SMs, controllers, DAUs, PMUs, PDCs, and fault isolators to the Internet, enabling pervasive connection. Encrypted communication between DAUs, PDCs, and control centres is possible using the LoRaWAN IoT protocol [32]. However, an attacker can enter the channel and change messages if the shared secret key is compromised.

Simple passwords are often not sufficient to protect IoT devices. Using spear-phishing, a 2015 Ukrainian power system cyberattack stole usernames and passwords from service provider network servers [5]. The IoT/SCADA devices were connected remotely over VPNs using the credentials [21]. Then, IoT/SCADA devices were remotely used to run malicious code to disrupt the system. Other attacks exploited IoT to access SG endpoints and interrupt power supply and generation. Many recent hacks are IoT-enabled, given the rapid usage of the Internet of Things. In [33], writers examined recent, confirmed IoT-enabled attacks, including proof-of-concept and real-world cases.

SG Cyber-physical vulnerabilities: Distributed Energy Resource (DER)

The key thrusts for the economic and environmentally sustainable future are digitisation and decentralization of electricity grids. Distributed energy resources (DER) are becoming commonplace in power systems to achieve this goal. Examples of DER include electric vehicles, battery storage, rooftop solar panels, etc. DERs help power companies save money on operations while giving customers and aggregators more control over the energy they generate and utilize. The growth of distributed energy resources (DERs) has prompted interest in hybrid SG communications for monitoring and control. DER may provide whole distribution networks, enhancing the current electrical grid [34].

DER can be used for various purposes. DER Energy may be used to lower costs and increase reliability. DER systems may improve local fuel efficiency and reduce pollution. DER technology can enhance electricity production and transmission and reduce distribution infrastructure and equipment needs. Additionally, local reliability and grid voltage may be improved via DER technologies. As the number of intermittent renewable energy sources (RES) increases, frequency and voltage will vary. The SG needs rapid, dependable communication and advanced sensing and protection technology to control and coordinate grid DERs.

The need for grid security rises with DER deployment. Table 1 highlights the cyberattack vectors targeting DER assets. Due to DERs' interconnectedness, interoperability, and support for remotely controllable features, cybersecurity is crucial [35]. Furthermore, DER communication requirements and various DER designs exacerbate power systems' cybersecurity issues.

DERs include communication links, cooperation, and remote control. Unexpected dynamic interactions that trip heavy transmission lines may disrupt regional electricity exports and imports. The authors in [36] state that a cyberattack framework can cause undervoltage and overvoltage in a renewable energy smart distribution system. Top-level optimization problems allow attackers to develop optimal and suboptimal false data injection attack routes that may Undervoltage or overvoltage the system. The attackers can then target vulnerable system portions at optimal times [37].

Analysis of communication protocol and device assaults shows significant differences in the functional level of attacks and targeted DER assets [38]. Cyberattacks target process sensors, actuators, and controllers at levels 0 and 1 of the Purdue model [18], whereas levels 3, 4, and 5 (communication, coordination, and control fabric) target DER systems. The min-max method presented in [39] demonstrates the significance of cyberattacks on energy centers and DER. Although an attacker could raise costs via energy hub components, a method that enabled and disabled various components was used to reduce the hack's economic impact.

Table 1. Attack Vector Description and Potential Threats for DER Assets [35]

Attack Vector	Description	Threat
Lack of interoperability	DER architectural diversity and implementation specification (e.g., security requirements) can result in intersystem insecure communications.	DER denial of legitimate messages and control commands
Data integrity violations	Stored, transmitted, or received data are modified without violation, causing DER malfunction or allowing unauthorized access to control/log information	Malicious modification of control parameter
Implementation errors	Security flaws within systems and/or communication modules enabling the remote control of DER assets and exfiltration of historical generation data	Command and control of load/demand-side devices
Supply-chain compromises	Installment of malicious hardware-based eavesdropping programs, worms, and oversights during manufacturing components, devices, or systems.	Sensitive information disclosure
Insecure firmware	Digital signatures of firmware updates are not verified, granting malware (viruses, worms, trojans, etc.) access to secure systems otherwise.	DER systems privilege escalation

Renewable energy sources (RESs) are rapidly entering the electrical grid due to declining reliance on traditional energy sources and increased power demand. Integrating renewable energy estimates with real-time SG system operations requires advanced IT. For example, attackers can alter wind and solar prediction data and send it to the control center to affect power scheduling, dispatch, real-time balancing, and reserve requirements. System abuse can occur when hackers change energy gain and reprogram wind turbines to reverse direction [17]. Such attacks could damage wind farms and hinder system performance. Malware attacks increase as renewable cyber-physical power systems (CPPSs) replace traditional power grids due to cyber technology and RES use [40]. On the other hand, a typical inverter-based power system within distributed energy resources (DERs) is more vulnerable to cyber attacks when it integrates with renewable energy. Specifically, false data injection attacks (FDIA) can cause cyber-physical switching attacks that can affect power converter components [41].

SG Cyber-physical Vulnerabilities: SM and Advanced Metering Infrastructure (AMI)

The growth of sophisticated Advanced Metering Infrastructures has brought new security challenges to the SG. The SM receives messages from HAN devices and routes them to the appropriate service provider [42]. The interactions between SMs' communication endpoints pose serious safety issues. Santamarta's work in [43] suggests that SMs may include factory login account backdoors, giving users control over the power readings. Telnet transmits unencrypted data, which is another security flaw. When attackers seize control of SMs, harmful interactions with other devices or misleading data can cause power outages and poor decision-making. They may use the meter as a "bot" to target other networked computers. Billing information might be altered to lower power prices to show misleading information.

Additionally, AMI's large-scale deployment makes it susceptible to many dangers, such as energy fraud, data theft, service outages, extortion, sabotage, terrorism, and hacktivism [44,45]. Malicious customers can hack home SMs and install malware to steal energy. Because the firmware was installed incorrectly, rogue nodes might send bogus data to DAUs, causing incorrect data collection. Energy corporations may use inaccurate data to make economic decisions [46]. Hacked sensors of SM can be used to alter power pricing [47].

Manipulating SM data at the end user's location can cost the service provider and benefit the competitor [19]. For example, the Puerto Rican Electric Power Authority lost $400 million yearly because SM manipulated electrical usage data. The attacker may gain private home information by disaggregating SM data using pattern recognition and feature extraction. To mitigate these risks, measures must be developed to safeguard SM data confidentiality [48].

3.2.3. SG Vulnerabilities in Load Management

For this survey's purpose, we define a *Load Management* program to be implemented by a utility using SG capabilities to increase grid stability and reduce costs. The focus of research in this area has been on *Demand Response*, *Load shedding*, and *Load shifting*.

SG Vulnerabilities in Load Management: Demand response (DR)

DR programs enable users to cut loads at peak demand to minimize SG energy consumption. Demand response is useful for smart grids because it may save costs and prevent load-related outages. These new computational advancements enabled by DR technology help SGs prevent blackouts and assist end-users and energy suppliers economically and environmentally. Energy systems require client interaction, making DR initiatives challenging. Energy cost, incentives, service satisfaction, and other variables affect consumer volunteerism.

An example DR program is depicted in Figure 8. DR programs let utilities remotely disconnect client appliances or reduce peak power demand, relieving the system. When users enrol in the DR program, the service provider collects data directly from meters that measure aggregate kilowatt-hours (KWH) from heating, cooling, ventilation, lights, and plugged equipment. The supplier then alerts clients of projected DR occurrences, such as high-load periods, allowing them to reduce their load.

The provider uses meter data during the DR event and projected behaviour to assess if the client reduced their load. Reduced loads are credited to consumers' bills in the following payment cycle. DR promotes consumer engagement with incentives [49]. Automatic Demand Response (ADR) consumers install smart devices that allow the utility to reduce their energy use automatically during high-demand periods without human involvement. While DR projects have focused on industrial complexes, researchers and professionals have also investigated home DR systems. Research indicates that demand response can support grid-interactive buildings with a high proportion of variable energy supplies and promote the use of renewable energy [50,51].

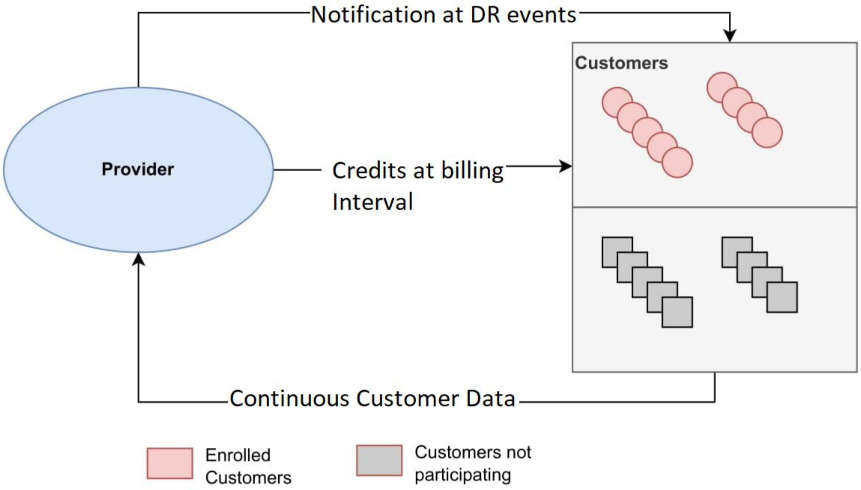
Notification at DR events
Customers
Provider
Credits at billing Interval
Continuous Customer Data
Enrolled Customers
Customers not participating

Figure 8. Demand Response model

Demand bidding and stoppable DLC are incentive-based DR schemes. RTP, TOU, and CPP are billing mechanisms. These incentive-based DR schemes pay users to reduce energy consumption during high energy prices. In demand response (DR) programs that implement time-based pricing schemes, consumers change how they use energy during high demand in reaction to various tariffs [52].

Pricing attacks and *energy theft assaults* are the two most common forms of cyberattacks designed to interfere with DR programs [53]. To attack power grids, attackers need only spread fake information to consumers about low electricity costs via the Internet or social media [54,55]. As a logical response to the incorrect information about low electricity prices, victims may increase their usage, possibly causing an abrupt load increase in the power grid. Then, the grid may experience an overload or peak load due to the unexpected spike in demand. Attackers committing energy theft assaults intentionally mislead utility companies about one or more consumers' energy production or consumption for their financial gain or the utilities' financial loss.

The authors in [56] examined DR load scheduling cyberattacks. The study simulated denial of service (DoS) and phishing attacks on Home Energy Management Systems (HEMS) in (DR) to manipulate price and load profile data. Based on field data, this study [57] shows how to identify anomalous and potentially malicious behaviour modifications as part of a cyber-physical intrusion detection mechanism. To evaluate DR situations, a test bed that simulates consumer behaviour and integrates hardware is proposed in [58]. Researchers used this test bed to examine how attacks affect components, protocols, software, and perceived consumer behaviour.

SG Vulnerabilities in Load Management: Load Shedding

The term *shedding load* refers to temporarily interrupting the electricity delivery at the point when the electricity demand is equivalent to supply. It is sometimes necessary to maintain the grid integrity by preventing the power grid from overloading. Load shedding, a form of load management, involves sporadically turning off the electricity or decreasing usage of primary sources until demand drops and more capacity becomes available.

As a critical CPS of the SG, the load-shedding scheme is subject to cyberattacks. [59] investigates the detection of attacks under dynamic load-altering assaults (D-LAA) by attacking two weak loads concurrently. The second phase studies how dynamic load-altering assaults (D-LAA) rebuild cyber-physical systems (CPS).

The SG uses load shedding as an emergency management solution for high-frequency deviation and supply-demand mismatch. Since the SG system's communication channels are easily hacked, attackers aim to disrupt the consensus approach of global information discovery. By creating an unknown input observer (UIO), a distributed load-shedding technique may detect and isolate misbehaving agents and prevent negative impacts [60].

