Energy Reports 11 (2024) 5760–5785

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Review article

Smart grids: A comprehensive survey of challenges, industry applications, and future trends

Jadyn Powell [a], Alex McCafferty-Leroux [b], Waleed Hilal [b], S. Andrew Gadsden [b,*]

[a] Western University, 1151 Richmond St, N6A 3K7, London, Canada
[b] McMaster University, 1280 Main St. W, L8S 4L7, Hamilton, Canada

ARTICLE INFO

Keywords:
Smart grids
Cybersecurity
Renewable energy integration
Energy storage
Interoperability
Machine learning

ABSTRACT

With the increasing energy demands of the 21st century, there is a clear need for developing a more sustainable method of energy generation, distribution, and transmission. Modern power grid infrastructures are currently managing these aspects, though their outdated configuration results in rigid and inefficient operation. The emerging technology of Smart Grids offers innovative solutions to these issues, utilizing advanced communication and computation structures. Through the integration of a bidirectional power and information flow, smart systems, and renewable energy sources, Smart Grids are the next generation of power grids, enabling cooperativity, automation, and efficiency. Even on small scales, the proposed benefits of the Smart Grid are substantial in maintaining sustainable energy use with growing demands. In this survey, we provide a comprehensive overview of Smart Grid technology, specifically focusing on the challenges presented by cybersecurity, interoperability, and renewable energy integration. These aspects were determined to be the most prevalent issues facing the advancement of Smart Grids, specifically for global application. We discuss these challenges thoroughly, determining the difficulties they induce and proposed solutions presented in literature. As such, this survey is intended to be a reference for other researchers, providing state-of-the-art approaches to solving these problems, as well as offering insights on ongoing issues and future endeavors. Additionally, we will highlight the current state of Smart Grid implementation through an analysis of programs and research being conducted by academic institutions, industry, and government.

1. Introduction

The electrical grid, pivotal in producing, transmitting, and distributing electricity, is instrumental to economic and social development. Its central role lies in spatially allocating electricity (Office of Electric Transmission and Distribution, 2003; Energy Sector Control Systems Working Group, 2011; Department of Energy and Climate Change, 2009; Electricity Advisory Committee, 2008a). Despite being lauded as one of the paramount engineering feats of the 20th century (Colson et al., 2012) and heavily relied upon by consumers, current electricity delivery methods are rigid.

Today's delivery systems, composed of various transmission and distribution networks, supply consumers with electricity from centralized generation stations (Gelazanskas and Gamage, 2013). Yet, this expansive, intricate system finds it challenging to meet the escalating demand for real-time, reconfigurable, and adaptive functionalities. Its continuous operation largely hinges on human intervention, owing to the absence of automated self-correcting features crucial in today's dynamic environments (Cunjiang et al., 2012). While there are ongoing incremental improvements in these systems, a thorough revamp of the infrastructure is indispensable to cater to the soaring demand for smart systems.

Enter the smart grid (SG), heralding a paradigm shift in electricity delivery. The SG integrates modern telecommunication and sensing technologies to enhance electricity delivery strategies (Blumsack and Fernandez, 2012). Unlike the traditional unidirectional grid, the SG introduces a bidirectional framework, facilitating a bidirectional flow of information and electricity (Fang et al., 2012). This evolution fosters increased customer engagement, enables the grid to operate more collaboratively, improves monitoring, enhances automation, and ensures widespread access to information (Blumsack and Fernandez, 2012).

With the SG's integration of advanced monitoring and sensing technologies, less human intervention is required. The grid evolves to possess self-healing abilities, enhanced demand response, and smoother renewable source integration. These advancements not only offer consumers and providers more flexibility but also open the doors to

* Corresponding author.
E-mail addresses: jpowel45@uwo.ca (J. Powell), mccaffea@mcmaster.ca (A. McCafferty-Leroux), hilalw@mcmaster.ca (W. Hilal), gadsden@mcmaster.ca (S. Andrew Gadsden).

https://doi.org/10.1016/j.egyr.2024.05.051
Received 23 January 2024; Received in revised form 9 May 2024; Accepted 20 May 2024
Available online 28 May 2024

technologies currently incompatible with the existing grid infrastructure (Hledik, 2009).

In light of the pressing need to combat climate change, the SG offers a promising avenue to slash carbon emissions in the power sector and seamlessly integrate renewable energy. Current power systems may become untenable, especially with energy production demands projected to soar by 70% by 2040. This spike underscores the urgency to develop an efficient, sustainable power system to meet future challenges (World Energy Outlook, 2016).

The objective of this paper is to furnish a comprehensive overview of the latest research on SGs, offering clear analyses of diverse research trajectories. We aim to collate recent contributions, chart advancements in the domain, and shed light on the SG's potential trajectory. The remainder of the survey unfolds as follows: Section 2 delves into related surveys in the domain. Section 3 elucidates the background of the SG. Section 4 tackles cybersecurity issues, threat classifications, and proposed solutions. Section 5 discusses the imperatives and challenges of interoperability, while Section 6 delves into renewable energy integration. Section 7 provides insights on SG industry applications and future trends, and Section 8 concludes the discourse.

2. Related publications

The evolution of SG research has seen numerous contributions spanning various areas. Over time, there has been a broad range of research literature published on SGs, including papers focused on broad-scale information, technologies, and architecture.

One of the first few survey papers provided about SG was published in 2010 and provides an overview of SG, including its drivers, evolution, standards, and research, development, and demonstration (RD&D) (Farhangi, 2010). Since then, several more survey papers have been published. This 2016 publication from Colak et al. (2016) provides a more updated overview of various SG components, such as cybersecurity, renewable energy integration (REI), and interoperability. More recent papers continued to be published, such as the following from 2020 (Dileep, 2020). This research provides an in-depth background of the SG's definition, architecture, functions, and possibilities. In a recent 2022 paper, Judge et al. provides a modern overview of the SG's performance and impacts and details the integration of renewable energy sources (Judge et al., 2022).

There are also other publications that thoroughly investigate a few of components of the SG. A 2020 paper provided a comprehensive overview of REI (Alotaibi et al., 2020), as well as Kawoosa and Prashar's work from 2021, which provides a comprehensive review of cybersecurity including classifications, threats, and proposed solutions (Kawoosa and Prashar, 2021).

Of the existing survey papers, two prominent limitations were present. Either the content was overly restrictive, or overly inclusive. The papers were very detailed about a small component of SG, or they provided a general overview of SG. Typically, these works do not present enough detail about the SG. Another significant issue is that few publications highlight the current state of implementation of SG worldwide. Regardless of various shortcomings, each paper presents valuable information for readers.

In this survey, the work of previous authors is extended, providing a thorough overview of SGs, their purpose, and benefits. We also address the limitations of the previously mentioned surveys, such as the inclusion of updated technologies, detailed but limited content, and emphasis on the overall state of the SG implementations. This paper also serves as an updated, comprehensive review of essential components of the SG, as well as its current state of implementation. This will be achieved by defining the SG, detailing its importance, and exploring its main components. The main components of the SG are also identified and explained, as well as the challenges and most updated proposed solutions. The current state of the SG is also highlighted, presenting some of the main countries' and continents' projects and the progress of implementing the SG.

3. Introduction to smart grid

3.1. Traditional electrical grids

The current electric power grid is a complex, physical infrastructure used for the distribution of electricity (Moretti et al., 2017). There are three main systems within the electric grid, including the electrical generation, transmission, and distribution systems. This integrated network is used to deliver electricity to consumers and includes the power plants used to generate electricity, the substations used to transform voltages, and the distribution facilities to deliver electricity from substations to consumers.

The physical infrastructure lacks automation, relying heavily on employee services for maintenance and repairs and continuously proves unsustainable as future technologies continue to develop, such as advanced metering, and remote monitoring. Despite being widely relied on, the current electric grid has a significant number of uncertainties, including aging infrastructure, and poor resiliency to disturbances. It is also nonlinear and incredibly complex (Khurana et al., 2010).

With the increased demand for more climate sustainable actions, the integration of renewable energy sources into the power grid is a necessary step. Unfortunately, this step will add even more complexity to the already complex system and present more challenges to several controllers at all levels of the power grid (Khurana et al., 2010). This clearly indicates that a more sustainable alternative to the electric grid, or heavy augmentation of it, will be necessary in the near future.

3.2. Smart systems

Smart systems are used to embed technology into already existing systems and processes to increase their efficiency and automation. They use incorporated functions such as sensing, actuating and controls to analyze situations making predictive and adaptive decisions.

Smart systems are able to learn, reason, control, and perceive themselves and their environment (Romero et al., 2020). They are able to self-organize and provide communication between various elements throughout the system (Romero et al., 2020). They can continuously perceive their surrounding environment, allowing the systems to update their internal knowledge, which is used for effective decision making (Romero et al., 2020). Through reasoning capabilities, smart systems are adaptable to both new states and objectives of their environment (Romero Aquino, 2021).

Smart systems have various applications and advantages, including improved security, interconnectivity, and improved functionality. The integration of smart systems to the current electrical grid will allow for solutions to various rising issues and for continued modernization in the future.

3.3. Smart grid

The SG is a new, modern grid combining smart systems with the current electrical grid. It uses a bidirectional flow of both information and electricity, creating an automated delivery mode (Hentea, 2021). It aims at improving energy efficiency and demand-side management, and reinforcing reliable grid protection through self-healing methods (Fang et al., 2012). It combines multiple bidirectional smart devices (e.g. sensors, actuators, and meters) which will provide real-time monitoring, balancing, and control at all times with high accuracy (Song et al., 2017a; Romero et al., 2020).

While the traditional grid can only distribute electrical power, the SG is able to make, communicate, and store its decisions, augmenting the current grid and enabling cooperative, responsive, and organic functions (Kitsios et al., 2017). It incorporates many unique technological features and increased monitoring, which makes the behavior of both the consumers and suppliers more apparent and therefore easier to understand (Venayagamoorthy, 2009). Fig. 1 above outlines the basic structure of a SG, showing the bidirectional flow of information and sequential power distribution (Tran et al., 2013).

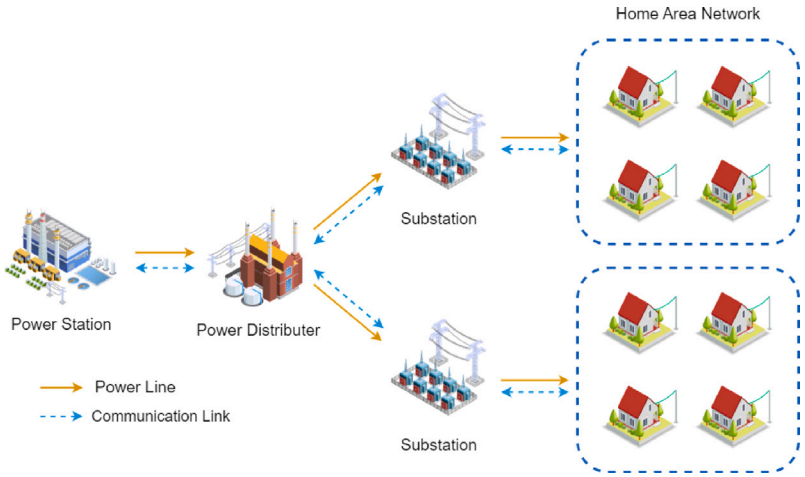

Fig. 1. Basic SG structure.
Source: Adapted from Tran et al. (2013).