In [61], the authors used a novel Reliable States WAUF LS (RSLS) approach to mitigate the vulnerability of Wide-Area Under-Frequency Load Shedding (WAUFLS) to avoid False Data Injection (FDI) cyberattacks. To protect the smart grid system from cyber attacks, utility companies can use a security game to study the impact of false data injection attacks on load shedding [62].

SG Vulnerabilities in Load Management: Load Shifting

In recent years, to operate and execute the utility program efficiently, prosumers (those who make and use energy) and demand response have gained popularity, notably in SG systems. Peak load shifting is essential for power system regulation as prosumers become more common [63]. The load pattern depicts commercial, institutional, and residential energy consumption fluctuations. Demand Side Management (DSM) approaches can alter end-user load patterns in power distribution systems [64]. DSM methods include filling gaps, reducing peaks, moving load, maintaining resources, adding new ones, and changing load shape.

Although load shifting in smart grids is beneficial for energy management and efficiency [63–68], it can also introduce vulnerabilities that malicious actors may exploit [69]. Smart grids use modern technology, complex communication networks, and substantial data interchange to coordinate and regulate power use through load shifting. Load shifting components can be vulnerable to cyber-attacks, increasing system vulnerability [70]. Unauthorized access to load-shifting communication infrastructure and control systems is a major risk. Hackers can acquire unauthorized control over load-shifting processes by exploiting weaknesses in system software, network protocols, or devices [71]. They may alter load schedules, interrupt grid operations, and create widespread power outages by hacking these crucial components.

The smart grid ecosystem's growing device connection and dependency creates another risk. Load shifting requires data communication between smart meters, sensors, and controls. An attacker with access to any of these devices might alter or introduce false data into the load-shifting process, causing faulty load forecasts or scheduling choices that destabilize the grid. Load shifting increases complexity and requires precise data and communication [72]. Any data integrity or communication channel violation might affect load-shifting efficacy and dependability. Data tampering, communication protocol manipulation, and denial-of-service assaults can undermine scheduling algorithms and cause operational interruptions.

3.3. Types of Attack and Threats on Cyber-Physical Systems of the SG

The aforementioned diverse vulnerabilities of the Cyber-Physical System of SG are the system's greatest weakness. These vulnerabilities provide an entry point for the attacker. To access power systems, the attacker employs *scanning*, also known as *reconnaissance*, to identify the services within the cyber-system. The goal of DoS and MITM attacks in the context of Wide-Area Measurement Systems (WAMS) is to disrupt the communication network so that authorized operators cannot access a power system. By initiating such assaults, the adversary can damage or impede the transfer of measurements and control directives by breaching the communication links between the substation and the control center. Before launching damaging attacks on the target physical device, reconnaissance attackers seek to get access to a compromised communication system employing Trojan or phishing emails. For example, this was the initial action taken by the cyber attacker who targeted a Ukrainian power grid

SCADA system to set up their attack vector and accomplish their final assault objective [5]. Table 2 shows once the CIA security constraints are breached, the target CPS components, measures, and risk mitigation techniques according to the categories of Detection (D), Prevention (P), and Correction (C), respectively.

Table 2 shows how the CIA characteristics of SG are affected by diverse cyber-attacks in different layers of the SG-CPS components.

Table 2. Attacks on cyber-physical systems and how they violate CIA security constraints

Attack	Target Components	Security Goals			Risk Mitigation Techniques	Countermeasures
		C	I	A		
Injection Attacks	Data Link, Transport, Application	✓	✓		D, P & C	Hybrid IDS, ML, BYOD Policy
Flooding Attack	Data Link, Network, Transport, Application		✓		D, P	Timestamp, Filtering, Random Session Keying
Man-in-the-Middle Attacks	Data Link, Network, Session	✓	✓		D, P	Encrypting the transmitted messages
Eavesdropping Attack	Physical, Network	✓			D, P	HTTPS/SSH Encryption, Personal Firewalls, VPNs
Replay Attack	Transport		✓		D, P	Running an executable program that sends safe values to Basic Process Contro System (BPCS)
Brute Force Attacks	Network, Session, Presentation	✓	✓		D, P	Timestamp, Filtering, Random Session Keying
Teardrop Attack	Network			✓	D, P	Timestamp, Filtering, Random Session Keying
Jamming Attacks	Physical, Data, Network			✓	D, P	Timestamp, Filtering, Random Session Keying
Spoofing Attacks	Physical, Data, Network, Transport	✓	✓	✓	D, P	Isolating the attacker node from the LAN
Social Engineering Attacks	Application	✓			D, P	Employee Training & Awareness
Buffer Overflow Attack	Transport, Application			✓	D, P	Timestamp, Filtering, Random Session Keying
Popping the HMI Attack	Application	✓	✓	✓	D, P	Timestamp, Filtering, Random Session Keying
DDoS Attack	Application, Network, MAC			✓	D, P	Backups, Secondary Devices, IDS, Leverage to Clouds
Phishing Attack	Application, Network, MAC	✓	✓		D, P	IDS, Anti-Phishing, Software/Training
Port Scanning	Control Center	✓			D, P	IDS, Anti-Phishing, Software/Training
Botnets	AMI	✓	✓	✓	D, C & P	IDS, Anti-Malware
Reconnaissance Attack	Control Protocol	✓	✓	✓	D, C & P	Redirecting the attacker to a honeypot
Malicious Software	Control Center, RTU	✓	✓	✓	D, P	Anti-virus, Installing Software Update Patches
Denial of Service	Field Devices, AMI	✓	✓	✓	D, P	Dropping packets coming from HMI, Generating an alert
Buffer Overflow	Field Devices, SCADA			✓	D, P	IDS, Anti-Phishing, Software/Training
Unauthorized Access	Control Center, RTU	✓			D, P	IDS, Anti-Phishing, Software/Training
Password Cracking	Control Center, RTU	✓			P & C	Password Policy, Periodic Password Changing
SM Tampering Attacks	AMI		✓		D, P & C	Anti-theft device, Detecting unauthorized access
SQL Injection	Control Center		✓		D, P	Least Privilege, Strong Code, Whitelisting
Data manipulation	SCADA	✓	✓		D, P	IDS, Anti-Phishing, Software/Training
Replay Attack	Field Devices	✓			D, P	IDS, Anti-Phishing, Software/Training
Spyware	Control Center	✓			D, P	Anti-Spyware, Defence in Depth
Malware	Control Center	✓	✓		D, P, & C	IDS, Firewalls, Anti-Malware,Anti-Virus

Table 2. *Cont.*

Attack	Target Components	Security Goals			Risk Mitigation Techniques	Countermeasures
		C	**I**	**A**		
Ransomware	Control Center	✓	✓	✓	D, C	Honeypot, Verified Backup/Update, Lesson Learnt
Worms	SCADA	✓	✓	✓	D, C	Honeypot, Verified Backup/Update, Lesson Learnt

3.4. Vulnerabilities Mitigation Techniques

Risk assessment is an important part of cybersecurity. *Risk* is defined as

$$Risk = Attack\_likelihood \times Possible\_Actions \times Consequences$$

The initial step in risk inspection is identifying cybersecurity assets, including hardware, network settings, software, and communication protocols. Next, several testing methods should be used to find power system vulnerabilities. Vulnerability assessment requires examining systems, scenarios, and access points. After detecting cyber vulnerabilities, the physical and application layers of the smart grid infrastructure must be assessed for attack damage. A fake cyber-attack can be launched to record the consequences of the attack while simulating a real-time model. Various studies have analyzed possible vulnerabilities [11]. Other tools that can be used to assess the extent of an attack include intrusion detection systems (IDS) and anomaly detection systems (ADS), which detect abnormal activity. Additionally, system hardening procedures can uncover the underlying cause of weaknesses in the SG and make it more robust to natural calamities and malicious assaults.

3.4.1. System Hardening Techniques

Hardening refers to securing the SG network, which includes implementing authentication, encryption, and validation, as well as employing an intrusion prevention system (IPS) and intrusion detection system (IDS) and using various anti-malware software. Vulnerability analysis and assessment is a key component to harden a system effectively. To secure all the SG system perimeter connecting components, vulnerability assessments should be conducted annually [73]. Various vulnerability analysis methods exist. The authors in [74] introduced a binary-based vulnerability finding approach for AMI and EV charging systems, extracting security characteristics from embedded software.

A simulation testbed is a software and hardware environment to analyze vulnerabilities in SG components, protocols, and other issues. A simulation testbed can identify vulnerabilities and enable the implementation of hardening techniques *before* deployment.

Other approaches to hardening the SG are as follows:

- **Securing AMI:** Advanced metering infrastructures (AMIs) expose the grid to many attack routes and intruders, requiring secure key generation and dissemination. For the security of the AMI network, identity-based cryptography creates secret keys between nearby SMs without contact [75].
- **Authentication:** Power data tampering in SG communications may complicate demand control. SG device authentication across geographies is crucial. A secure authentication key agreement (AKA) technique may protect SG interaction privacy [76]. This method authenticates SG devices and utilities to create a secret session key. An energy-efficient authentication and key negotiation method for SG scenarios has been developed using Chebyshev polynomial computing [77].
- **Machine Learning Approach:** Many researchers have used machine learning to detect power theft. For example, a robust deep learning model using GoogleNet and gated recurrent units (GRU) has been developed [78].
- **Cryptography and key management:** Communication security and privacy are SG systems' top priorities. Authentication allows users and service providers to connect securely. A biometric SG communication protocol uses elliptic curve (ECC) cryptography for mutual authentication [79]. A lightweight key management protocol uses hash and private keys to encrypt communication and facilitate key agreement [80].
- **Encrypted Tunneling via SSH or IPSEC:**

  Devices must authenticate communication sources and recipients and provide secrecy in their communication. Both IPsec and TLS can provide for authentication and encryption. Likewise, homomorphic encryption can protect power-use data during transmission between SMs [81]. Strong authentication should verify identity. Organizations should utilize explicit access permissions to give network access with an implicit refuse policy. SG parties need a trustworthy authentication procedure for communication. The protocol must be real-time, have low communication and computation overhead, and be attack-resistant, especially against Denial-of-Service assaults. In [79,82], a secure mutual authentication mechanism for SGs was presented using edge computing.

- **IPS & IDS:** To strengthen host-based defences against both external and internal assaults, network intrusion prevention system (IPS) and network intrusion detection system (IDS) technologies should be used.
- **Honeypots & Deception Techniques:** Honeypots are used to conceal and defend the cyber-physical system as SG. Honeypots have been designed for CPS, such as networked robotic systems [15]. Simulations show that honeypots can deceive attackers into thinking their attacks work.
- **Antivirus Software Validation:** Antivirus software protects embedded and general-purpose devices from malware. Software for embedded devices must be manufacturer-approved. Each product must store keying material for software validation. To verify newly downloaded software, the system needs updated antivirus software.
- **Human-Centric Mitigation Approaches:** Unorganized communication teams frequently function as system attackers. If teams aren't trained and structured when there are many interested parties, an "insider attack" may occur, resulting in many mistakes and accidental exposure.
- **Upgrading Equipment:** Older electrical power systems coexist alongside IT system components that are often more frequently replaced. Upgrading old equipment is recommended, as newer gear may not communicate with electrical grid devices or integrate with their security mechanisms.

Table 3 list families of security practices identified from research, workshops, and stakeholder interviews on cybersecurity controls and system hardening from the 2014 NISTIR 7628 r1 Guidelines for Smart Grid Cybersecurity to High-DER in SG environments, guiding future research and recommendations [83].

Table 3. Distributed Energy Resource Security and Privacy Control Families in SG environment (Source: NIST SP 800-53 R5).

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness & Training	PL	Planning
AU	Audit & Accountability	PM	Program Management
CA	Assessment, Authorization & Monitoring	PS	Personal Security
CM	Configuration Management	PT	Processing & Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification & Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System & Communication Protection
MA	Maintenance	SI	System & Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

3.4.2. Detection Techniques

Unfortunately, no system can be impenetrable. For example, *zero-day vulnerabilities* exist when software or hardware is released. Additionally, supervisory Control and Data Acquisition (SCADA) systems are an integral part of the SG's implementations, and they have archaic components that are inherently incompatible with modern approaches to IT security [84,85]. Therefore, when an attack occurs in an attempt to take advantage of an existing vulnerability, some means of detecting the attack must be implemented. The SG domain necessitates anomaly and intrusion detection systems to manage such systems' operations and identify threats, cyberattacks, and intrusions resulting from the faults of authorized/unauthorized users or deliberate attacks.

Anomaly Detection Techniques: Anomaly detection using SG data may be applied in several domains, such as cyber-security, fault detection, and power theft prevention. The unusual aberrant behaviours might have arisen due to several factors, such as peculiar consumption habits of users, malfunctioning grid systems, power outages, foreign cyber-attacks, or energy theft. Lately, identifying irregularities in the smart grid has gained significant attention from researchers and is extensively utilized in several influential domains. An important obstacle in the smart grid is the efficient implementation of anomaly detection for many abnormal behaviours.

Much research has been done in the SG anomaly detection field. Most of the recent works on this is based on machine learning. The sheer number of research in this area focuses on the consumption process, mainly to find unusual patterns or behaviours in power loads. Phase measurement unit (PMU) measurements datasets [86], real-time simulations on IEEE Bus testing platforms [87] and power utility logs [88,89]. In addition to a wide range of machine learning approaches such as anomaly detection methods [90–94], time series analysis techniques [95–97], grid load variations [98], IoT premises [99–101], and anomaly detection based on smart meter data [102–107] are also used to analyze anomalies in smart grid systems. With an aim at anomaly detection for electricity usage, the authors in [108–110] employed cloud computing technology. They surveyed the anomaly detection framework for power usage and suggested a cloud-based approach.

Intrusion Detection Techniques: The intrusion detection system (IDS) is a powerful safeguard and a protection mechanism against various cyber-attacks and threats in the SG system. Typically, IDS detection techniques in the SG system fall into three categories: abnormality-based, specification-based, and signature-based.

A unique anomaly-based intrusion detection system (IDS) called ARIES can effectively safeguard SG communications, as described in [111]. ARIES detects abnormalities and cyberattacks in network flows, Modbus/TCP packets, and operational data using three detection levels. In [112], to protect the modern electrical grid's head-ends (HEs), distribution access points/data aggregation points (DAPs), and subscriber energy meters (SEMs), a behavior-rule-based intrusion detection system (BRIDS) is recommended. Another framework has been offered in [113] that lets stateful analysis methods build stateful rules that can be run on Suricata, an open-source network intrusion detection system, to process their stateful analysis. An IEC 61850 stateful analysis application was constructed to demonstrate the framework's implementation.

A multicast-based cyber intrusion detection system (NIDS) for substation automation systems (SASs) was proposed by the authors of [114]. The suggested network-based intrusion detection system scans multicast messages for anomalies and malicious behaviour based on IEC 61850. The author presented a new intrusion detection system (IDS) in [115] for IEC 61850-based substation cyber security. The proposed IDS combines physical expertise, protocol requirements, and logical behaviour to thwart cyberattacks. Model-based detection, access control detection, protocol whitelisting, and multiparameter-based detection are available options. Implement and validate this SCADA-specific ID using data from a 500 kV smart substation and a realistic cyber-physical testbed. For better adapting the extreme learning machine (ELM) to the field of SG security, a genetic algorithm (GA)–based ELM SG AMI intrusion detection system was created [116]. The rule-based IDS is more interpretable and can detect attacks that haven't been seen before because the rules are represented symbolically. The authors in [117] provide a thorough and organized evaluation of rule learning methods and how they might be used as IDS in SG.

A substantial amount of work has been done on intrusion detection in AMI. A robust mutation-based intrusion detection system presented by the authors in [118,119] makes the behaviour unpredictable for the attacker while keeping it deterministic for the system, a real-time distributed intrusion detection system (DIDS) was presented in [120,121] for AMI architecture using stream data mining and multi-layer implementation.

4. Role of Simulation for SG Security

Although SG technologies positively affect the economy, society, and environment, testing the coexistence of heterogeneous Cyber-Physical-Smart-Grids (CP-SGs) and conventional technologies is difficult. Before deploying in real-time systems, the SG system's hardware and software components must be thoroughly examined. One examination method is to create a prototype that accurately and adequately replicates the operational conditions [122]. Simulation serves various purposes in the SG paradigm, as depicted in Figure 9. To promote research and development, describing the present state-of-the-art technologies in industrial control system simulation testbeds and evaluating emerging technologies and security holes is essential. The development of CP-SGs and the accompanying testbeds, which include a variety of testing paradigms, have been reviewed in this work. We specifically review CP-SG testbed architectures, their related functionality, and critical weaknesses.

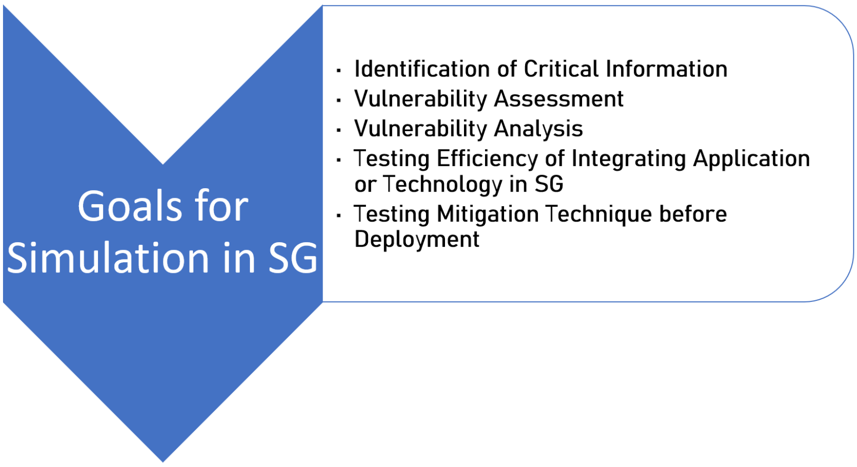
Goals for Simulation in SG
Identification of Critical Information
Vulnerability Assessment
Vulnerability Analysis
Testing Efficiency of Integrating Application or Technology in SG
Testing Mitigation Technique before Deployment

Figure 9. Goals of simulation in SG

The goals specified can be achieved by simulating various applications, technologies or features of the SG system that are frequently practised for SG research and analysis. Figure 10 illustrates different kinds of SG simulation adopted in practice.

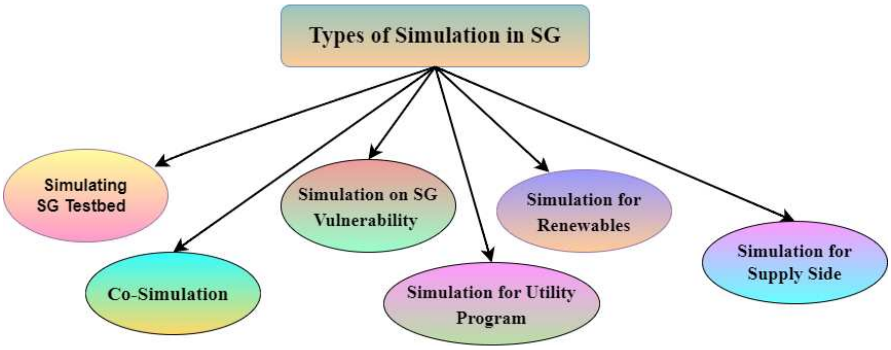
Types of Simulation in SG
Simulating SG Testbed
Co-Simulation
Simulation on SG Vulnerability
Simulation for Utility Program
Simulation for Renewables
Simulation for Supply Side

Figure 10. Types of simulation frequently practised in SG system

4.1. Testbed: A Simulated Smart Grid

The concept of the testbed for the SG system is logically depicted in Figure 11. Typically, a testbed refers to a simulated or controlled environment for any engineered system integrating various hardware and software components or a specific technology. In the context of smart grid research, the testbed is pivotal for the researcher or practitioners to study the systems' behaviour under different situations, such as attack and test case scenarios. Those scenarios are performed in a controlled or simulated environment so that the researchers or analysts can quickly assess the system's behaviour and capabilities without affecting any live operation or production and make necessary actions or decisions for any improvement or development in the system before making any large-scale deployment. In practice, numerous simulated components are integrated into the testbed focused on various aspects of the smart grid. Additionally, input data drives all testbed simulations. The input data are typically just grid power information, such as meter readings from AMI or feeder data. However, input data must be realistic, including input data for simulations integrating security testing. Unfortunately, attack data on smart grids is difficult to find and implementing attacks on live smart grids is not feasible. Methods must be developed with synthetic data that have realistic characteristics[123–125].

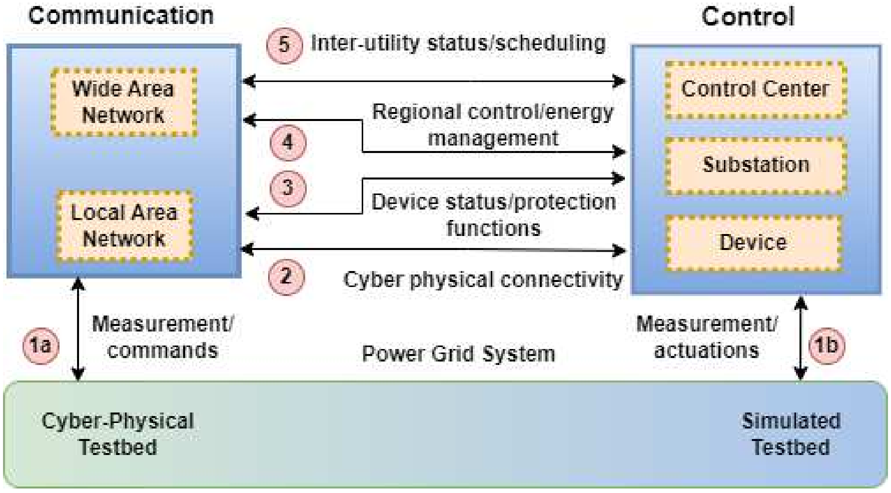

Figure 11. Concept of the testbed for the SG system

A real-time CPS testbed is an effective substitute because it can document interactions between cyber-control and physical subsystems [11]. A taxonomy of existing cyber-physical smart grid testbeds and illuminating suggestions to pinpoint the essential components and design choices when creating upcoming smart grid testbeds are described in [126]. According to the authors in [127], academia and industry have a significant need for remotely accessible testbeds that serve a variety of use cases relating to the CPS security of the grid. These use cases include vulnerability evaluations, impact analyses, product testing, attack-defence exercises, and operator training. CPS testbeds can have a variety of architectures and capabilities and typically fall into one or more of the following categories.

- **Software-based Testbeds:** The deployment and implementation of these testbeds are thought to be more cost-effective because modelling processes are utilized in place of real devices and information systems. Modelling technologies like Matlab, Modelica, Ptolemy, and PowerWorld simulate real-world ICS operations in many virtual testbeds. In contrast, numerous ICS processes are modelled using software like OPNET, OMNet++, and, most recently, NS3. Low fidelity is a significant drawback to employing virtual devices in the techniques mentioned earlier. Although several attack scenarios have been presented in some recent works based on such software or virtual testbed [128,129], due to the lack of software models for particular devices, they are also limited in their capacity to simulate specific cybersecurity scenarios.
- **Hardware-based Testbeds:** A network intrusion detection system (NIDS) testbed developed in [130] acts as a bridge between theory and practice by expanding and exploiting "hardware-in-the-loop" and "cyber-in-the-loop" capabilities to detect anomalies in network traffic. Such CPS testbed's advantages are (1) a large-scale power system's behaviour can be reasonably simulated using power systems simulation tools like Real-Time Digital Simulator (RTDS), DIgSILENT, PowerWorld, TSAT, and PSS®E; (2) a testbed can be tailored to a specific field of security studies like distribution systems, transmission systems, SCADA systems, and AMI networks; and (3) a testbed can be expanded by connecting multiple testbeds via communications like the Internet and LAN.
- **Hybrid Testbeds:** The testbed has three distinct physical, cyber, and control layers. Substation hardware, such as Remote Terminal Units (RTUs), a Real-Time Digital Simulator (RTDS), and

intelligent electronic devices (IEDs) make up the physical layer. An important piece of the electrical grid smart is the cyber layer. It allows for constant two-way interaction between the substation and the command post. It also improves SG automation in several other ways. New concepts and vulnerabilities must be evaluated, especially for hardware-in-the-loop test platforms [131]. For further research into the security holes in the IEC 61850 protocol and analysis of its possible impact in the context of smart grid connectivity, the authors in [132] have proposed a cyber-physical testbed, using OPAL-RT for HIL. The authors used the testbed to implement a realistic scenario of a power protection system's components interacting with IEDs.