3.3.1. Control and monitoring

The grid is operated, monitored, and controlled using Information and Communications Technologies (ICT). ICT enables energy companies to control the power demand, allowing for reliable and efficient power delivery at a reduced cost (Rajfallovska, 2016). Based on information received from consumers, the SG prepares and executes streamlined operations using bidirectional communications between electric power companies and consumers (Camacho et al., 2011). We can consider SG as being intelligent as it applies protection systems of the central/grid control, grid computing, complete diagnostic monitoring of transmission equipment, and self-healing power system networks using distributed computer agent (Paul et al., 2014). By using a Supervisory Control and Data Acquisition (SCADA) system, these technologies can be facilitated (Paul et al., 2014). SCADA is a specialized control system used to remotely monitor, control, and manage critical processes and equipment. SCADA systems collect data from sensors and instruments in the field, transmit and process the data. They allow operators to make informed decisions, initiate control actions, and respond to alarms and faults through the providing of real-time information about the status of processes and equipment.

3.3.2. Smart meters

Smart meters are another unique component of the SG which enables advanced metering infrastructure (AMI). This allows for more data to be collected and in a much more effective manner. Smart meters collect data every minute, whereas old metering data was recorded hourly or monthly. To improve metered grid data (i.e. voltage and current phasors) accuracy at more frequent sampling intervals, phasor measurement units (PMUs) can be applied. The PMU's implementation into SG has been extensively researched (see Paramo et al. (2022)), significantly contributing to the SG's advancements in the control, estimation, and security of power grids. As a comparison, modern PMUs collect up to 60 data points per second, whereas the current SCADA systems collect a single data point every 1 to 2 s (Khurana et al., 2010). Applying the AMI in the power distribution system and the PMU in the power transmission grid will provide the power grid a much more in-depth look at grid performance compared to the data available from SCADA technology (Khurana et al., 2010). Incorporating the use of additional smart technology in consumer's homes will expand control and monitoring of multiple devices connected to the power grid.

The integration of AMI implies a variety of advantages for SG technology. Considering demand response, AMI can enhance the application of such programs, monitoring real-time energy consumption. Demand response in the context of power grids is the incentivizing of consumers to reduce energy consumption across the grid to manage resources. As such, utility companies can notify customers to decrease their consumption when the energy demand is relatively high, preventing power-outages and balancing loads. Energy efficiency is also considered with AMI, where distributed generation can be enabled. Data collected from renewable energy sources (solar, wind, etc.) can be analyzed to manage resources effectively, as the power generated from these sources by the distributor or consumer is typically variable. Again, this can be taken advantage of to better prevent against outages and imbalance, while also harnessing a deeper understanding of irregular sources. Technology involved in integrating these resources is further discussed in Section 6.

Consumer engagement is an additional implication of AMI integration, where remote management and enhanced customer service can be expected. AMI collects significantly more data than current frameworks, which allows customers to manage usage effectively and for distributors to provide guidance on how their consumption can be more efficient. Two-way communication facilitates this process. Improved utility management is also suggested, where theft recognition and remote enabling capabilities allow distributors further control over energy. Remote enabling (or disabling) removes the physicality from the process, being able to quickly control energy supply to customers who avoid bill payments or are no longer residing at their previous location. The detection of energy theft is also facilitated with AMI, where consumption data can be analyzed to formulate patterns and therefore recognize anomalies. In theft, this would be indicated by no usage, where past data suggests that the consumer has regular usage at a specified time.

3.3.3. Anticipated benefits of smart grid

There are many anticipated benefits from the integration of SGs, originally listed by the National Institute of Standards and Technology (NIST) (NIST, 2010), and subsequently redefined by Fang et al. (2012). The benefits are categorized and described below.

- Grid Reliability and Quality Improvement
    1. Improving the quality and reliability of power transmission
    2. Improving resilience to grid related disruptions (e.g. power and data)
    3. Presenting opportunities for improving grid security
- Grid Efficiency and Optimization
    1. Optimizing the utilization of facilities, thereby avoiding back-up power plant construction

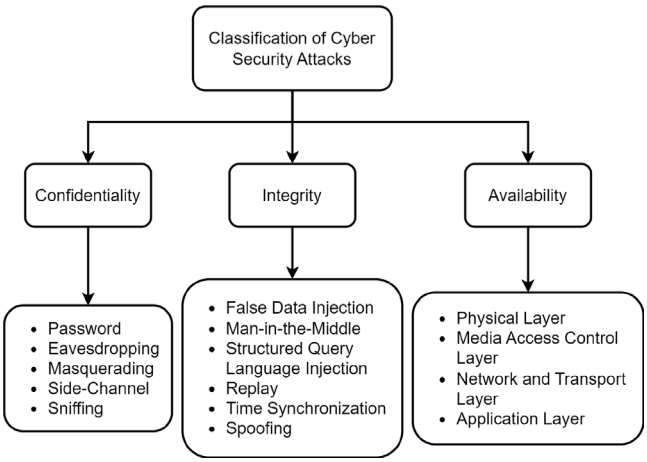

Fig. 2. SG classification of cybersecurity attacks.

2. Enhancing the capacity and efficiency of existing power networks
3. Automating maintenance and various operations

- Grid Modernization and Adaptation

1. Enabling self-healing reactions and predictive maintenance when subjected to disturbances
2. Advancing the renewable energy source deployment
3. Distributed power source accommodation
4. Standardizing new energy storage alternatives and the transition to plug-in electric vehicles

- Environmental Sustainability and Efficiency

1. Reducing greenhouse gas emissions through electric vehicle normalization and utilizing modern power sources
2. Minimizing inefficient generation during periods of peak-usage, and therefore oil consumption

- Market and Consumer-Related Enhancements

1. Increasing consumer choice
2. Enabling the introduction of new markets, services, and products

The benefits as described by NIST in NIST (2010) offer numerous benefits to the individuals, countries, and companies that adopt SGs. With environmental, security, and operational benefits augmented into the power grid, consumers can also expect to see an increased amount of choices offered to consumers considering their energy consumption, as well as new markets, services, and products. An example that applies to the United States (US) and many other countries, the implementation of SGs will be important for reducing the dependence on foreign oil and increasing clean energy production (NIST, 2010), therefore creating jobs and new commodities, manufacturing methods, etc. from that research. The first four major points on the list above are directly related to the following three sections of this survey, being cybersecurity, interoperability, and REI in SGs. Focusing research efforts on implementing these aspects into the power grid will continue to result in achieving the outlined benefits, vital to a sustainable living and future. It was remarked by the Department of Energy (DOE) in 2008 (Electricity Advisory Committee, 2008b) that if modern power grids were 5% more efficient than they currently are, the energy savings would be equal to the effect of eliminating the emissions of 53 million automobiles.

4. Cybersecurity

As electrical grids become more sophisticated, the number of risks they are vulnerable to increases (Berl et al., 2013). Some risks and threats are linked to the incorporation of digital communications, including cybersecurity and data privacy, reliability, and technical failures, while others come from changes in how power companies and their customers interact (Khurana et al., 2010).

The SG allows for close interaction at all levels of the power distribution, consumption, generation, and transmission systems. This means there is a high degree of coordination and communication amongst the various levels of the power grid system. This close interaction presents many more opportunities and the increased possibility of cyberattacks and cascade failures, which could affect all of the aforementioned systems (Khurana et al., 2010). This could lead to potentially catastrophic consequences, including energy market chaos, SG IT infrastructure failures, power blackouts, dangers to human safety, and damaged customer devices (Khurana et al., 2010). Less severe but more frequent consequences are also a possibility, such as small-scale outages (Khurana et al., 2010). The electric grid is essential, so it is necessary to devise and implement defense systems capable of supervising mass amounts of data, evaluating system status, identifying failures, predicting threats, and suggesting corrections (Khurana et al., 2010).

SG is considered by Gunduz and Das (2020) to be one of the most consequential applications of the Internet of Things (IoT). An IoT network enables devices the ability to communicate either directly, or through an internet gateway (Gunduz and Das, 2018, 2020). IoT-based SG systems are large, critical infrastructures, with complex architectures which are vulnerable to cyberattacks. Utilizing IoT applications is convenient for SGs, however, it poses several vulnerabilities. Considering that the monitoring and control operations are performed on internet-based protocols, the SG could potentially be appealing as critical infrastructure to malicious entities (Gunduz and Das, 2020). Due to this appeal, it is necessary to examine weaknesses in an SG component's security systems, as well as potential cybersecurity threats within its infrastructure (Gunduz and Das, 2020; Gündüz and Das, 2018a).

4.1. Classifying types of attacks

Due to the enormity of the system, both in terms of geographical distribution and complex infrastructure, identifying and classifying each individual possible attack would be nearly impossible. Instead, three principal security objectives are defined and must be incorporated into SG. These three security objectives are confidentiality, integrity, and availability, also known as the CIA triad, as seen in Fig. 2. The CIA triad is essential for both the management, operation, and protection of the system and communication infrastructures (Ardagna et al., 2021).

Cyberattacks in SGs target no less than one of the CIA triad objectives and are conducted to exploit information to use to attackers' advantage or to harm others (Gunduz and Das, 2020). Some attacks are coordinated to exploit various components of the SG and to launch simultaneous attacks. The most challenging attack to defend against, a coordinated attack can surpass common defenses, requiring multilayer security solutions with robust approaches (Gunduz and Das, 2020), such as those analyzed in Chen et al. (2021), Tian et al. (2019), Zhang et al. (2022). These types of attacks target all the components, requirements, and security objectives in an SG (Gunduz and Das, 2020).

Cyberattacks such as these can occur at numerous communication layers within SG (Wang and Lu, 2013). These layers, the network and transport layer, the MAC layer, and the physical layer are all affected differently by various types of attacks (Gunduz and Das, 2020). Identifying the types of cybersecurity threats enables effective and appropriate countermeasures (Gündüz and Das, 2018b). Security procedures achieved by investigating the cybersecurity requirements according to attack types and the communication layers affected will produce effective solutions for the security of the SG (Gunduz and Das, 2020).

Table 1
Types and descriptions of confidentiality attacks.