- **Lab-based Testbeds:** The goals of the cyber-physical system are achieved through the employment of hardware, software, communication protocols, and many forms of media. Construction of a testbed can be a considerable undertaking at a significant expense. Labs allow access to constructed testbeds to a wider audience. Such labs give researchers a new way to evaluate the tangible effects of various hacks on SG systems without having to recreate the testbed. Two types of labs with testbeds exist to study and analyze SG security: 1) National Level Testbed labs and 2) Testbed labs at Research Institutes. For instance, the ISAAC is an adaptive testbed designed by the University of Idaho CPS SCADA Cybersecurity [133] in a natural automation controller environment to investigate and observe the impact of prospective cyberattacks and evaluate novel cybersecurity solutions on the SG. The PowerCyber testbed was built at Iowa State University [134] with the architecture, applications, and novel capabilities like virtualization, Real-Time Digital Simulators (RTDS), and ISEAGE WAN emulation to evaluate the availability and integrity of attack scenarios and explore cyber-physical consequences. Lab testing methods for today's electrical power systems use state-of-the-art co-simulation, Power hardware-in-the-loop, controller hardware-in-the-loop, and real-time simulation technologies. These methods expedite studying electrical systems and power electronics components by approving technological solutions in high-fidelity environments [135]. In this paper, experts from the Survey of Smart Grid International Research Facility Network's task on advanced laboratory testing methods discuss their methods, procedures, studies, and experiences applying them to test various prototypes and new power system solutions for R&D.

4.2. Co-Simulation

Researchers are developing novel methodologies for validating the control, interoperability, and dependability of distributed energy resources, Internet of Things systems, and modern power equipment to address power system control, vulnerability, stability, operation, and cybersecurity. However, various simulation environments are often targeted for specific purposes, processes, or simulated devices. Therefore, researchers frequently use testbeds to support their complex simulation needs that integrate sophisticated co-simulations [136–138]. *Co-simulation* refers to combining two or more simulation models that use distinct simulation runtime and representation models. A co-simulator enables many unified simulation scenarios by connecting several software and hardware emulators. It facilitates simulating the interaction between communicating components and a power grid, which is necessary to evaluate mutual consequences.

The SG concept is based on the widespread application of cutting-edge information technology, digital communication, and artificial intelligence to improve the features of the current power system's real-time monitoring and regulation of supply and demand. Thus, academics have paired several simulators more frequently in recent years to create innovative co-simulations In [139], MACSimJX co-simulation is presented, which combines multi-agent systems and Simulink simulator and JADE (Java Agent Development Environment) for controlling the microgrid that comprises wind power and storage system. Mets et al. [140] provide a thorough overview of co-simulations for power systems, concentrating on elements like synchronization and classifying the power and network simulators frequently applied. The frameworks for study are divided into three areas by the authors: power systems (for example, OpenDSS), communication networks (for example, OMNeT++), and SGs simulators (for example, GridLAB-D). The assessment includes several SG simulators, four network simulators, and twelve power system simulators. A high-performance computing (HPC) simulation platform is the framework for network co-simulation (FNCS) described by the authors in [141]. The broker controls communication between the network simulator ns-3 and the grid simulator GridLAB-D. The framework allows for synchronous simulation in adjustable time steps. In [142], the authors used typical simulator coupling in co-simulation, including conservative synchronization.

GridAttackSim is a proposed smart grid attack co-simulation framework by [143]. It comprises six primary parts: a preprocessing module, attack pattern library, GridLAB-D, NS-3, FNCS broker, and model manager. The co-simulation methodology on which this framework is built makes it possible to simultaneously simulate attacks on the communication network and the power grid. In their analysis of simulation methods for SG co-simulations, Li and Zhang [144] emphasize the importance of communication. The authors compare the most popular communication simulators (ns-2, OPNET, and OMENeT++). They describe Current SG simulations (SmartGridLab, GridSim, SCORE, and GridLAB-D), and consider extensions can can also be used to enable network simulations in simulators. They explore several co-simulation platforms integrating power and communication features, including EPOCHS, GECO, and VPNET.

4.3. Simulation on SG Vulnerability

Using the Real-Time Digital Simulator (RTDS®) power grid simulator with LabVIEW and PXI modules that simulate the SCADA system and intelligent electronic devices (IEDs). The authors have implemented a real-time framework of [27] to analyze the security vulnerabilities of communication protocols used in the SG. Opnet's SITL simulator, open-source Linux tools, and server infrastructure are used to model a real-world communication network. Another study by the authors of [145] outlines attack scenario challenges for evaluating and modelling SG configuration based on simulation. The key elements include the development of a Smart Grid Simulator (SGS) and a comprehensive Attack Scenario Model (ASM). The ASM comprises three main concepts: Attack Type, Schema, and Attack Schedule. These elements are used to model various Attack Behavioral Patterns, allowing flexible definition and simulation of attacks and showing the impact of attacks on the smart metering infrastructure (SMI) in SG. The SGS integrates the ASM, enabling configuration, simulation, and observation of Smart Grid behaviour under different attack scenarios.

In the paper [146], the authors evaluate internal security vulnerabilities in the SG, explicitly targeting the DNP3 protocol by conducting penetration testing in a simulated virtual environment. They specifically address Man-in-the-Middle (MITM) attacks. The goal is to optimize detection and mitigation strategies against smart grid attacks by employing theoretical modelling through game theory. The importance of an Intrusion Detection System (IDS) is highlighted for identifying potential attackers. Mitigation techniques are explored to ensure the overall security of the smart grid infrastructure.

Attackers can perform simultaneous attacks if they have enough resources of the SG infrastructure. To analyze simultaneous attack vulnerability, the authors in [147] use a redesigned cascading failure simulator with a shorter computation time. Updated damage measuring matrix includes generating power loss and steady-state time. Attackers perceive simultaneous attacks that cause a complete blackout quickly as the strongest. To demonstrate the General power system test scenarios, they employed W&W 6 and IEEE 30 bus systems in this study. The redesigned simulator automatically finds the strongest attack combinations for maximal generating power loss and black-out period attack damage. A study by the authors in [148] proposes and evaluates an attack probability-based vulnerability assessment approach for smart grid security. The likelihood of assault, attack transmission from parent to child nodes, basic metering system efficacy, Kalman estimates, and the effects on an advanced metering infrastructure were considered. The suggested architecture was tested by injecting fake data injection attacks (FDIA) and examining their propagation in the IEEE-300 bus simulating smart grid using MATPOWER. Their results suggest that severity evaluation standards, including

CVSS, AMI measurements, and Kalman estimates, helped assess smart grid vulnerability in FDIA attack scenarios. In [149], the authors introduced SCADASim to examine two practical case studies by performing DDoS and spoofing attacks on smart grid simulation. This solution addresses conceptual and implementation issues in the OMNET++ simulation environment, enabling real-world devices like smart meters and RTUs to be connected. The proposed framework is a novel solution that combines network simulation with real device connection to generate realistic SCADA system simulations. Results show that SCADASim replicates SCADA devices accurately.

4.4. SG Simulation for Load Management

The load management may include high-level applications or services like AMI, DSM/DR, or billing. Load management services at the application layer typically utilize middleware that offers general functionality for all services. The communication interface allows components to send messages, discover devices, and access services regardless of mimicking the networking technology (e.g., ZigBee, PLC, TCP, UDP). The middleware layer aims to accommodate various services while minimizing development effort[150]. Given that poorly designed load management applications or attacks on load management applications in the SG can lead to significant monetary losses for the utility and can even lead to blackouts or grid failures, testing, via simulation and before deployment, of load management programs, should be done.

The authors in [151] modelled volt/var control, demand response, and distribution automation using the GridSpice simulation platform to keep the voltage profile over the feeder flat and steady. A framework, ASTORIA, has been introduced to address the lack of comprehensive metrics and evaluation tools for assessing security properties in utility company infrastructures, designed for attack simulation in Smart Grids [152]. ASTORIA integrates a power flow and a network simulator to create a realistic Smart Grid environment. NS-3 and PY-POWER were used as the power flow and network simulators, respectively, at the heart of ASTORIA. Integrating NS-3 and PY-POWER is possible by using Mosaik as a broker. Using ASTORIA, attacks can be injected, and their impacts can be evaluated in a simulated environment. Attack profiles, made out of configuration files with standard file formats, execute these attacks. Attack characteristics such as attack type, attack schedule, attack frequency/intensity, and attack source and target components are all configurable via these profiles. They practised two common forms of cyberattack on SCADA systems: a denial-of-service attack and a virus infection. However, concrete parameters for evaluating security are not provided in the study. The weaknesses in the system are shown primarily through the usage of sampled data.

In another study [153], the authors provide a unique distributed system for Demand Response (DR) co-simulation in smart grids and real-time management. Our system allows near-real-time co-simulation, which validates revolutionary disaster recovery tactics that employ the Internet of Things to run software-in-the-loop. Thus, it can realistically simulate power system behaviour and install and update DR rules without affecting system operation. The solution also uses internet-connected smart devices at client sites and throughout the SG to collect energy statistics and offer actuation instructions. The framework can handle DR in a real Smart Grid. This is demonstrated via a real-world smart grid DR-policy test.

4.5. SG Simulation for Renewable Energy Sources

Recent times have seen a rise in the deployment of renewable energy sources within grid systems, which has presented significant new challenges in integrating them into existing networks [154]. The authors of [155] introduce the development of a smart grid infrastructure driven by safety, economic, and environmental considerations. The approach involves modelling and simulating key components such as photovoltaic arrays, wind turbines, storage devices, and load demand in the Discrete Event System Specification (DEVS) environment. Real wind speed and solar radiation profiles are used in the simulation. The simulation results, including the maximum stored power and power shortages, serve as valuable tools for power system designers, aiding them in making informed decisions about the required capacities for photovoltaic arrays, wind turbines, and storage at specific locations within the smart grid.

Using a large-scale simulated network, researchers employing both physical and software-based controllers with configurations for both local and remote control tested a multi-level control strategy for energy sharing among distributed resources of renewable energy sources (RES) and distributed generation (DG) [156]. This study outlined the procedure for choosing reliable communication systems for the BMW Farm's supervisory control and data acquisition (SCADA), power protection, and control. Similarly, the British Columbia Institute of Technology (BCIT) has set up a campus-based RER-powered microgrid that is campus-based [157]. The study examined how well the BCIT microgrid's ZigBee and WiMAX-based communication network performed. BCIT, which has a campus in Vancouver, created the first campus-wide microgrid. A hybrid PV/Wind model is exploited in [158] to integrate renewable energy in SG systems as a hybrid system model by simulation. In addition, along with other physical devices, batteries are used to stock the excess energy in the simulated model. On the operational technology network for wind energy, Sandia National Laboratories and Idaho National Laboratory deployed cutting-edge cybersecurity tools, such as security, orchestration, automation, and response (SOAR) tools that have an impact on the physical grid system components and stop the adversary kill chain [159].

A general methodology for creating mathematical and computational models of the various parts of the smart grid architecture model (SGAM) was created by the authors of [160] to integrate renewable energy. SGAM-inspired integrated mathematical modelling allows for the building of interoperable complex system simulations by combining various SG components, related communication models for data exchange and software modules, and control, estimation, and data analytics elements.

4.6. SG Simulation for the Demand Side

One of the key features of a smart grid is demand side management (DSM), which enables users to make knowledgeable decisions about how much energy they use and assists energy suppliers in lowering peak load demand and modifying load profiles. Consequently, the smart grid is more sustainable and has lower total operating costs and carbon emissions. Most demand-side management tactics in traditional energy management systems use system-specific algorithms. Additionally, current solutions manage only a few controlled loads of limited sorts. The research in [161] provides a load-shifting-based demand-side management solution for future smart grids with many devices of various kinds and proposes a minimization problem for day-ahead load shifting. This minimization issue was solved using a heuristic-based Evolutionary Algorithm (EA) that quickly adapts heuristics. A smart grid comprising residential, business, and industrial loads was simulated. Simulations reveal that the suggested demand-side management technique saves a lot while lowering smart grid peak load demand.

DSM aims to equalize daily energy consumption by implementing various strategies and regulations. The study [162] addresses the challenge of implementing a DSM program to figure out how loads behave daily in the electrical system, which is typically not possible in systems that rely on traditional electro-mechanical meters. In contrast to supply-side management, which involves increasing the number of generation units and total installed capacity, the goal is to employ energy management techniques to regulate consumption and increase the amount of energy delivered. The research trends in demand-side management in smart grid environments are discussed in the study, suggesting a genetic algorithm-based scheduling system for load control. The simulation results demonstrate that the recommended technique effectively lowers the PAR and power consumption cost.

Another study by the authors of [163] proposes an efficient pricing simulation method for future smart grids, aiming to benefit both users and power companies economically and environmentally. Smart pricing methods are suggested to reflect wholesale price fluctuations accurately and address social objectives. The proposed solution involves users equipped with energy consumption controllers connected to smart meters and communication infrastructure. A Vickrey-Clarke-Groves (VCG) mechanism is introduced to maximize social welfare by optimizing user utility functions and minimizing total energy costs. Users provide information about their energy demand, and the utility company determines electricity bill payments. The proposed mechanism is claimed to be efficient, promote user truthfulness, and result in nonnegative transfers. Simulation results indicate potential benefits for both users and utility companies.

5. Research Gap Analysis and Recommendation

This paper reviewed recent research on CP-SG simulations, simulation methods, structures, functionality, and significant vulnerability studies. The ultimate goals of the research works cited by this paper are 1) to establish a power grid that delivers energy effectively and 2) to establish a secure power grid. A vital sub-goal of the research is to ensure that smart grids are secure and effective *before deployment*, as deploying grids or grid upgrades that are not effective or secure can result in significant financial loss, interruption of services, and even loss of life. Table. 4. shows the cross-cutting related works on various research classes simulating SG for vulnerability study.

Table 4. Cross-cutting related works on various research classes simulating SG for vulnerability study.

	Simulation on SG testbed	Simulation on SG Technolog & Application	Simulation on SG Communication Networ	Simulation on SG power grid & Communication Network
Vulnerabilities Assessment	[58,122,127,137,164,165] [132,136,140,147,164]	[40,64,166–168] [148,149,152,159]	[16,140,145,146,169,170]	[143,165,168,171]
Vulnerability Mitigation	[89,101,147,154,164,164] [134,178]	[75,94,115,156,159,172,173]	[114,170,174–176]	[115,130,177]

A breakdown of the most researched fields, as shown in4, follows. The most explored work classifications from the table are Simulation on SG Technology & Application and Simulation on SG Testbed for the vulnerabilities assessment. The second most researched fields are Simulation on SG Technology & Application and Simulation on SG Testbed, focussing on SG vulnerabilities mitigation. However, the least researched works focussed on vulnerability mitigation based on simulating the SG communication network and simulating the SG power grid along with the communication network.

Efficient engineering requires applying the appropriate practices to develop working solutions and secure ones [179]. Furthermore, once implemented, a system must be tested to demonstrate the performance *and security* [180] of the design and implementation. Likewise, testing a smart grid for effectiveness and resiliency before deployment requires a simulation environment that holistically covers the problem domains. In other words, the most effective simulations should not only accurately simulate the effective operation of the grid but also allow testing of the SG to ensure that security has been integrated throughout the SG. As shown in Figure 12, such thorough evaluation should be done before deployment of new applications, devices, and network technologies and should include vulnerability assessment and testing of vulnerability mitigation techniques. Therefore, the most effective simulations should cross-cut the classes of work found in the literature by supporting techniques represented by each class.

Few works cited have discussed integrating these technologies in simulation, especially for integrating security testing. We found, as indicated by Table 4, that few research studies have been done on integrating various components, such as SG technologies or applications, to simulate the SG environment to assess specific vulnerabilities and devise mitigation techniques. In particular, none of the current research explored simulating the SG for examining the SG application, vulnerability analysis, and mitigating vulnerability in a networked environment. Significant work must be done to fill the gap in integrating techniques, particularly simulated security testing, across all smart grid components to ensure an effective and secure smart grid.

Unfortunately, security testing is done in isolation. For example, works on the security of Modbus and other smart grid protocols exist. However, these works do not reveal vulnerabilities due to dependencies in more complex environments, nor do they reveal the effects on the SG application. Therefore, to create effective and complete testing of the SG, we propose that more research is needed to discover innovative ways to incorporate various technologies for an integrated simulation environment. In particular, more work needs to be done in the following areas:

Policy design: A complete investigation needs to be done to formalize the policies for integrating security in the Smart Grid. These policies must be tailored for the various subsystems in the smart grid and integrated into the SG. For example, AMI has well-known security policies, such as the authentication requirement of key pair access. However, we have found no formal attempt to integrate the policies of various security components into an integrated, cohesive whole, nor have we found any attempt to integrate security policy management into SG simulation for testing and validation.

Policy instancing: Additionally, tools must be developed to support policy implementation into SG simulation. Such tools should include libraries for commonly implemented security algorithms and protocols that are easy to integrate into the simulation, with support for HIL and co-simulation. Likewise, support for instancing policy with mechanisms should be included to test the various ways to enforce the security policies.

Security Vulnerability Analysis and Testing support: SG simulation tools that support security testing should support enacting real-world attacks on the SG simulation, both at the device and network levels. Likewise, simulations should include tools that provide a component-by-component and holistic investigation of the effectiveness of the attack on targeted system vulnerabilities. For example, what would be the overall effect on the grid if a MODBUS write register attack occurred on a specific number of meters? Additional tools that indicate possible mitigation techniques would be useful. Furthermore, methods for generating synthetic data should be augmented with methods for integrating synthetic attack data needed to drive the simulation scenarios for vulnerability testing. The synthetic attack data must represent real-world attacks and must represent realistic attack frequency and severity.

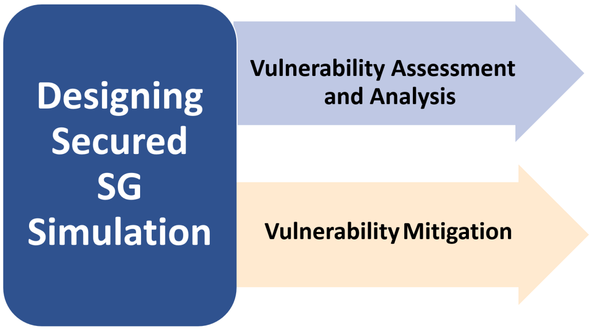
Designing Secured SG Simulation
Vulnerability Assessment and Analysis
Vulnerability Mitigation

Figure 12. This work attempts to determine where research in applications, vulnerabilities, technologies, and simulation meets and what the gaps are.

6. Conclusions and Future works

Cyber and physical levels of the SG both include flaws and oversights that could jeopardize system stability and performance. Security vulnerabilities are among the most significant issues in the SG. Simulation can be an important method for identifying and fixing these flaws before deployment. Therefore, this paper aims to provide an overview of existing works in smart grid simulation, focusing on security and recommendations for future research directions. We examined the resources that adversaries can manipulate, as well as their capabilities and goals, and then showed how protocol-level and device-level vulnerabilities can be used to launch cyberattacks that harm the performance of power systems. We described specific attacks, threats, and vulnerabilities and presented various works in simulation and analysis. Furthermore, we have found that more work needs to be done to integrate grid simulation tools, especially security methods, for practical analysis.

We have implemented an initial framework as an example for such integration. To conduct cybersecurity research, as is typical of the surveyed work on simulation, we have taken advantage of simulators that are entirely software-based or combine software and hardware. Our simulation environment is shown in Figure 13. The simulation testbed includes Typhoon-HIL® for simulating grid components, integrated hardware components (HillTop) including smart meters and controllers, simulated AMI, DR protocol devices (Virtual End Nodes (VENs) and Virtual Top Nodes (VTNs)), and consumer models. We have based our models on actual communications networks employed and the regulated electrical and physical processes in their OT and IT implementations. This initial simulation setup has allowed us to analyze not only the performance of particular grid instances but also allowed us to evaluate their security. Given the integration of tools and interfaces that allow attacking the grid instance, we have evaluated the effects of those attacks [58].

However, although this simulation testbed allows us to test the security of the grid implementation and its effectiveness, it still lacks abilities that would satisfy the gaps that we found in the literature. In particular, it cannot compose security policies and match them with appropriate mechanisms, as well as the attack method that can be used to test the security mechanisms. Such composition needs a configuration language and well-designed, interoperable interfaces for easy composition. These additional capabilities would allow us to easily test various scenarios by mixing and matching various policies and mechanisms. The ability to test various scenarios would enhance the simulation testbed's precision, security evaluation capabilities, reproducibility, and scalability while reducing the simulation configuration's expense, difficulty, and complexity. Additionally, we need to expand the testbed's synthetic data generation techniques with the ability to generate real-world attack data. We will continue our efforts, add these capabilities to the framework, and test and evaluate their usefulness.

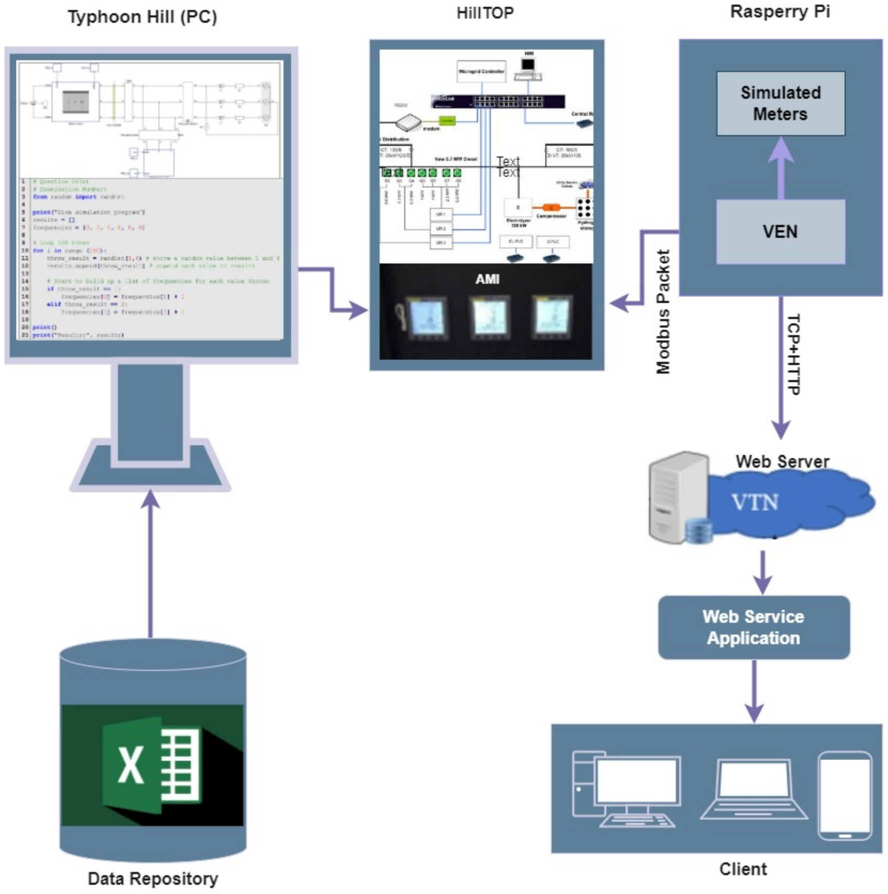

Figure 13. The implemented framework for an integrated approach of SG simulation

Abbreviations

AMI	Advanced Metering Infrastructure
SM	Smart Meter
CA	Cyber-attacks
DER	Distribute energy resources
DR	Demand response
IoT	Internet of Things
FDIA	False data injection attack
DoS	Denial of Service
ICT	Information and communication technologies
SG	Smart Grid
GEB	Grid-interactive Efficient Buildings
MiTM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
SCADA	Supervisory Control and Data Acquisition
CIA	Confidentiality, Integrity, and Availability
CPS	Cyber-physic system
IDS	Intrusion detection system
DSM	Demand side management
DNP3	Distributed network protocol version 3.0
APT	Advanced Persistent Threat