Type of Attack	Description of Attack
Password Attacks	Attempts to gain access by using an authorized person's password
Eavesdropping Attacks	Intercept wireless transmission on LAN, sniff IP packets in SG networks, or eavesdrop on messages shared between nodes
Masquerade Attacks	Attackers pretend to have authorization in order to access privileges
Side Channel Attacks	Performed to obtain cryptographic keys
Sniffing Attacks	Performed to gain access to TCP/IP packets or PMU contents transmitted over a network

4.2. Confidentiality attacks

Confidentiality attacks do not intend to change transmitted information over power networks. Instead, these attacks are used with the intention of achieving access to information by unauthorized parties (Rawat and Bajracharya, 2015). This information includes the customer's account details and power usage. If malevolent entities were to obtain customer account information, they may be able to commit identity theft, privacy invasions, phishing, and selling customer information. If they obtain power usage information, they may be able to commit billing fraud and energy theft.

Confidentiality attacks are typically considered to have minimal effects on the functionality of the communications in SG. However, the importance of customer privacy has gained more attention as more progress is made with the SG (Gunduz and Das, 2020). Table 1 below describes various attacks described in this paper that target confidentiality, such as password attacks, masquerade attacks, and side-channel attacks.

Smart meters measure and store large quantities of data and autonomously transport it to providers, consumers, and utility companies. If attackers intercept the private information of the consumer, it can be abused in many ways (Gunduz and Das, 2020). For example, it can be used to learn what appliances they use, keep track of their lifestyle, and by studying their power usage, determine whether they are at home or not (Gunduz and Das, 2020; Baig and Amoudi, 2013). It may even be possible to differentiate between various activities, such as watching television or sleeping (Khurana et al., 2010). Power usage analysis of businesses may also be able to indicate attackers' changes in business operations. Confidentiality is a leading issue for business owners and users (Rawat and Bajracharya, 2015).

Password attacks have various methods, such as password guessing or sniffing, social engineering, and dictionary attacks (Gunduz and Das, 2020). Social engineering is an especially popular method as it is used to penetrate systems through utilizing social skills, as opposed to technical attacks (Gunduz and Das, 2020; Yang et al., 2011).

Eavesdropping attacks are a passive attack type, which damages data confidentiality (Gunduz and Das, 2020). Eavesdropping attacks intercept wireless transmissions on local area networks (LAN), messages shared between communication network nodes, or sniff IP packets in SG networks (Gunduz and Das, 2020).

When masquerading attacks occur, attackers pretend to have authorization to access privileges (Gunduz and Das, 2020). Common applications of these types of attacks are identity spoofing and impersonation (Delgado-Gomes et al., 2015). Identity spoofing attacks enable attackers to imitate an authorized individual, without the possession of a user's password (Yang et al., 2011; Baig and Amoudi, 2013). Such attacks include Man-in-the-Middle (MITM), message replay, and network spoofing. Spoofing attacks involve modifications to the parameters of SG devices and can include procedures of Media Access Control (MAC), IP, and address resolution protocol (ARP) spoofing (Gunduz and Das, 2020).

Side-channel attacks are performed to obtain cryptographic keys (Gunduz and Das, 2020). Common types of this attack include timing attacks, power analysis attacks, and electromagnetic analysis attacks (Baig and Amoudi, 2013; Yang et al., 2011). Devices such as smart meters and home appliances are especially vulnerable to these attacks and can result in violations of privacy, information about usage, and administrative access (Gunduz and Das, 2020).

Using various tools for packet analysis or sniffing, an attacker can obtain TCP/IP packets of smart meters sent over the network or PMU contents (Gunduz and Das, 2020). TCP/IP packets, PMU, and smart meters are the primary targets of sniffing attacks, and lacking encryption, important information can be detected or collected by attackers (Gunduz and Das, 2020). The current practice for smart meters is the implementation of an X.509 certificate, which is a standard for device identification and cryptographic session establishment over the internet (Khurana et al., 2010). However, the cryptographic keys are static for each device, meaning that new methods should include a key management solution that can update cryptographic keys periodically (Khurana et al., 2010).

4.3. Integrity attacks

Attacks that target integrity aim to modify and/or disrupt the exchange of data within SG (Wang and Lu, 2013), which can lead to safety issues involving equipment or people (Yan et al., 2012). Integrity attacks focus on the content of the originally sent data (e.g. billing data, account data, control commands, sensor and voltage values, operating status of devices, etc.), and once intercepted are modified, reordered, or delayed (Gunduz and Das, 2020; Khelifa and Abla, 2015; Tan et al., 2017). Data integrity checks are often utilized to mitigate these attacks since this information is both personal to customers and valuable to companies. There are also fault-tolerant methods against data integrity attacks, as discussed in Jadidi et al. (2023), Liu et al. (2020). Though they are generally considered to be not as "brute-force" as other methods, attacks targeting data integrity are more sophisticated than attacks, targeting other categories of the CIA triad (Wang and Lu, 2013). Table 2 below describes various attacks described in this paper that target integrity.

The false data injection (FDI) attack is emerging as one of the most dangerous types of cyberattacks for SG. FDI occurs when bad data is injected into neighborhood area network (NAN) measurements or smart meters, targeting SG infrastructure (Gunduz and Das, 2020; Peng et al., 2019). The objective of the FDI is to damage the integrity of both monitoring and measurement sub-systems, resulting in cascaded poor judgment throughout the SG network (Rizzetti et al., 2015). Monitoring measurement manipulation would result in incorrect evaluations of the operating state of the system and therefore the destabilization of the SG, and to imprecise operational actions, such as pricing, planning, self-healing, or general flexibility (Gunduz and Das, 2020). Oozeer and Haykin comment that conventional malicious data detection and state estimation techniques have been applied to detect bad data in energy system state estimators and reduce observation errors (Oozeer and Haykin, 2019a). They are unable to, however, detect FDI attacks (Oozeer and Haykin, 2019a), leading to the development of more advanced or intelligent methods. If it is assumed that an attacker has already compromised one or more meters, Liu et al. (2011) suggested that the attacker is able to inject counterfeit data into the SCADA center, simultaneously passing the data integrity check utilized

Table 2
Types and descriptions of integrity attacks.

Type of Attack	Description of Attack
FDI Attacks	Incorrect data is introduced into NAN measurements or smart meters. They damage the integrity of monitoring and measurement subsystems, resulting in cascaded poor judgment in the SG network
MITM Attacks	Performed to damage the transmission between the smart meter and data concentrator units
SQL Injection Attacks	Transforms databases through the injection of script commands or malicious queries into the database, resulting in command over the system, modified or erased data, and additional manipulated data
Replay/Playback Attacks	Retransmits or delays messages after acquiring them through masquerading attacks. Initiated so attackers can direct energy to different locations and cause physical damage to the system
Time Synchronization Attacks	Targets timing data in SG, mainly PMU and WAPMC. TSA may generate incorrect location errors, triggering a false alarm indicating an issue, which can cause communication line interruptions, resulting in cascading faults
Spoofing Attacks	An attacker can impersonate other devices by exploiting the openness of the address fields on the MAC layer, enabling the ability to send false information

in the current state estimation process (Wang and Lu, 2013). The load redistribution attack (Yuan et al., 2011) is a variation of FDI, where only line power flow and load bus injection measurements and are influenced in the attack (Wang and Lu, 2013). Research in Yuan et al. (2011) demonstrates that these attacks can be considered as realistic FDI attacks, having constrained access to specific meters (Wang and Lu, 2013).

Data integrity attacks exploit vulnerabilities to corrupt processes in SG (Gunduz and Das, 2020; Bedi et al., 2018). Common methods of such attacks include MITM attacks and Structured Query Language (SQL) injections, each having their own variations. For MITM, these include compromised certificates, modified packet source/destinations, and route table poisoning (Gunduz and Das, 2020; Bedi et al., 2018). In SG applications, the data concentrator unit is connected to home area network (HAN) smart meters. Utilizing data modification attack methods (typically MITM), attackers are able to damage the data transmission between these two sub-systems, negatively influencing the accountability of the system and the CIA triad (Gunduz and Das, 2020).

SQL injection attacks are intended to inject script instructions and alter databases (Gunduz and Das, 2020). Smart meters continuously forward power consumption data to secure databases for both utilities and users, a prime target for these types of attacks. Malicious queries are injected into the database in order to add manipulated data, modify or delete existing data, or gain authority over the system (Gunduz and Das, 2020). These injections can result in disruptions to SG functions and even eventually result in blackout. Unless the queries formed by the database users are sufficiently validated before insertion, SQL injection can occur (Gunduz and Das, 2020).

Replay or playback attacks are designed to direct energy to a separate location in the grid and cause physical harm to the system (Gunduz and Das, 2020; Rawat and Bajracharya, 2015). Similar to previously discussed attacks, there are a variety of types of replay attacks, including covert attacks, which are their closed-loop versions (Sanjab et al., 2016) existing in short lengths of time and having a particular frequency (Ma et al., 2023). Replay attacks are likely to cause extremely serious effects on system stability, on global or localized scales across the SG, with losses being accumulated from either the delay itself or the attack signal. These attacks can be counteracted on authentication or fault detection/estimation levels. Numerous efforts have been proposed to counteract these attacks and preserve stability, such as in Abdelwahab et al.'s active detection using watermarking (Abdelwahab et al., 2020) and Pavithra and Rekha's fault detection and fast encryption algorithm (Pavithra and Rekha, 2021). Replay attacks occur when an entity acting as the primary source obtains the network traffic, and forwards the data to a destination. Following the acquisition of data through masquerading attacks, replay attacks are intended to delay or re-transmit messages (Gunduz and Das, 2020). Data can be injected into the system by attackers without significant modifications to measurable outputs, as well as target unencrypted sensors to initiate the replay attacks. Monitoring sensor outputs, attackers repeat them while injecting their attack signal (Gunduz and Das, 2020). Not only are false control signals are injected into the network in replay attacks, but attackers are able to analyze and access the data that is transmitted between devices and meters to obtain the target's energy generation and usage characteristics (Gunduz and Das, 2020).

Time synchronization attacks (TSAs) primarily target timing data in SG applications (Gunduz and Das, 2020). Event location, fault detection in transmission lines, monitoring voltage stability, and other applications of the PMU or WAPMC can be influenced by TSA, as these processes are heavily reliant on exact timing (Baig and Amoudi, 2013). For instance, global positioning system (GPS) spoofing, a type of TSA, aims at imitating a GPS signal, providing false times or locations that are typically used for breaches in defense (Larcom and Liu, 2013). TSAs may generate incorrect location errors and trigger false alarms, indicating an issue, as proven by the outcome demonstrated in Zhang et al. (2013). Gunduz and Das suggest that this false alarm can cause interruptions in communication lines, possibly triggering cascading faults in a SG (Gunduz and Das, 2020).

In the SG, spoofing is particularly harmful as it targets two categories from the CIA triad: availability and integrity. Exploiting the openness of address fields in a frame on the MAC layer of the SG, an attacker utilizing spoofing can disguise themselves as other devices to send false information from Wang and Lu (2013). Premaratne et al. explain in Premaratne et al. (2010) that in power substation networks, malicious nodes are able to broadcast forged ARP packets to collapse connections of all intelligent electronic devices (IEDs) to the substation gateway node.

4.4. Availability attacks

Attacks targeting availability, referred to as denial-of-service (DoS) attacks, aim to corrupt, block or delay communications in SGs (Wang and Lu, 2013; Pandey and Misra, 2016). A DoS attack can impair the operation of electronic devices and severely degrade a power system's communication performance, since it is expected to be consistently accessible (Wang and Lu, 2013). Attackers flood transmission lines in the network with large volumes of traffic, which results in the loss of legitimate data packets and thus not processed (Oozeer and Haykin, 2019a). The SG inherits the vulnerabilities in the TCP/IP stack and becomes vulnerable to DoS attacks since it applies TCP/IP stack and

Table 3
Types and descriptions of availability attacks.

Type of Attack	Description of Attack
DOS Attacks	Performed in an effort to corrupt, block, or delay SG communications
Physical Layer Attacks	Intended to crowd wireless communication lines with noise, blocking connection between users and smart meters
MAC Layer Attacks	Performed in an attempt to modify the MAC parameters of a device in order to cause performance degradation of other devices sharing the same communication channel
Network and Transport Layer Attacks	These attacks are launched in order to initiate degradation in end-to-end communication performance
Application Layer Attacks	Primarily focused on the transmission bandwidth in routers, computers, or communication channels, intended to exhaust computer resources, such as its CPU or I/O bandwidth

IP protocols (Aloul et al., 2012). Since availability is the dominant security requirement for SG, advanced and effective countermeasures must be adopted to defend against these types of attacks (Gunduz and Das, 2020). Table 3 below describes various attacks described in this paper which target availability.

DoS attacks can occur at various of communication layers within the SG, all having varying affects and severities (Wang and Lu, 2013), as described below.

4.4.1. Physical layer attacks

An effective method in launching physical layer attacks, especially for wireless communications, is with channel jamming, extensively covered in Strasser et al. (2008), Popper et al. (2009), Liu et al. (2010). It is quite simple to perform DoS attacks at this layer since it connection with communication channels is required, rather than authenticated networks (Wang and Lu, 2013). Wireless jamming is the primary attack in local area systems, since wireless technology will be widely used throughout these networks (Mohagheghi et al., 2009; Choi et al., 2008; Zhou et al., 2010; Leon et al., 2007; Pendarakis et al., 2007). These attacks aim to congest wireless communication lines with noise-corrupted signals, blocking connection between smart meters and users (Baig and Amoudi, 2013). Blocking data packages from being received, and communication channels being continuously seen as busy by routers result in a significant drop in smart meter performance and reliability (Gunduz and Das, 2020). Research performed by Lu et al. (2011) reinforce this, showing that jamming attacks can result in a variety of impairments to power substation systems, ranging from the delayed delivery of time-critical messages to total denial-of-service. Stavrou and Keromytis (2005) detail that an effective approach to these attacks is dispatching random unauthenticated packets to all wireless stations in the network, preventing attacks from following. With their novel spread spectrum approach, they effectively reject DoS attacks of differing degrees of sophistication and size, without the requirement of software or hardware augmentation (Stavrou and Keromytis, 2005). Another method proposed by Lee et al. (2012) offers security on the physical layer from random frequency hopping, similar to the spread spectrum approach.

4.4.2. Medium access control (MAC) layer attacks

The MAC layer is responsible for point-to-point communication (Wang and Lu, 2013). A compromised device could be used by a malicious entity to deliberately modify the MAC parameters, resulting in performance degradation of multiple devices that are coupled to a single communication channel. Therefore, MAC layer complications often contribute a relatively weaker class of a DoS attack (Wang and Lu, 2013).

4.4.3. Network and transport layer attacks

Considering the TCP/IP protocol model, the transport and network layers must provide reliability control for information delivery over multi-hop communication networks (Wang and Lu, 2013). At these layers, the DoS attacks can result in deteriorated performance of end-to-end communication (Wang and Lu, 2013), including worm propagation attacks over the Internet and distributed traffic flooding (Schuba et al., 1997; Yaar et al., 2003; Mirkovic and Reiher, 2004). Several studies have been conducted to assess the impact of transport- and network-layer DoS attacks on the power system performance (Wang and Lu, 2013). Jin et al. (2011) investigated the influence of a buffer-flooding attack on a DNP3-based SCADA network with real software and hardware, demonstrating the vulnerability of SCADA systems to DoS attacks (Wang and Lu, 2013).

4.4.4. Application layer attacks

Lower-layer attacks, which occur on the application layer, mainly focus on transmission bandwidth in routers, computers, or communication channels, and are intended to exhaust computer resources, like CPU or I/O bandwidth (Wang and Lu, 2013). Ranjan et al. (2009) demonstrate the overwhelming ability of these attacks towards a computationally limited computer, inducing failure from a continuous stream of computationally heavy demands. The SG is particularly vulnerable to the DoS attack, since its is comprised of innumerable computing and communication modules, some equipped with limited computational abilities (Wang and Lu, 2013).

4.5. Attack defenses

While there are standard protocols to help defend the SG against more thoroughly researched and understood confidentiality, integrity, and availability attacks, research into the newer attacks on the SG have increased, such as FDI attacks. However, sophisticated methods of defense are being developed as new threats arise in parallel. In this section we present a variety of methods concerning data and system protection against cyberattacks, outlining the topic generally and reviewing the state-of-the-art as found in literature.

4.5.1. Machine learning-based classification and detection

One approach that can be taken in mitigating the impact of harmful cyberattacks in SG is through detection and classification algorithms. Generally, the classification and detection of faults in any system is important to correct the fault, where in learning what these faults are and how they occur, we can employ self-healing methods. In the context of SGs, such faults can exist as cyberattacks, threatening the integrity of consumer data or accounting of distributor energy. They can also exist as the result of environmental or error factors, as SGs are highly complex nonlinear systems. Cyberattacks that influence such variables are discussed at length throughout Section 4. The concept of

fault detection was briefly discussed in Section 4.3, where methods such as state estimation and watermarking were applied for time synchronization and data replay attacks. These methods are, however, not always effective for complex attacks. For instance, the FDI attack has been observed to be undetectable with conventional methods. Currently, the best methods in detecting increasingly sophisticated attacks and natural faults lies in leveraging machine learning. Utilizing data, machine learning techniques such as deep or convolutional neural networks are demonstrated to provide accurate and rapid diagnoses of faults and cyberattacks.

He et al. (2017) proposed a real-time detection mechanism using deep learning-based mechanisms. Applying deep learning techniques, they recognize the behavioral patterns of the attacks through a historical analysis of the measurement data, and successfully implement the revealed features for real-time FDI attack detection. The results of their simulation illustrate the resilience of their detection scheme to the various amounts of attacked measurements, detection thresholds of the state vector estimator (SVE), and degree of environmental noise levels (He et al., 2017). Additionally, the ability of the employed scheme to achieve high detection accuracy in the presence of the occasional operation faults is demonstrated. Shi et al. (2021) proposed an approach aimed at statistical FDI attack detection based on a new dimensionality reduction method and a Gaussian mixture model. They proposed a technique that involves two phases: a dimensionality reduction process in the first phase and a semi-supervised learning process based on the Gaussian mixture model in the second (Shi et al., 2021). The simulation results from the tests demonstrate that the proposed scheme detected the FDI attacks with high detection precision and achieved the desired discrimination performance (Shi et al., 2021).

Oozeer and Haykin demonstrated how the entropic state and reinforcement learning was able to detect FDI attacks and drive them to a controllable state, under the action of cognitive risk control (CRC). The entropic state was originally proposed for use in smart grids in Oozeer and Haykin (2019a), and expanded on by the same authors in Oozeer and Haykin (2019b). In a cognitive dynamic system (CDS), the goal of the system is to both control the state and minimize the amount of unknown information in the perceptor. The latter is performed by minimizing this entropic state, which is done by dynamically optimizing the estimation process (Oozeer and Haykin, 2019a). The authors introduce the entropic states as a "new metric" for the SG, having two key purposes: to be used to detect FDI attacks and to provide an indication of the SG's health from cycle-to-cycle (Oozeer and Haykin, 2019a). Through task-switching control, the cognitive dynamic system (CDS) was able to enable a new executive with a different set of actions, augmenting the system configuration to bring the risk to a manageable state during an attack (Oozeer and Haykin, 2019a). The entropic state represents the information gap, quantifying uncertainty and in the case of Oozeer and Haykin (2019b), can be used to detect an attack. This CRC method has been applied to other systems, such as vehicle-to-vehicle (V2V) communication systems (Feng and Haykin, 2019), and the CDS method in control systems is a rising research topic. Machine learning based methods can also be applied for availability attack prevention on various layers, such as in research conducted by Jokar and Leung (2018) who proposed a detection and prevention scheme based on ZigBee.

4.5.2. Blockchain

To improve the scalability and distributed nature of SGs, systems have been integrated with the internet. Using the internet and wireless frameworks, SG components can communicate and exchange information across vast distances almost instantly, and users can access energy from anywhere. However, as energy consumers and distributors grow in number, the amount of connections (home, device, automobile, etc.) will also grow exponentially. This poses a problem for SG technology, where maintaining control over a continuously growing centralized network would require a variety of advanced communication and information infrastructures (Mollah et al., 2021). The centralization of large internet-based networks also requires sophisticated security protocols to be implemented, where the compromising of the central node implies the compromising of all the data in the network. To reduce to the detriments of a large centralized network and achieve more efficient operation, the command node can be decentralized. However, this can further introduce complexities in security as the number of nodes and users attached to them increases (Mollah et al., 2021), and additional innovative solutions are required. For achieving data security in a decentralized SG, researchers are currently investigating the application of Blockchain technology.

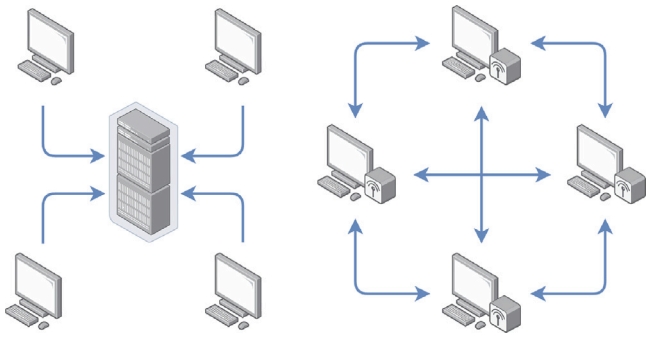

Fig. 3. (Left) Client–Server Network (Right) Peer-to-Peer Network.