CP-SG	Cyber-Physical-Smart-Grid
NIDS	Network Intrusion Detection System
ICS	Industrial Control System
IED	Intelligent Electronic Device
HIL	Hardware-in-the-loop
CF	Cascading failure

References

1. Smith, M.; Ton, D. Key connections: The us department of energy? s microgrid initiative. *IEEE Power and Energy magazine* **2013**, *11*, 22–27.
2. Mikalauskas, I. Economic, Social and Environmental Benefits of Smart Grids. *European Journal of Interdisciplinary Studies* **2015**, *7*.
3. Gopstein, A.; Nguyen, C.; O'Fallon, C.; Hastings, N.; Wollman, D.; others. *NIST framework and roadmap for smart grid interoperability standards, release 4.0*; Department of Commerce. National Institute of Standards and Technology . . . , 2021.
4. 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.
5. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* **2016**, *388*, 1–29.
6. GICSP, E.H.; Assante, M.; Conway, T. An abbreviated history of automation & industrial controls systems and cybersecurity. *SANS Institute, Tech. Rep.* **2014**.
7. Kure, H.I.; Islam, S.; Razzaque, M.A. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences* **2018**, *8*, 898.
8. Otuoze, A.O.; Mustafa, M.W.; Larik, R.M. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology* **2018**, *5*, 468–483.
9. Yu, X.; Xue, Y. Smart grids: A cyber–physical systems perspective. *Proceedings of the IEEE* **2016**, *104*, 1058–1070.
10. Ghansah, I. *Smart grid cyber security potential threats, vulnerabilities and risks: Interim project report*; California Energy Commission, 2012.
11. Sun, C.C.; Liu, C.C.; Xie, J. Cyber-physical system security of a power grid: State-of-the-art. *Electronics* **2016**, *5*, 40.
12. Colak, I.; Sagiroglu, S.; Fulli, G.; Yesilbudak, M.; Covrig, C.F. A survey on the critical issues in smart grid technologies. *Renewable and Sustainable Energy Reviews* **2016**, *54*, 396–405.
13. Reda, H.T.; Anwar, A.; Mahmood, A. s. *Renewable and Sustainable Energy Reviews* **2022**, *163*, 112423.
14. Niu, X.; Li, J.; Sun, J.; Tomsovic, K. Dynamic detection of false data injection attack in smart grid using deep learning. 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2019, pp. 1–6.
15. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems* **2020**, *77*, 103201.
16. Chen, J.; Mohamed, M.A.; Dampage, U.; Rezaei, M.; Salmen, S.H.; Obaid, S.A.; Annuk, A. A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. *Applied Sciences* **2021**, *11*, 9972.
17. Pandey, R.K.; Misra, M. Cyber security threats—Smart grid infrastructure. 2016 National power systems conference (NPSC). IEEE, 2016, pp. 1–6.
18. Ackerman, P. *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*; Packt Publishing Ltd, 2017.
19. Krebs, B. FBI: Smart meter hacks likely to spread. *Krebs on Security. Available online: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/(accessed on 25 April 2012)* **2012**.
20. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks* **2014**, *67*, 74–88.
21. Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics* **2019**, *15*, 6522–6530.

22. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions. *Communications and Network* **2022**, *14*, 119–170.
23. Baig, Z.A.; Amoudi, A.R. An Analysis of Smart Grid Attacks and Countermeasures. *J. Commun.* **2013**, *8*, 473–479.
24. Batalla, J.M.; Vasilakos, A.; Gajewski, M. Secure smart homes: Opportunities and challenges. *ACM Computing Surveys (CSUR)* **2017**, *50*, 1–32.
25. Efstathopoulos, G.; Grammatikis, P.R.; Sarigiannidis, P.; Argyriou, V.; Sarigiannidis, A.; Stamatakis, K.; Angelopoulos, M.K.; Athanasopoulos, S.K. Operational data based intrusion detection system for smart grid. 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019, pp. 1–6.
26. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering* **2018**, *67*, 469–482.
27. Chen, B.; Pattanaik, N.; Goulart, A.; Butler-Purry, K.L.; Kundur, D. Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR). IEEE, 2015, pp. 1–6.
28. Bashendy, M.; Eltanbouly, S.; Tantawy, A.; Erradi, A. Design and implementation of cyber-physical attacks on modbus/tcp protocol. World Congress on Industrial Control Systems Security (WCICSS-2020), 2020.
29. Radoglou-Grammatikis, P.; Siniosoglou, I.; Liatifis, T.; Kourouniadis, A.; Rompolos, K.; Sarigiannidis, P. Implementation and detection of modbus cyberattacks. 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST). IEEE, 2020, pp. 1–4.
30. Darwish, I.; Igbe, O.; Saadawi, T. Experimental and theoretical modeling of DNP3 attacks in smart grids. 2015 36th IEEE Sarnoff Symposium. IEEE, 2015, pp. 155–160.
31. Tightiz, L.; Yang, H. A comprehensive review on IoT protocols' features in smart grid communication. *Energies* **2020**, *13*, 2762.
32. Pliatsios, D.; Sarigiannidis, P.; Lagkas, T.; Sarigiannidis, A.G. A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 1942–1976.
33. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials* **2018**, *20*, 3453–3495.
34. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.; Chopra, S.S. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies* **2020**, *13*, 5739.
35. Zografopoulos, I.; Hatziargyriou, N.D.; Konstantinou, C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal* **2023**.
36. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Computer networks* **2020**, *169*, 107094.
37. Naderi, E.; Pazouki, S.; Asrari, A. A coordinated cyberattack targeting load centers and renewable distributed energy resources for undervoltage/overvoltage in the most vulnerable regions of a modern distribution system. *Sustainable Cities and Society* **2023**, *88*, 104276.
38. Zografopoulos, I.; Konstantinou, C.; Hatziargyriou, N.D. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *arXiv preprint arXiv:2205.11171* **2022**.
39. Pazouki, S.; Naderi, E.; Asrari, A. A remedial action framework against cyberattacks targeting energy hubs integrated with distributed energy resources. *Applied Energy* **2021**, *304*, 117895.
40. Xu, S.; Tu, H.; Xia, Y. Resilience enhancement of renewable cyber–physical power system against malware attacks. *Reliability Engineering & System Safety* **2023**, *229*, 108830.
41. 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.
42. Ma, R.; Chen, H.H.; Huang, Y.R.; Meng, W. Smart grid communication: Its challenges and opportunities. *IEEE transactions on Smart Grid* **2013**, *4*, 36–46.
43. Santamarta, R. Here be backdoors: A journey into the secrets of industrial firmware. *Black Hat USA* **2012**.
44. Takiddin, A.; Ismail, M.; Nabil, M.; Mahmoud, M.M.; Serpedin, E. Detecting electricity theft cyber-attacks in AMI networks using deep vector embeddings. *IEEE Systems Journal* **2020**, *15*, 4189–4198.

45. Yao, J.; Venkitasubramaniam, P.; Kishore, S.; Snyder, L.V.; Blum, R.S. Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks. 2017 51st Annual Conference on Information Sciences and Systems (CISS). IEEE, 2017, pp. 1–6.
46. Murrill, B.J.; Liu, E.C.; Thompson, R.M. Smart meter data: Privacy and cybersecurity. Congressional Research Service, Library of Congress, 2012.
47. Ünal, F.; Almalaq, A.; Ekici, S.; Glauner, P. Big data-driven detection of false data injection attacks in smart meters. *IEEE Access* **2021**, *9*, 144313–144326.
48. Giaconi, G.; Gunduz, D.; Poor, H.V. Smart meter data privacy. *arXiv preprint arXiv:2009.01364* **2020**.
49. Shoreh, M.H.; Siano, P.; Shafie-khah, M.; Loia, V.; Catalão, J.P. A survey of industrial applications of Demand Response. *Electric Power Systems Research* **2016**, *141*, 31–49.
50. Fan, S.; Li, Z.; Yang, L.; He, G. Customer directrix load-based large-scale demand response for integrating renewable energy sources. *Electric Power Systems Research* **2020**, *181*, 106175.
51. Chen, Y.; Xu, P.; Gu, J.; Schmidt, F.; Li, W. Measures to improve energy demand flexibility in buildings for demand response (DR): A review. *Energy and Buildings* **2018**, *177*, 125–139.
52. Iqbal, S.; Sarfraz, M.; Ayyub, M.; Tariq, M.; Chakrabortty, R.K.; Ryan, M.J.; Alamri, B. A comprehensive review on residential demand side management strategies in smart grid environment. *Sustainability* **2021**, *13*, 7170.
53. Tang, D.; Fang, Y.P.; Zio, E. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods. *Reliability Engineering & System Safety* **2023**, *235*, 109212.
54. Sperstad, I.B.; Kjølle, G.H.; Gjerde, O. A comprehensive framework for vulnerability analysis of extraordinary events in power systems. *Reliability Engineering & System Safety* **2020**, *196*, 106788.
55. Abedi, A.; Gaudard, L.; Romerio, F. Review of major approaches to analyze vulnerability in power system. *Reliability engineering & System safety* **2019**, *183*, 153–172.
56. Anuebunwa, U.R.; Rajamani, H.S.; Abd-Alhameed, R.; Pillai, P. Investigating the impacts of cyber-attacks on pricing data of home energy management systems in demand response programs. 2018 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2018, pp. 1–5.
57. Heussen, K.; Tyge, E.; Kosek, A.M. Residential demand response behaviour modeling applied to cyber-physical intrusion detection. 2017 IEEE Manchester PowerTech. IEEE, 2017, pp. 1–6.
58. Manicavasagam, R.; Palmer, A.; Rogers, M.; Mahajan, S.; Craven, R.; Emeghara, C.; Senz, R. Testbed for Evaluating and Analyzing Smart Grid Behavior in Demand Response Scenarios. 2022 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2022, pp. 122–127.
59. Su, Q.; Li, S.; Gao, Y.; Huang, X.; Li, J. Observer-based detection and reconstruction of dynamic load altering attack in smart grid. *Journal of the Franklin Institute* **2021**, *358*, 4013–4027.
60. Yan, J.; Guo, F.; Wen, C. Attack detection and isolation for distributed load shedding algorithm in microgrid systems. *IEEE Journal of Emerging and Selected Topics in Industrial Electronics* **2020**, *1*, 102–110.
61. Khalaf, M.; Ayad, A.; Salama, M.M.; Kundur, D.; El-Saadany, E.F. Mitigation of Cyber-attacks on Wide-Area Under-Frequency Load-Shedding Schemes. *IEEE Transactions on Smart Grid* **2022**.
62. Pilz, M.; Naeini, F.B.; Grammont, K.; Smagghe, C.; Davis, M.; Nebel, J.C.; Al-Fagih, L.; Pfluegel, E. Security attacks on smart grid scheduling and their defences: a game-theoretic approach. *International Journal of Information Security* **2020**, *19*, 427–443.
63. Praveen, M.; Rao, G.S. Ensuring the reduction in peak load demands based on load shifting DSM strategy for smart grid applications. *Procedia Computer Science* **2020**, *167*, 2599–2605.
64. Jamil, M.; Mittal, S. Hourly load shifting approach for demand side management in smart grid using grasshopper optimisation algorithm. *IET Generation, Transmission & Distribution* **2020**, *14*, 808–815.
65. Zeeshan, M.; Jamil, M. Adaptive moth flame optimization based load shifting technique for demand side management in smart grid. *IETE Journal of Research* **2022**, *68*, 778–789.
66. Nasir, T.; Bukhari, S.S.H.; Raza, S.; Munir, H.M.; Abrar, M.; Muqeet, H.A.u.; Bhatti, K.L.; Ro, J.S.; Masroor, R. Recent challenges and methodologies in smart grid demand side management: State-of-the-art literature review. *Mathematical Problems in Engineering* **2021**, *2021*, 1–16.
67. Abdelsalam, A.A.; Zedan, H.A.; ElDesouky, A.A. Energy management of microgrids using load shifting and multi-agent system. *Journal of Control, Automation and Electrical Systems* **2020**, *31*, 1015–1036.

68. Logenthiran, T.; Srinivasan, D.; Vanessa, K. Demand side management of smart grid: Load shifting and incentives. *Journal of Renewable and Sustainable Energy* **2014**, *6*, 033136.
69. Youssef, E.N.S.; Labeau, F.; Kassouf, M. Detection of Load-Altering Cyberattacks Targeting Peak Shaving Using Residential Electric Water Heaters. *Energies* **2022**, *15*.
70. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Transactions on Smart Grid* **2018**, *9*, 2862–2872. doi:10.1109/TSG.2016.2622686.
71. Dabrowski, A.; Ullrich, J.; Weippl, E. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. 2017, pp. 303–314. doi:10.1145/3134600.3134639.
72. Cui, P.; Feng, L.; Xun, P.; Zhu, P. Load Scheduling of Thermostatical House-Hold Appliances Against Abrupt Changes in Smart Grid. 2017 10th International Symposium on Computational Intelligence and Design (ISCID), 2017, Vol. 1, pp. 470–475. doi:10.1109/ISCID.2017.129.
73. Delgado-Gomes, V.; Martins, J.F.; Lima, C.; Borza, P.N. Smart grid security issues. 2015 9th International conference on compatibility and power electronics (CPE). IEEE, 2015, pp. 534–538.
74. Kwon, Y.; Kim, H.K.; Koumadi, K.M.; Lim, Y.H.; Lim, J.I. Automated vulnerability analysis technique for smart grid infrastructure. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2017, pp. 1–5.
75. Seferian, V.; Kanj, R.; Chehab, A.; Kayssi, A. Identity based key distribution framework for link layer security of AMI networks. *IEEE Transactions on Smart Grid* **2016**, *9*, 3166–3179.
76. Xiang, X.; Cao, J. An efficient authenticated key agreement scheme supporting privacy-preservation for smart grid communication. *Electric Power Systems Research* **2022**, *203*, 107630.
77. Zhang, L.; Zhu, Y.; Ren, W.; Wang, Y.; Choo, K.K.R.; Xiong, N.N. An energy-efficient authentication scheme based on Chebyshev chaotic map for smart grid environments. *IEEE Internet of Things Journal* **2021**, *8*, 17120–17130.
78. Shehzad, F.; Javaid, N.; Almogren, A.; Ahmed, A.; Gulfam, S.M.; Radwan, A. A robust hybrid deep learning model for detection of non-technical losses to secure smart grids. *IEEE Access* **2021**, *9*, 128663–128678.
79. Khan, A.A.; Kumar, V.; Ahmad, M. An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. *Journal of King Saud University-Computer and Information Sciences* **2022**, *34*, 698–705.
80. Moghadam, M.F.; Nikooghadam, M.; Mohajerzadeh, A.H.; Movali, B. A lightweight key management protocol for secure communication in smart grids. *Electric Power Systems Research* **2020**, *178*, 106024.
81. Deepak, K.; Chandrasekaran, K. Investigating elliptic curve cryptography for securing smart grid environments. 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP). IEEE, 2020, pp. 1–7.
82. Chen, C.M.; Chen, L.; Huang, Y.; Kumar, S.; Wu, J.M.T. Lightweight authentication protocol in edge-based smart grid environment. *EURASIP Journal on Wireless Communications and Networking* **2021**, *2021*, 1–18.
83. Gopstein, A.; Hastings, N.; Feldman, L.; Agarwal, R.; Bartol, N. Distributed Energy Resource Security: Potential Guidelines and Research Topics **2021**.
84. Pour, M.M.; Anzalchi, A.; Sarwat, A. A review on cyber security issues and mitigation methods in smart grid systems. *SoutheastCon 2017* **2017**, pp. 1–4.
85. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies* **2021**, *14*, 5894.
86. Ghafouri, M.; Au, M.; Kassouf, M.; Debbabi, M.; Assi, C.; Yan, J. Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids. *IEEE Transactions on Smart Grid* **2020**, *11*, 5227–5238.
87. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R.; Leung, H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* **2019**, *7*, 80778–80788.
88. Yılmaz, Y.; Uludag, S. Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *Journal of the Franklin Institute* **2021**, *358*, 172–192.
89. Shahinzadeh, H.; Mahmoudi, A.; Moradi, J.; Nafisi, H.; Kabalci, E.; Benbouzid, M. Anomaly detection and resilience-oriented countermeasures against cyberattacks in smart grids. 2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS). IEEE, 2021, pp. 1–7.

90. Panthi, M. Anomaly detection in smart grids using machine learning techniques. 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T). IEEE, 2020, pp. 220–222.
91. Liu, X.; Nielsen, P.S. Regression-based online anomaly detection for smart grid data. *arXiv preprint arXiv:1606.05781* **2016**.
92. Himeur, Y.; Ghanem, K.; Alsalemi, A.; Bensaali, F.; Amira, A. Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. *Applied Energy* **2021**, *287*, 116601.
93. Feng, C.; Li, T.; Chana, D. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2017, pp. 261–272.
94. Fengming, Z.; Shufang, L.; Zhimin, G.; Bo, W.; Shiming, T.; Mingming, P. Anomaly detection in smart grid based on encoder-decoder framework with recurrent neural network. *The journal of china universities of Posts and Telecommunications* **2017**, *24*, 67–73.
95. Zhang, J.E.; Wu, D.; Boulet, B. Time series anomaly detection for smart grids: A survey. 2021 IEEE Electrical Power and Energy Conference (EPEC). IEEE, 2021, pp. 125–130.
96. Hyndman, R.J.; Wang, E.; Laptev, N. Large-scale unusual time series detection. 2015 IEEE international conference on data mining workshop (ICDMW). IEEE, 2015, pp. 1616–1619.
97. Zhang, L.; Shen, X.; Zhang, F.; Ren, M.; Ge, B.; Li, B. Anomaly detection for power grid based on time series model. 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). IEEE, 2019, pp. 188–192.
98. Wei, Q.; Ma, R.; Wang, Y.; Chen, M.; Sun, Y.; Liu, M.; Lin, X. Glad: A method of microgrid anomaly detection based on esd in smart power grid. 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). IEEE, 2020, pp. 103–107.
99. Gaddam, A.; Wilkin, T.; Angelova, M. Anomaly detection models for detecting sensor faults and outliers in the IoT-a survey. 2019 13th International Conference on Sensing Technology (ICST). IEEE, 2019, pp. 1–6.
100. Erhan, L.; Ndubuaku, M.; Di Mauro, M.; Song, W.; Chen, M.; Fortino, G.; Bagdasar, O.; Liotta, A. Smart anomaly detection in sensor systems: A multi-perspective review. *Information Fusion* **2021**, *67*, 64–79.
101. Marino, D.L.; Wickramasinghe, C.S.; Amarasinghe, K.; Challa, H.; Richardson, P.; Jillepalli, A.A.; Johnson, B.K.; Rieger, C.; Manic, M. Cyber and physical anomaly detection in smart-grids. 2019 Resilience Week (RWS). IEEE, 2019, Vol. 1, pp. 187–193.
102. Liu, X.; Nielsen, P.S. Scalable prediction-based online anomaly detection for smart meter data. *Information Systems* **2018**, *77*, 34–47.
103. Yuan, Y.; Jia, K. A distributed anomaly detection method of operation energy consumption using smart meter data. 2015 international conference on intelligent information hiding and multimedia signal processing (IIH-MSP). IEEE, 2015, pp. 310–313.
104. Jaiswal, R.; Maatug, F.; Davidrajuh, R.; Rong, C. Anomaly detection in smart meter data for preventing potential smart grid imbalance. 2021 4th Artificial Intelligence and Cloud Computing Conference, 2021, pp. 150–159.
105. Yen, S.W.; Morris, S.; Ezra, M.A.; Huat, T.J. Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. *International journal of electrical power & energy systems* **2019**, *109*, 1–8.
106. Rossi, B.; Chren, S.; Buhnova, B.; Pitner, T. Anomaly detection in smart grid data: An experience report. 2016 ieee international conference on systems, man, and cybernetics (smc). IEEE, 2016, pp. 002313–002318.
107. Banik, S.; Saha, S.K.; Banik, T.; Hossain, S.M. Anomaly Detection Techniques in Smart Grid Systems: A Review. 2023 IEEE World AI IoT Congress (AIIoT). IEEE, 2023, pp. 0331–0337.
108. Feng, L.; Xu, S.; Zhang, L.; Wu, J.; Zhang, J.; Chu, C.; Wang, Z.; Shi, H. Anomaly detection for electricity consumption in cloud computing: framework, methods, applications, and challenges. *EURASIP Journal on Wireless Communications and Networking* **2020**, *2020*, 1–12.
109. El-Awadi, R.; Fernández-Vilas, A.; Redondo, R.P.D. Fog computing solution for distributed anomaly detection in smart grids. 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2019, pp. 348–353.

110. Jaiswal, R.; Chakravorty, A.; Rong, C. Distributed fog computing architecture for real-time anomaly detection in smart meter data. 2020 IEEE sixth international conference on big data computing service and applications (BigDataService). IEEE, 2020, pp. 1–8.
111. Radoglou Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Panaousis, E. ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors* **2020**, *20*, 5305.
112. Mitchell, R.; Chen, R. Behavior-rule based intrusion detection systems for safety critical smart grid applications. *IEEE Transactions on Smart Grid* **2013**, *4*, 1254–1263.
113. Karimipour, H.; Geris, S.; Dehghantanha, A.; Leung, H. Intelligent anomaly detection for large-scale smart grids. 2019 IEEE Canadian conference of electrical and computer engineering (CCECE). IEEE, 2019, pp. 1–4.
114. Hong, J.; Liu, C.C.; Govindarasu, M. Detection of cyber intrusions using network-based multicast messages for substation automation. ISGT 2014. IEEE, 2014, pp. 1–5.
115. Yang, Y.; Xu, H.Q.; Gao, L.; Yuan, Y.B.; McLaughlin, K.; Sezer, S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks. *IEEE Transactions on Power Delivery* **2016**, *32*, 1068–1078.
116. Zhang, K.; Hu, Z.; Zhan, Y.; Wang, X.; Guo, K. A smart grid AMI intrusion detection strategy based on extreme learning machine. *Energies* **2020**, *13*, 4907.
117. Liu, Q.; Hagenmeyer, V.; Keller, H.B. A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access* **2021**, *9*, 57542–57564.
118. Ali, M.Q.; Al-Shaer, E. Randomization-based intrusion detection system for advanced metering infrastructure. *ACM Transactions on Information and System Security (TISSEC)* **2015**, *18*, 1–30.
119. Liu, X.; Zhu, P.; Zhang, Y.; Chen, K. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Transactions on Smart Grid* **2015**, *6*, 2435–2443.
120. Alseiari, F.A.A.; Aung, Z. Real-time anomaly-based distributed intrusion detection systems for advanced Metering Infrastructure utilizing stream data mining. 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). IEEE, 2015, pp. 148–153.
121. Banik, S.; Banik, T.; Banik, S. Intrusion Detection System in Smart Grid-A Review **2023**.
122. Smadi, A.A.; Ajao, B.T.; Johnson, B.K.; Lei, H.; Chakhchoukh, Y.; Abu Al-Haija, Q. A Comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges. *Electronics* **2021**, *10*, 1043.
123. Zhang, C.; Kuppannagari, S.R.; Kannan, R.; Prasanna, V.K. Generative adversarial network for synthetic time series data generation in smart grids. 2018 IEEE international conference on communications, control, and computing technologies for smart grids (SmartGridComm). IEEE, 2018, pp. 1–6.
124. Tushar, W.; Huang, S.; Yuen, C.; Zhang, J.A.; Smith, D.B. Synthetic generation of solar states for smart grid: A multiple segment Markov chain approach. IEEE PES Innovative Smart Grid Technologies, Europe. IEEE, 2014, pp. 1–6.
125. Zheng, X.; Wang, B.; Xie, L. Synthetic dynamic PMU data generation: A generative adversarial network approach. 2019 International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA). IEEE, 2019, pp. 1–6.
126. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials* **2016**, *19*, 446–464.
127. Ashok, A.; Krishnaswamy, S.; Govindarasu, M. PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid. 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2016, pp. 1–5.
128. Shampa Banik, T.; Manicavasagam, R.; Banik, T.; Banik, S. Simulation and Analysis of Cyber-Attack on Modbus Protocol for Smart Grids in Virtual Environment **2023**. doi:10.20944/preprints202309.0984.v2.
129. Banik, S.; Banik, T.; Hossain, S.M.; Saha, S.K. Implementing man-in-the-middle attack to investigate network vulnerabilities in smart grid test-bed. 2023 IEEE World AI IoT Congress (AIIoT). IEEE, 2023, pp. 0345–0351.
130. Koutsandria, G.; Gentz, R.; Jamei, M.; Scaglione, A.; Peisert, S.; McParland, C. A real-time testbed environment for cyber-physical security on the power grid. Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, 2015, pp. 67–78.
131. Adepu, S.; Kandasamy, N.K.; Mathur, A. Epic: An electric power testbed for research and training in cyber physical systems security. Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2. Springer, 2019, pp. 37–52.
132. Reda, H.T.; Ray, B.; Peidaee, P.; Anwar, A.; Mahmood, A.; Kalam, A.; Islam, N. Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid. *Sensors* **2021**, *21*, 1554.