Blockchain technology is becoming increasingly prominent as a method in decentralizing data. Fig. 3 contrasts the centralized and distributed frameworks, where centralized systems request resources and perform tasks from a single server, and the decentralized framework is peer-to-peer and partitions tasks across different entities. Most popular in cryptocurrency, Blockchain can be described as a distributed ledger with an increasing number of securely linked records known as blocks (Kumari et al., 2020). Cryptographic hashes are used for security within the block links, where subsequent blocks contain the cryptographic hash of the previous, as well as data concerning transactions and time. The cascading and related information between linked blocks effectively forms an irreversible chain of data. Blockchain networks are peer-to-peer (P2P), where their decentralization offers increased efficiency and security across data. Blockchain can vary in its permissions (Kumari et al., 2020), where for secure data transfer in SG applications, private Blockchain is most desirable against cyberattacks.

Mollah et al. compose a comprehensive survey on blockchain implementation in SG (Mollah et al., 2021), primarily for the purposes of data security in AMI, decentralized energy trading, monitoring and control, and EV charging. Kumari et al. (2020) contribute to this topic, facilitating efficient demand response management with blockchain-based secure energy trading. Their method was inspired by rising energy needs and the inherent vulnerabilities of the current centralized energy trading system to help accommodate this issue. For decentralizing and securing this system, authors employ blockchain technology, where they evaluate their framework's performance based on computation time and communication costs. Results were compared to that of a traditional centralized framework and determined that quality of service was significantly improved. Mengelkamp et al. (2018) also explores this application of blockchain, as well as Bansal et al. for electric vehicles (Bansal et al., 2019).

For energy monitoring, Gao et al. implement blockchain for the mitigation of compromised data over wireless networks, as well as improving consumer's understanding of their energy consumption (Gao et al., 2018). They outline the structure of their sovereign blockchain approach, using a unique block structure, where threading side blocks from parent blocks are used to identify consumers and their requests. All blocks on the chain are monitored, such that when attackers breach the structure of data access, the system is alerted. Their platform is

demonstrated against other systems to be robust while maintaining full consumer control and immutability over data. In research from Kumar et al. (2023), blockchain is leveraged alongside digital twins and deep learning for SG operation and security. Their blockchain-based authentication method features the ability to withstand a large number of attacks, while their deep learning framework enhances attack detection with their self-attention mechanism and softmax classifier. They demonstrate enhanced efficiency compared to conventional methods with their novel approach. Additional SG research that focuses on blockchain implementation for data security within the system include (Faheem et al., 2024; Mahmood et al., 2023).

4.5.3. Authentication

Another way of increasing cybersecurity in decentralized SG is through the application of authentication protocols. An alternative method in data privacy, authentication processes are different from Blockchain, where users must confirm their eligibility for access to devices or data. There are a variety of such schemes (El-hajj et al., 2019), including procedure, context, token, and identity-based, where their performance is based on the attack or context. Multi-way identification and hardware can also be introduced to improve the security of access. Generally, cyberattacks such as the MITM attack and replay attack can be negated by the use of more sophisticated authorization protocols.

Badar et al. utilize a secure authentication protocol for home area networks in SG-based cities (Badar et al., 2023). Their proposed framework incorporates lightweight mutual authorization with cryptographic one-way hash functions, promoting surveillance and security in SG metering infrastructure. Additionally, they implement a physical unclonable function (PUF) for meter data encryption, ensuring cyberattack resilience due to its un-reproducible property. To validate their proposed method, they demonstrate its effectiveness against a variety of attacks (MITM, replay, etc.) and compare its computation and cost performance against alternative methods. Another lightweight authentication protocol was developed by Fouda et al. (2011), based on the Diffie–Hellman key establishment protocol and hash-based authentication. Additionally, Saxena et al. discuss a joint authentication/authorization scheme for confidentiality attacks that requires these processes to be verified simultaneously (Saxena et al., 2016), and W. Chim et al. propose their tamper-resistant-device-based Privacy-preserving Authentication Scheme for Smart grid networks (known as PASS) (Chim et al., 2011).

4.5.4. Data encryption

Encryption is another security parameter that aligns with Blockchain and authentication, encoding data that is transferred end-to-end, protecting it from malicious entities. To add, interception prevention is not a feature of encryption, but encrypted data that is intercepted would be unusable without the key. Encryption using cryptographic keys is a crucial process in Blockchain technology and usually, these keys are pseudo-randomly generated, granted to authorized recipients. Decryption without such keys is possible, though sophisticated resources in algorithmic computation are typically needed for modern methods. Although, if we consider the limited memory, battery life, and computational ability of typical SG components (tablets, thermostats, meters, etc.), the encryption process itself is constrained in its complexity. Because of this heterogeneity, effective and lightweight encryption processes must be employed for SG applications to protect data against cyberattacks.

Countering confidentiality attacks with data encryption and authentication processes are among the more widely applied methods, used for nearly every interaction made on the internet. Concerning SG, Gao et al. explore a hybrid method of data encryption that compresses and encrypts the data in a single step (Gao et al., 2014). This approach, known as EncryCS, was determined to improve both security and transmission efficiency (Gao et al., 2014). Alternatively, Syed et al. pursued homomorphic encryption for secure training of deep learning networks used for fault identification and localization of smart grids (Syed et al., 2020). To terminate the various types of integrity attacks, end-to-end encryption and authentication schemes are necessary (Gunduz and Das, 2020). Sanjab et al. (2016) discuss implementing sequence numbers and timestamps as an effective solution against replay attacks in SG applications. Shapsough et al. (2015) outlines cryptography algorithms as methods to prevent data integrity attacks. Rawat and Bajracharya (2015) also lists increased security in SG monitoring through utilizing the PMU more frequently, volt-VAR control based schemes, power fingerprinting techniques, and the prevention of integrity attacks towards data by using trusted network connection-based approaches. As a means of countering MITM attacks, security gateways can be utilized to encrypt network traffic (Gunduz and Das, 2020). Security gateways are able to create VPN tunnels for network connection, data encryption at the source, and decryption at the target (Gunduz and Das, 2020). Typically, the encryption processes occur within hardware solutions. Also, both the target and source of information should be authenticated to interrupt and stop MITM attacks, as shown in Mrabet et al. (2018).

4.5.5. Infrastructure

To manage these cybersecurity techniques and put them into practice, SG security infrastructure must be considered. SG infrastructure in this context can apply to a variety of hardware and software procedures for maintaining robust security, such as cloud computing, data centers, and various secure infrastructure systems, like firewalls and public key infrastructure (PKI). These frameworks are additive to previously discussed network security methods, reinforcing these concepts or making them possible. For instance, utilizing cloud computing complements the limited computation of typical SG components, enabling enhanced security by off-loading the processes.

Applying measures as discussed by Bedi et al. (2018), SQL injection attacks can be significantly lessened across SG networks. They list various SQL defenses such as initiating penetration tests, static code checking, positive pattern matching, input type checking, avoiding the use of dynamic SQL, limiting database access to remote users, and filtering semicolons during type checking (Bedi et al., 2018). Metke and Ekl (2010) also discussed including trusted computing methodologies and PKI, which tethers a user's identity to a public key using a digital certificate. They believed that utilizing PKI technologies is the most desirable solution for SG security, including the "policies and procedures which describe the set up, management, updating, and revocation of certificates", beyond software and hardware improvement (Metke and Ekl, 2010). Ugale et al. relates SG security and reliability to efficient and dependable communication infrastructures, where the standard in meeting these requirements is attributed to cloud computing (Ugale et al., 2011). Adopting the distributed computing framework in SGs and their devices allows for increased computation, resulting in the ability to utilize advanced control and encryption frameworks. As such, higher efficiency and levels of security can be achieved globally in the system. Data storage capacities are additionally increased, which can be leveraged by intelligent frameworks (e.g., machine learning based anomaly detection) for more informed decision making.

5. Interoperability

Interoperability refers to the ability to exchange and make use of information. Interoperability presents one of the main features of SG and consists of the capacity of the network technologies, sensors, and electrical devices to use the interchanged information (Ayadi et al., 2019). In order for SGs to respond to changes automatically and dynamically in grid conditions, there is a need for sensors to provide real-time status and information (Song et al., 2017a). This will require seamless connectivity throughout the transmission and distribution system, to enhance the energy flow coordination with real-time analysis and information (Kim et al., 2020). Interoperability improves the reliability of SG by transferring collected information directly to the equipment, thus improving and protecting the operations of the grid (Kim et al., 2020).

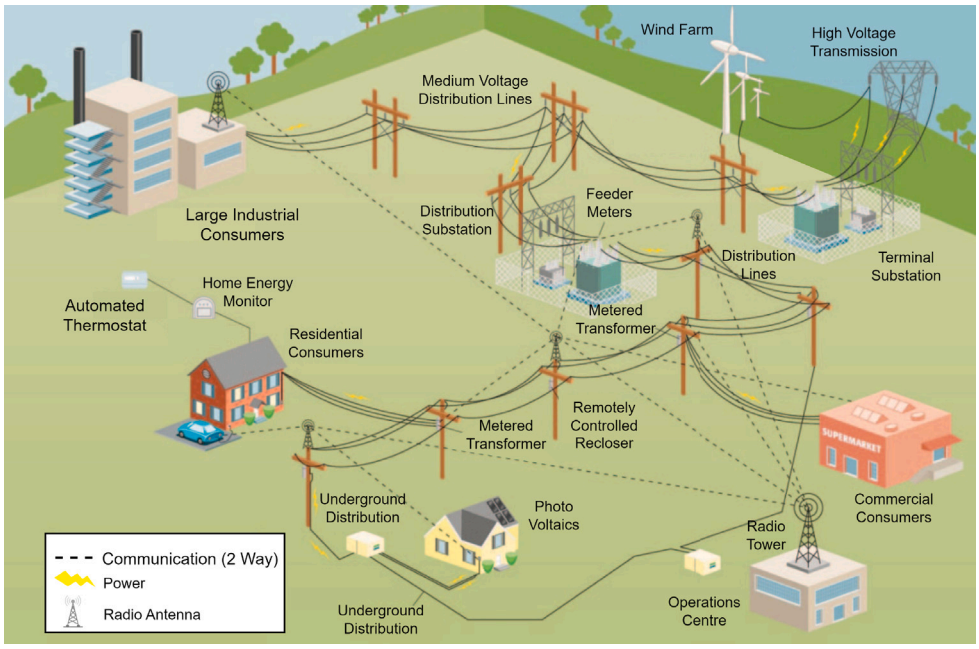

Fig. 4. Infrastructure of SG interoperability (Ayadi et al., 2019).