133. Oyewumi, I.A.; Jillepalli, A.A.; Richardson, P.; Ashrafuzzaman, M.; Johnson, B.K.; Chakhchoukh, Y.; Haney, M.A.; Sheldon, F.T.; de Leon, D.C. Isaac: The idaho cps smart grid cybersecurity testbed. 2019 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2019, pp. 1–6.
134. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid* **2013**, *4*, 847–855.
135. Montoya, J.; Brandl, R.; Vishwanath, K.; Johnson, J.; Darbali-Zamora, R.; Summers, A.; Hashimoto, J.; Kikusato, H.; Ustun, T.S.; Ninad, N.; others. Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: A survey of smart grid international research facility network activities. *Energies* **2020**, *13*, 3267.
136. Alves, T.; Das, R.; Morris, T. Virtualization of industrial control system testbeds for cybersecurity. Proceedings of the 2nd Annual Industrial Control System Security Workshop, 2016, pp. 10–14.
137. Meghwani, A.; Srivastava, S.; Srivastava, A. Development of real-time distribution system testbed using co-simulation. 2020 21st National Power Systems Conference (NPSC). IEEE, 2020, pp. 1–6.
138. Ahmad, I.; Kazmi, J.H.; Shahzad, M.; Palensky, P.; Gawlik, W. Co-simulation framework based on power system, AI and communication tools for evaluating smart grid applications. 2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA). IEEE, 2015, pp. 1–6.
139. Mylonas, E.; Tzanis, N.; Birbas, M.; Birbas, A. An automatic design framework for real-time power system simulators supporting smart grid applications. *Electronics* **2020**, *9*, 299.
140. Venkataramanan, V.; Srivastava, A.; Hahn, A. Real-time co-simulation testbed for microgrid cyber-physical analysis. 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). IEEE, 2016, pp. 1–6.
141. Ciraci, S.; Daily, J.; Fuller, J.; Fisher, A.; Marinovici, L.; Agarwal, K. FNCS: A framework for power system and communication networks co-simulation. Proceedings of the symposium on theory of modeling & simulation-DEVS integrative, 2014, pp. 1–8.
142. Mihal, P.; Schvarcbacher, M.; Rossi, B.; Pitner, T. Smart grids co-simulations: Survey & research directions. *Sustainable Computing: Informatics and Systems* **2022**, *35*, 100726.
143. Le, T.D.; Anwar, A.; Loke, S.W.; Beuran, R.; Tan, Y. Gridattacksim: A cyber attack simulation framework for smart grids. *Electronics* **2020**, *9*, 1218.
144. Joubert, G.D.; Raji, A.K. Development and validation of a real-time testbed for renewable energy integration studies: South African grid code case study. *Journal of Engineering, Design and Technology* **2023**.
145. Tundis, A.; Egert, R.; Mühlhäuser, M. Attack scenario modeling for smart grids assessment through simulation. Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, pp. 1–10.
146. Darwish, I.; Igbe, O.; Saadawi, T. Vulnerability assessment and experimentation of smart grid DNP3. *Journal of Cyber Security and Mobility* **2016**, pp. 23–54.
147. Paul, S.; Ni, Z. Vulnerability analysis for simultaneous attack in smart grid security. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2017, pp. 1–5.
148. Rashed, M.; Kamruzzaman, J.; Gondal, I.; Islam, S. Vulnerability Assessment framework for a Smart Grid. 2022 4th Global Power, Energy and Communication Conference (GPECOM). IEEE, 2022, pp. 449–454.
149. Queiroz, C.; Mahmood, A.; Tari, Z. SCADASim—A framework for building SCADA simulations. *IEEE Transactions on Smart Grid* **2011**, *2*, 589–597.
150. Mets, K.; Ojea, J.A.; Develder, C. Combining power and communication network simulation for cost-effective smart grid analysis. *IEEE Communications Surveys & Tutorials* **2014**, *16*, 1771–1796.
151. Anderson, K.; Narayan, A. Simulating integrated volt/var control and distributed demand response using GridSpice. 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS). IEEE, 2011, pp. 84–89.
152. Wermann, A.G.; Bortolozzo, M.C.; da Silva, E.G.; Schaeffer-Filho, A.; Gaspary, L.P.; Barcellos, M. ASTORIA: A framework for attack simulation and evaluation in smart grids. NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016, pp. 273–280.
153. Barbierato, L.; Estebsari, A.; Pons, E.; Pau, M.; Salassa, F.; Ghirardi, M.; Patti, E. A distributed IoT infrastructure to test and deploy real-time demand response in smart grids. *IEEE Internet of Things Journal* **2018**, *6*, 1136–1146.

154. Abedi, A.; Romerio, F. Multi-period vulnerability analysis of power grids under multiple outages: An AC-based bilevel optimization approach. *International Journal of Critical Infrastructure Protection* **2020**, *30*, 100365.
155. Jarrah, M. Modeling and simulation of renewable energy sources in smart grid using DEVS formalism. *Procedia Computer Science* **2016**, *83*, 642–647.
156. Mongrain, R.S.; Yu, Z.; Ayyanar, R. A real-time simulation testbed for hierarchical control of a renewable energy-based microgrid. 2019 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2019, pp. 1–6.
157. Ahmad, A.; Khan, J.Y. Real-time load scheduling, energy storage control and comfort management for grid-connected solar integrated smart buildings. *Applied Energy* **2020**, *259*, 114208.
158. Yassine, B.I.; Boumediene, A. Renewable energies evaluation and linking to smart grid. *International Journal of Power Electronics and Drive Systems* **2020**, *11*, 107.
159. Mccarty, M.; Johnson, J.; Richardson, B.; Rieger, C.; Cooley, R.; Gentle, J.; Rothwell, B.; Phillips, T.; Novak, B.; Culler, M.; others. Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment. *IEEE Access* **2023**, *11*, 15297–15313.
160. Panda, D.K.; Das, S. Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. *Journal of Cleaner Production* **2021**, *301*, 126877.
161. Logenthiran, T.; Srinivasan, D.; Shun, T.Z. Demand side management in smart grid using heuristic optimization. *IEEE transactions on smart grid* **2012**, *3*, 1244–1252.
162. Gaur, G.; Mehta, N.; Khanna, R.; Kaur, S. Demand side management in a smart grid environment. 2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC). IEEE, 2017, pp. 227–231.
163. Samadi, P.; Mohsenian-Rad, H.; Schober, R.; Wong, V.W. Advanced demand side management for the future smart grid using mechanism design. *IEEE Transactions on Smart Grid* **2012**, *3*, 1170–1180.
164. Amin, B.R.; Taghizadeh, S.; Rahman, M.S.; Hossain, M.J.; Varadharajan, V.; Chen, Z. Cyber attacks in smart grid–dynamic impacts, analyses and recommendations. *IET Cyber-Physical Systems: Theory & Applications* **2020**, *5*, 321–329.
165. Abdelrahman, M.S.; Kharchouf, I.; Nguyen, T.L.; Mohammed, O.A. A Hybrid Physical Co-Simulation Smart Grid Testbed for Testing and Impact Analysis of Cyber-Attacks on Power Systems: Framework and Attack Scenarios. *Energies* **2023**, *16*, 7771.
166. Athari, M.H.; Wang, Z. Impacts of wind power uncertainty on grid vulnerability to cascading overload failures. *IEEE Transactions on Sustainable Energy* **2017**, *9*, 128–137.
167. Le, T.D.; Anwar, A.; Beuran, R.; Loke, S.W. Smart grid co-simulation tools: Review and cybersecurity case study. 2019 7th International Conference on Smart Grid (icSmartGrid). IEEE, 2019, pp. 39–45.
168. Moulema, P.; Yu, W.; Griffith, D.; Golmie, N. On effectiveness of smart grid applications using co-simulation. 2015 24th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2015, pp. 1–8.
169. Darwish, I.; Igbe, O.; Celebi, O.; Saadawi, T.; Soryal, J. Smart grid DNP3 vulnerability analysis and experimentation. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing. IEEE, 2015, pp. 141–147.
170. Jokar, P.; Leung, V.C. Intrusion detection and prevention for ZigBee-based home area networks in smart grids. *IEEE Transactions on Smart Grid* **2016**, *9*, 1800–1811.
171. Caire, R.; Sanchez, J.; Hadjsaid, N. Vulnerability Analysis of Coupled Heterogeneous Critical Infrastructures: a Co-simulation approach with a testbed validation. IEEE PES ISGT Europe 2013. IEEE, 2013, pp. 1–5.
172. Danilczyk, W.; Sun, Y.L.; He, H. Smart grid anomaly detection using a deep learning digital twin. 2020 52nd North American Power Symposium (NAPS). IEEE, 2021, pp. 1–6.
173. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *Ieee Access* **2019**, *7*, 46595–46620.
174. Zhang, Y.; Wang, L.; Sun, W.; Green II, R.C.; Alam, M. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid* **2011**, *2*, 796–808.
175. Boumkheld, N.; Ghogho, M.; El Koutbi, M. Intrusion detection system for the detection of blackhole attacks in a smart grid. 2016 4th International Symposium on Computational and Business Intelligence (ISCBI). IEEE, 2016, pp. 108–111.

176. Beigi-Mohammadi, N.; Mišić, J.; Khazaei, H.; Mišić, V.B. An intrusion detection system for smart grid neighborhood area network. 2014 IEEE International Conference on Communications (ICC). IEEE, 2014, pp. 4125–4130.

177. Palahalli, H.; Ragaini, E.; Gruosso, G. Smart grid simulation including communication network: A hardware in the loop approach. *IEEE Access* **2019**, *7*, 90171–90179.

178. Lo, C.H.; Ansari, N. CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid. *IEEE Transactions on Emerging Topics in Computing* **2013**, *1*, 33–44.

179. Flechais, I.; Mascolo, C.; Sasse, M.A. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics* **2007**, *1*, 12–26.

180. Potter, B.; McGraw, G. Software security testing. *IEEE Security & Privacy* **2004**, *2*, 81–85. doi:10.1109/MSP.2004.84.

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.