It will improve efficiency and stability of the SG network to avoid overwhelming load on the grid and reduce possible blackouts (Ma et al., 2013). Fig. 4 (Ayadi et al., 2019) provides an example of infrastructure for SG interoperability.

The SG's measurements, communications, and control technologies are used to support system operations maintaining a balance between load demand and electrical generation (Song et al., 2017a). The geographical disbursement of sensing and measurement devices on the world-scale pose a challenge towards general scalability, availability, and interoperability (Song et al., 2017a). Interoperability and data exchange between sensors are major challenges for the SG.

An example of a vital operation that heavily relies on the monitoring and measurement of electrical parameters in the distribution and transmission networks is grid control (Song et al., 2017a). Sensors are implemented to measure the physical parameters of transmission lines, power generation, distribution lines, substations, energy storage, and consumers (Song et al., 2017a). Such sensors include current transformers (CTs), voltage transformers (VTs), smart meters, humidity and temperature sensors, accelerometers, pyranometers and pyrheliometers (for solar irradiance measurement), internet protocol (IP) network cameras, power quality monitors and many more (King, 2018).

Control and Monitoring applications require various types of information, such that the sensor data should meet the expected distribution network operations. Some requirements of SG sensors are:

- Accurate synchronization of sensors to Coordinated Universal Time (UTC) (Song et al., 2017a).
- Exceedingly accurate sensitivity and accuracy of measurements, such as for voltage/current magnitudes and phase angle (Song et al., 2017a; Goldstein, 2017)
- Rapid processing of intelligent algorithms and data, such as producing synchronized frequencies, phasors, and rate of change of frequency (ROCOF) estimates (Song et al., 2017a; Mak, 2010)
- Fast, reliable, and secure standards-based data transmission and network communications (Song et al., 2017a).
- Sensor variety featuring dynamic range and high bandwidth, such as measuring frequencies, voltages, and currents accurately across a wide range (Song et al., 2017a; Yurish, 2010)
- Smart capabilities, including self-localization, self- identification, self-calibration, self-diagnostics, and self-awareness (Song et al., 2017a; Yurish, 2010)
- A multitude of sensing capabilities for physical (temperature, climate, weather, etc.) and electrical (power flow, current, voltage, etc.) parameters (Song et al., 2017a).
- Standardized testing methodologies and interfaces to assist in achieving Smart Sensor (SS) interoperability and plug-and-play capabilities (Song et al., 2017a).

5.1. Communication and data exchange

Effective communication is critical to the successful deployment of SG, where domains and sub-domains of the substations will use an assortment of private and public, wired, and wireless communication networks to interchange information (Farrokhabadi et al., 2017). Here we outline the communication infrastructure required for this inherent SG property, which is an important consideration for interoperability between equipment. With updating communication methods and SG equipment, maintaining interoperability is an essential research consideration for contending with future energy demands. Interoperability in this respect enables SGs to communicate and develop rapidly, at a reduced cost, in a versatile manner for all components.

In general, telecommunication infrastructure is crucial, however wireless communications offers much more freedom for information collection, dissemination, and processing. Many suggestions for communication methods have been made and some of the most commonly considered communication technologies are ZigBee, Wireless Mesh, and Power Line Communication (PLC). ZigBee is a short-range wireless communication used in home area networks (Bari et al., 2014), wireless mesh network communication connects multiple devices as nodes in a larger network (Saadatmand et al., 2017), and PLC is a wire line communication technique that is applied at very low costs (Ayadi et al., 2019). Some relatively new, less explored communication options are detailed as follows. Fig. 5 below also provides a representation of the multiple communication layers involved in SG.

5.1.1. Wireless sensor network (WSN)

Wireless sensor networks (WSNs) are able to construct an extremely reliable power grid with self-healing capabilities, necessary in the deployment of SGs (Ma et al., 2013). Modern advancements in WSNs have enabled the development of embedded electric utility monitoring systems (Gungor et al., 2010). Some potential applications in the SG

Table 4
Summary of communication solution papers.

Year	Reference	Method
2012	Li et al. (2012)	Wireless communications for advanced metering infrastructure.
2013	Markovic et al. (2013)	Cloud computing model
2011	Feng and Yuexia (2011)	SG communications architecture three different operating modes: relay control, distribution, and home levels.
2020	Shahinzadeh et al. (2020)	Joint 5G-IoT frameworks in SG and the associated enhancement in interoperability.
2021	Alaerjan (2021)	Distributed Data Interoperability Layer (DDIL)
2018	Alaerjan et al. (2018)	Data distribution system-based approach.
2021	Cavalieri (2021)	Merging of two common communication systems in both IoT and SG domains: oneM2M and IEC 61850
2020	Bergmann et al. (2020)	An approach to drive semantic interoperability, led by NIST, the DOE, and multiple other national US laboratories.

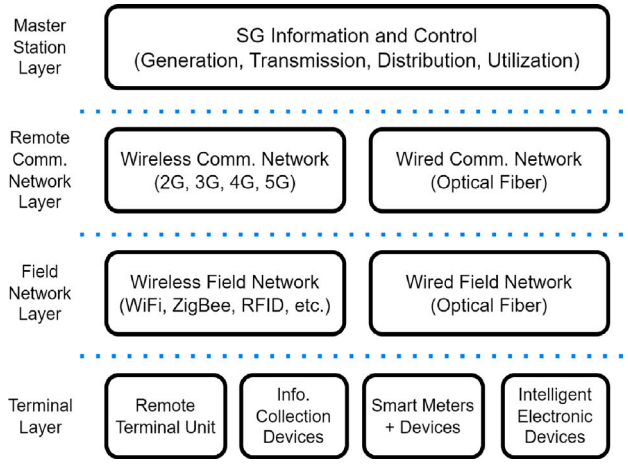

Fig. 5. SG communication layers (Shahinzadeh et al., 2020).

include fault sensing, remote monitoring, and wireless automatic meter reading (WAMR) (Gungor et al., 2010; di Bisceglie et al., 2009). WSNs can be implemented and utilized across the whole SG network because of its flexibility, rapid development, and low cost (Ma et al., 2013).

5.1.2. SG interoperability platform (SGIP)

To address common interoperability issues, the novel SGIP communication method consists of managing data and communication driven interoperability, enabling data-centric communication in SG (Kim et al., 2017a). The data-driven interoperability is guaranteed through the implementation of a common semantic model, ensuring systems communicate in the same way (or, "in the same language") (Kim et al., 2017a). The SGIP design is based on many questions and several requirements, including support of both publish–subscribe and client–server communication, support of reconstructing data objects, and configurable quality of service (QoS) attributes for reliable communication (Kim et al., 2017a). Efforts have been made by NIST as well to establish a SG interoperability panel (also called SGIP) and interoperability in smart sensors (Song et al., 2018).

5.1.3. Advancements in communication

Table 4 presented below, summarizes the papers related to communications as examined in this section.

The authors in Li et al. (2012) proposed the application of wireless communications for AMI. Focused on efficiency and security, they propose a method that enables smart meter transmission when the large changes are exhibited, referred to as Change and Transmit (CAT) (Li et al., 2012). It was based on data that implies that the real-time power consumption of households is most often constant and the change of power use follows the Poisson distribution (Li et al., 2012). From this trend, however, an attacker could eavesdrop and know when a user is home. Considering this, the CAT method also utilizes an Artificial Spoofing Packet (ASP) to send false packets to attackers (Li et al., 2012). The scheme proposed by the authors accounts for the Poisson power consumption nature to administer their wireless communication infrastructure and was effective for mitigating attacks, comparing the effectiveness of adjusted defense schemes.

Markovic et al. (2013) provides an in-depth discussion on a cloud computing model for SGs, where the delivery of computing is introduced as a service. This means that information, software, and storage are provided to devices as a product. Cloud computing is an architecture deemed suitable for SG applications, since its services can achieve storage and transfer of data, communication, and real time computation at substantial scales (Markovic et al., 2013). The authors highlight the benefits and disadvantages of cloud-based schemes, where for instance, its dependence on internet connectivity poses operational and security issues (Markovic et al., 2013). Additionally, specific applications and use-cases are outlined in the scope of cloud computing in SG, with an emphasis on modern systems (state of the art a decade ago) and future challenges that have been the subject of research since.

Proposed in Feng and Yuexia (2011) is an SG communications architecture using modern wireless communication technologies, operating in three different modes: relay control, distribution, and home levels. The distribution mode is cooperative, and because of its structure, it can dynamically solve complex coverage problems with low losses and costs, and unified resources, suitable for SGs (Feng and Yuexia, 2011). The relay-based system is also cooperative, featuring a node structure that can communicate with other nodes directly or by picking off its connection to another node (Feng and Yuexia, 2011). This can also be thought of as the wireless mesh discussed in Saadatmand et al. (2017). The home or indoor mode is short range, but can achieve high quality and fast connections using little power, similar to a WiFi network (Feng and Yuexia, 2011). Exhibiting low latency and high bandwidth characteristics, the architecture proposed that encompasses all three nodes was effective in several video monitoring and on-demand experiments, scalable for SGs.

Researchers in Shahinzadeh et al. (2020) presented an introduction to 5G communication networks and the Role of Joint 5G-IoT Framework for SG Interoperability Enhancement. They analyzed the fundamentals of 5G communication and the 5G-IoT purposes in SG. From their review, it was concluded by the authors that the development of communication infrastructure with 5G-IoT has positive impacts on the flexibility, autonomy, reliability, speed, security, and economy of operation of the SG (Shahinzadeh et al., 2020). Speed in SG communication is a crucial benefit, where cybersecurity and stability are improved with decreased transmission delays.

In their research, Alaerjan (2021) presented a Distributed Data Interoperability Layer (DDIL). This layer is a connectivity layer, enabling seamless data exchange between applications in IoT domains.

Table 5
Summary of interoperability testing papers.

Year	Reference	Method
2018	Papaioannou et al. (2018)	Analysis of current methods and principles of interoperability testing. Proposes a method for developing SG interoperability tests.
2017	Song et al. (2017a)	Passive interoperability test scheme for smart sensors, ensuring interoperability of sensor data.
2022	Song et al. (2022)	Procedure for modeling the interoperability of smart sensor interactions, while applying finite state processes and labeled transition systems to automatically and quantitatively measure and assess the interoperability.
2020	Ginocchi et al. (2020)	Testing methodology proposed in Sanjab et al. (2016) and investigates a flexibility activation mechanism in a power grid system.

Using model transformation techniques, the DDIL addresses data interoperability issues. It is "developed into a set of configurable features to support the flexibility requirements in IoT applications" (Alaerjan, 2021). The DDIL was designed to be modular and extendable, and develop four applications based on different protocols to test its effectiveness in a simulated SG environment (Alaerjan, 2021). Experimental results demonstrated that the proposed DDIL successfully allows seamless data exchange between the communicating applications, even on constrained devices (Alaerjan, 2021). Alaerjan et al. (2018) also detailed a data distribution system-based approach for addressing interoperability challenges that exist in SG. A unified data model was adopted to build data distribution system topics, acting as the primary data exchange medium. Their experiment corroborated the viability of the data distribution system and its potential in supporting the interoperability of protocols (Alaerjan et al., 2018).

Researchers in Cavalieri (2021) proposed a novel solution towards the unification of two of the most commonly applied communication systems in IoT and SG domains: oneM2M and IEC 61850. Their semantic interoperability solution is primarily based on the concept of common ontology between different ontologies and oneM2M ontology-based interworking (Cavalieri, 2021). It was also proposed to be applied to the interworking strategy. A detailed illustration of the architecture was provided, consisting of the IEC and IoT servers, the IoT domain, the interworking proxy application entity (IPE), and the proposed ontology (Cavalieri, 2021). Cavalieri's proposal forwards the advancement of IoT implementation in SG, contributes to the limited scope of literature focused on IPE, and expands on the oneM2M definition (Cavalieri, 2021).

Presented in Bergmann et al. (2020) by Bergmann et al. was an approach to drive semantic interoperability, led by NIST, the DOE Building Technologies Office, and several other US national laboratories. Their approach consists of the following steps: a semantic interoperability standard to regulate and identify the interoperable attributes of applications and equipment, industry coordination and engagement, and tools to assist in testing and implementation, ensuring product compliancy with semantic interoperability specifications (Bergmann et al., 2020). Their approach accelerates the timeline for the adoption of other semantic interoperability specifications (Bergmann et al., 2020).

5.2. Standards

Standards help to ensure interoperability and confidentiality considering communication in SGs. Communication standards are a set of rules dictating the method, timing, and content of communication for a variety of scenarios and paths. They are generally used in SG and other interacting systems to increase communication quality and efficiency, and reduce uncertainty in task execution. In the context of SG, furthering the development of these standards is essential in grid modernization, where increased communication fidelity implies the improved implementation, speed, and robustness of cybersecurity measures, remote metering, data analysis, etc. Standards are an additive and necessary parameter to existing SG technologies. There are a plethora of existing standards and protocols that have been established for SG equipment specifically or other technologies. Additionally, new standards are constantly being developed to increase SG interoperability. Two key guidelines used to designate standards are if they support the evolution of SG interoperability, and the standard's level of support from the establishing agency.

There are numerous standards for varying types of SG applications, discussed extensively in a survey from Demertzis et al. (2021). Such standard categories examined in their work include smart transmission systems, advanced distribution management and automation, energy resources, and AMI. They also discuss developing standards at the time of writing, or standards that require additional mappings and configurations. An example of a crucial standard is IEEE 1815-2012 (DNP3), which is a set of communications protocols applied between elements for the automation of process systems (Song et al., 2017a). DNP3 plays a vital role in SCADA systems, developed for communications between different types of control and data acquisition equipment (IE.E.E. Standards Association, 2012). There are lists of standards presented in the document created by the NIST based on comments from stakeholders, public review, and workshops (Ma et al., 2013). For example, IEEE 1588 is used for time synchronization and management of equipment across SGs, and IEC 61850 Suite is for communications within transmission and distribution sectors, as noted by NIST (NIST, 2010).

5.3. Testing

Although standards help with some interoperability challenges presented in SG, issues can still arise. Interoperability testing is key to achieving seamless interoperability of SG applications, due to the complexity involved in aspects of modern power systems (Ginocchi et al., 2020). Interoperability testing is used to verify that multiple devices and/or systems are capable of interoperability based on the same standards, preventing against the failure of a system with non-standardized equipment (Durand, 2012). Table 5, seen below, summarizes the papers related to interoperability testing examined in this section.

The authors of Papaioannou et al. (2018) presented an analysis of current methods and principles of interoperability testing, and proposed a method for developing/prototyping SG interoperability tests. Papaioannou et al. describes the method as a series of steps, the first being identifying the use case of the method, with the second and third involved in determining the BAP and BAIOP profiles (Papaioannou et al., 2018). The following steps are involved in the experiment's statistical design, interoperability testing, and final analysis (Papaioannou et al., 2018). The method provided a modern theoretical analysis of working methods proposed for addressing SG interoperability.

Researchers in Song et al. (2017a,b) proposed a passive interoperability test scheme for smart sensors to ensure the interoperability

of sensor data. Passive methods are typically generalized as interoperability fault monitoring methods, whereas active methods apply some stimuli to the system to test what normal operation is Ginocchi et al. (2020). The research describes the capabilities of smart sensors, as well as the model's compatibility with PMU (Song et al., 2017a). The method was tested, and the results demonstrate the functionality of the proposed interoperability test scheme. Passive methods are also explored in Chen (2013).

The authors of Ginocchi et al. (2020) used the testing methodology proposed in Papaioannou et al. (2018) and applied it to a specialized SG use case. The situation examines a flexibility activation mechanism and flexibility source interactions in power grid systems (including DSO SCADA) and Remote Terminal Units to support a voltage regulation service. The method incorporates a design of the experiment and testing procedures described by Papaioannou et al. (2018), using a physical test bed that simulates the power grid and communication network (Ginocchi et al., 2020). Experimental results proved the applicability of the procedure from Papaioannou et al. (2018) for testing the large scale interoperability of more complicated SGs. It was determined that rigorous analyses of statistics are required for a proper investigation of interoperability performance and parameter interactions (Ginocchi et al., 2020).

Song et al. (2022) describes a procedure for modeling the smart sensor interoperability considering interactions. Applied to a case study of the interaction between an IEEE C37.118 PMU-based sensor and phasor data concentrators, the model was designed generically as a message operation between sender/receiver (Song et al., 2022). They used finite state processes and labeled transition systems to quantitatively and automatically assess and measure interoperability (Song et al., 2022). The model worked to improve interoperability by identifying and resolving interoperability issues in the case study, without a time constraint (Song et al., 2022). Based on other standard protocols, their model could additionally be applied for interoperability modeling of other smart sensors.

6. Renewable energy integration (REI)

While the traditional power grid is comparatively limited, the electrical energy flow and generation in SG is considerably more adaptable (Fang et al., 2012). SG allows for safe integration of renewable energy resources into the grid, supplementing the power supply with the power generated and stored by a consumer (Khurana et al., 2010). Modern grids are also capable of this net metering system in some places, such as for homes that have solar panels. The utilization of renewable energy sources in the electrical grid is rapidly increasing, due to a need for reduced dependency on conventional energy sources (i.e., fossil fuels) and high power demands. The integration of renewable energy sources into SG is being continuously studied and advanced due to its realized importance (Mohamed et al., 2015).

6.1. Challenges

Renewable energy source integration into the power grid poses multiple technical issues (Ochoa and Harrison, 2011). These include reliability, efficiency, energy conversion cost, power quality, security, safety, and the appropriate management of loads (Ming et al., 2010; Liserre et al., 2010; Shafiullah et al., 2010). Renewable energy generation is incredibly variable, and the quantity of power generated is greatly impacted by the weather forecast. Integrating variable generation presents many unique challenges to the performance of the power grid, including key factors such as the power movement type and generator design, expected run types, the position of the grid in relation to renewable energy sources, the interactions between different renewable energy sources, and the general characteristics of the grid (Ming et al., 2010; Shafiullah et al., 2010). There are many significant challenges SG system developers (Fadaeenejad et al., 2014), with plenty of research being conducted about current and future issues. After surveying current and future applications for SG REI, (Gaviano et al., 2012) ensured that electronic device communication is a crucial technology to integrate renewable energy sources.

6.2. Benefits

Despite there being numerous challenges, there are also multiple positive impacts that the integration of renewable energy will have on the grid system. First, is the positive environmental impact. REI within the grid enables less dependency on energy generated by fossil fuels which will reduce carbon dioxide emissions (Ayadi et al., 2020). The impact on the climate can be minimized by making it simpler to incorporate renewable energy sources, where SGs leverage automation systems, usage data and models, and bidirectional communications for improved efficiency (Khurana et al., 2010). Second, there is a positive social aspect. When people utilize their own energy production systems (such as rooftop solar panels), they can receive rebates for generating their own energy, as well as having a contingency if there is a power grid failure (Ayadi et al., 2020). Finally, there is a positive economic aspect as increased integration of renewable energy will create new jobs.

6.3. Variability

Non-renewable energy sources are typically controllable and reliable and generate a consistent amount of energy (Worighi et al., 2019). Unfortunately, renewable energy sources do not generate a stable quantity like non-renewable sources and are heavily influenced by a variety of conditions. Consequently, one of the main challenges of using renewable energy sources are their intermittency and stochastic behavior (Akhtar and Rehmani, 2015). Renewable energy sources are fundamentally different than non-renewable generation since the production is uncertain, intermittent, and not dispatched (unable to be controlled on demand) (Bitar et al., 2011). Variability is the term used to encompass these three characteristics and presents one of the most important obstacles of the deep penetration of integrating renewable generation into the power grid system (Moura, 2009). Penetration in the context of renewable energy and SG refers to the percentage of electricity generated for a SG by a renewable resource, where in deep penetration, a high percentage of total energy is generated by these sources. Deep penetration is a more recent vision for the SG, but the limited predictability and variability of these renewable energy sources have presented a myriad of technical challenges for grids (Eltigani and Masri, 2015). These challenges include methods of energy storage management, effective forecasting, power system stability, voltage control, and demand management systems (Xie et al., 2011; Shafiullah et al., 2010; Commission et al., 2012; Wasiak and Hanzelka, 2009; Camacho et al., 2011).

Modern operations of the electrical power system are designed to accommodate the natural load demand variability, as well as adapt to both unplanned and planned contingencies, at different timescales (Bitar et al., 2011). This is performed through implementing operational reserves, load frequency control, unit and scheduling commitment, load shedding, and demand response (Bitar et al., 2011). At deep penetration levels, renewable energy sources add significant variability, not capable of being handled by the current system. Previous research has suggested that the existing management mechanisms could only handle renewable generation up to 20% penetration levels (Energy Great Lakes Regional Wind, 2010; Energy et al., 2010). The reconfiguration of these mechanisms comes with significant operational and cost issues (DeCesaro et al., 2009).

Solar and wind energy pose the main problems for deep penetration of REI, since hydroelectric, geothermal, and biomass energy sources are considered, by their nature, relatively more predictable and stable, having no notable issues with SG integration (Ming et al., 2010; Shafiullah et al., 2010). This is mainly due to the fact that they are mature processes, but more importantly, power companies have near-full control over the fuel source.

6.3.1. Solar

Solar power generation has a natural daily cycle of variability, and beyond this, weather changes such as cloud cover can significantly affect the source's power output. For instance, solar insolation can vary by more than 80% of its peak in a very short time (Marcos et al., 2011). Considering this, the absorption of solar rays are needed for solar panels to generate electricity, hence it is essential to optimize both the size and direction of the panels to maximize energy generation (Worighi et al., 2019). Additionally, it is vital to consider other factors such as the maximum power output of the panel and supporting devices such as inverters. Also, solar panel performance depends on several factors such as the quantity of sunlight, air density, temperature, and efficiency (Worighi et al., 2019).

6.3.2. Wind

Wind is another renewable energy source with high variability. Wind speed and direction are consistently unpredictable due to weather changes and seasons. Severe weather can result in wind turbines operating at unsafe speeds, forcing a shutdown, and it is also difficult to obtain accurate and reliable forecasting of wind power production (Bitar et al., 2011). To achieve the integration of wind power in SG, four conditions must be met: the phase sequence of the power frequency and the wind power frequency must be close to the grid, the terminal voltage magnitude must match the grid, and the phase angle between the two voltages must be within five percent (Caribbean Renewable EnergyDevelopment Programme (CREDP), 2004).

6.4. Forecasting

Challenges in grid operations with deep penetration of renewable energy sources become far more manageable if accurate solar and wind energy production forecasts are available beforehand Bitar et al. (2011). Meteorology plays a substantial role in improving REI into the grid network. Knowing the relevant long-term weather patterns is needed to develop a smarter power grid (Shafiullah et al., 2010). Accurate forecasting can mitigate the negative effects of integrating renewable energy sources and can allow for statistical correlations between meteorological hazards and production (Ourahou et al., 2020). In addition to scheduling systems, forecasting accuracy is essential for establishing sustainable load management systems, and for using renewable resources appropriately (Shafiullah et al., 2010).

Accurate weather forecasting can alleviate some of the variability issues encountered by wind and solar. As the accuracy of the weather forecast increases, the prediction of how much energy will be generated by renewable sources will become more accurate, reducing uncertainties in generation. Weather forecasting has existed for centuries, however, more modern methods are being developed to produce more accurate forecasts. Hewage et al. (2021) proposed an effective deep learning-based, fine-grained weather forecasting model. For forecasting, the proposed model utilized multiple layers that used surface weather parameters across a time span. Their experiment showed the model produced better results than the typical weather research and forecasting (WRF) model, proving its accurate forecasting potential up to 12 h (Hewage et al., 2021). Also for SG, Wang et al. (2024) developed an accurate deep learning model for solving the difficult problem of wind speed forecasting. They demonstrated higher precision predictions than other models using their two-stage data processing method (Wang et al., 2024).

6.5. Power quality

There are many potential technical challenges that can be faced with increasing the penetration of renewable energy sources. Among the most crucial concerns of these is power quality. It is generally desirable for electrical power to be transmitted reliably, and in a stable manner across an entire system. Power quality is a measure of how consistently the transmitted energy meets these specification, where failure in achieving consistently high levels of quality can result in system damage, shutdown, or malfunction. This notion is especially important for the commercial power grid and SG, where data loss can be an additional consequence to region-wide power loss.

There are a variety of factors that can influence power quality, which can be the result of deep renewable energy penetration in the context of SG. These challenges include voltage fluctuation, reactive power, power system transients and harmonics, switching actions, electromagnetic interference (EMI), synchronization, low power factor, long transmission lines, storage systems, forecasting and scheduling, and load management (Ming et al., 2010; Liserre et al., 2010; Cartwright, 2006). In literature, there have been numerous advancements in counteracting these issues in the context of SG, which will be reviewed for select factors in this section. For efficiency, it is vital for devices connected to traditional power grids and SG to meet the required power quality standards.

6.5.1. Voltage fluctuation

Voltage fluctuation can occur randomly or systematically, and are characterized by variations in normal voltage values. This can degrade equipment performance or result in current or voltage instability, which can consequentially result in overheating, efficiency loss, etc. Normally, fluctuations less than 10% do not significantly effect electronic equipment (Masoum and Fuchs, 2015), but effects vary across frequency and equipment sensitivities. Voltage fluctuation is a substantial consequence of solar- and wind-based energy because of the intermittency of generation (Shafiullah et al., 2010), reducing the longevity of most equipment since even small fluctuations disturbs sensitive electronic components (Linh, 2009; El-Tamaly et al., 2007). Periodic disturbances to network voltages, known as flicker, are a significant issue seen in weak grids. The degree of flicker is quantified by the allowable difference in voltage in terms of frequency and the short-term severity level (Shafiullah et al., 2010; Bossanyi et al., 1998).

A short survey was conducted by Colak and Kayisli (2021) considering voltage and frequency fluctuations effects in smart power electronics, where active control methods were examined for solutions in wind power. Faraji et al. propose their own central control system for stabilizing the traded active power between the smart photovoltaic (PV) inverter and upstream network, as well as a volt-VAR control strategy for symmetric and asymmetric fluctuations in the PV inverter (Faraji et al., 2024). Their solution to power quality issues for solar power networks was demonstrated to be an improvement over the studied conventional methods. Visser et al. also consider PV solar power systems in an urban power grid, proposing three separate voltage regulation strategies for mitigating fluctuations (Visser et al., 2022). Specifically, they explore active power curtailment, grid reinforcement, and supercapacitors. Kuwałek (2021) alternatively studies the identification and localization of voltage fluctuations considering power grids, indicating the origin of the disturbance load and estimating parameters associated with it. Their novel approach targets smart metering infrastructure, using a statistical assessment of the estimated voltage signal component propagation.

6.5.2. Harmonic distortion

Harmonic distortion can be characterized by the presence of undesirable frequency components in power systems. Non-linear appliances with power electronics inject harmonics into the grid, which have the potential to induce voltage distortion issues (Shafiullah et al., 2010). Such power quality issues can result in increasing temperatures, faulty regulation, timing issues, and efficiency losses. To keep the total harmonic distortions to an acceptable level, these operation harmonics must be minimized. According to IEEE standards, power system harmonics should be limited in two ways: by the harmonic voltage supplied by the utility to any customer at the point of common coupling

(PCC) and the harmonic current injectable by users into the utility system at the PCC (Shafiullah et al., 2010; Khadem et al., 2010).

Using a hybrid control approach with Namib beetle optimization and recalling enhanced neural networks (NBO-RERNN), Rajesh et al. achieve improved power quality by mitigating harmonics in a PV generation system (Rajesh et al., 2024). With a cascaded multilevel inverter, the optimality of their hybrid controller is increased, fulfilling load demands and reducing the impacts of additional disturbances in the grid. Ghaffari et al. also explore harmonic distortion and efficiency loss mitigation in SG, where they instead apply optimal siting and sizing of wind turbines and their storage systems (Ghaffari et al., 2024). Zhao and Milanović (2024) were able to achieve accurate prediction of individual order and total harmonic distortions in a renewable energy-integrated SG, using sequential artificial neural networks with limited monitoring. In identifying the origins of harmonics, authors are ale to mitigate their effects on power effectiveness. Joga et al. alternatively apply dual-tree complex wavelet transforms (DTCWTs) of voltage and current signals to extract features from non-active power quantities to identify harmonics (Joga et al., 2024).

6.5.3. Electromagnetic interference

Another factor contributing to the degradation of power quality is EMI. The result of electromagnetic induction, conduction, or coupling, EMI induces a disturbance on electronics that can severely degrade their performance or functionality. Considering power transmission, this is especially harmful, resulting in efficiency losses or failure in components. Additionally, EMI can deteriorate data paths in wireless networks, which are vital to SG operation. Shadare et al. outline notable sources of EMI in SGs (Shadare et al., 2017), where power electronic interfaces (such as AMI) can introduce errors such as compromised energy readings. Since integrating systems that produce EMI is inevitable, numerous protection and mitigation strategies have been researched.

Artificial intelligence is leveraged for EMI fault detection and classification in SG transmission lines (Chetan Khadse and Chaudhari, 2021) by Khadse et al.. Bayesian regularization networks are trained on feature extracted fault datasets, where their proposed framework exhibits high accuracy, outperforming conventional methods. EMI can also be intentional, where malicious entities induce failures or errors in SG using high power EMI sources placed in proximity to essential equipment. Arduini et al. (2023) studies the effects of this type of exposure on SCADA protection relays, identifying failure modes and conducting a risk assessment. Nateghi et al. investigate intentional EMI, identifying the effects of EMI sweep frequency jamming signals in wireless smart meters (Nateghi et al., 2021).

6.5.4. Reactive power

Where active power is the power expended by the load, reactive power exists as stored energy and is reflected back to SG. Reactive power occurs due to out of phase voltage and current in AC circuits. Reactive power is the portion where no net transfer occurs, and the energy oscillates between the load and source. Considering efficiency of power transfer and power quality, reactive power is undesirable, as increasing it increases the current drawn for a load, increasing losses due to heat. This would also increase the cost of system operation and the frequency of maintenance. To mitigate the detrimental effects of reactive power in SG, researchers have developed a variety of methods for real-time optimization.

Muthukumaran and Kalyani (2021) apply reactive power optimization in SG by means of evolutionary algorithm for demand side management control. The proposed method improves voltage profile and minimizes power loss, compared to other meta-heuristic algorithms like particle swarm optimization (PSO). Chandrasekaran et al. alternatively apply artificial neural networks for renewable energy based SGs for managing reactive power balance, resulting in the same benefits (Chandrasekaran et al., 2021). Additionally, Abdelhady et al. apply real-time reactive power correction using a genetic algorithm (Abdelhady et al., 2020), and Alenius et al. (2020) propose an active reactive power compensation using an adaptive control method and inductance estimation.

6.5.5. Devices

Various devices and control systems can be implemented into the grid to help mitigate the power quality challenges. In order to minimize potential challenges, efficient power converter design, which considers the physical and dynamic properties of individual energy sources, is essential. Inverters are designed for the purpose of integrating distributed generation into the grid, while maintaining power quality standards (Khadem et al., 2010). If they are, however, not applied correctly, additional harmonics could be introduced through high frequency switching of the inverters. By designing electronics to feature control systems, power quality can be improved while mitigating voltage fluctuations and harmonic distortion (Khadem et al., 2010). Custom devices such as series active power filters, shunt active power filters, and a hybrid of the two are some of the latest developments, overcoming both voltage and current disturbances by absorbing the load or by compensating the harmonic and reactive power generated (Liserre et al., 2010; Linh, 2009; El-Tamaly et al., 2007; Khadem et al., 2010).

6.5.6. Synchronization

The synchronization of grid phase, frequency, and voltage is a popular area of research towards power quality control. One of the most common methods is based on phase-locked loop, a control method where input and output signals have related phases (Shafiullah et al., 2010). Other techniques for synchronization, described in Liserre et al. (2010), include using multiple filters paired with a nonlinear transformation or detecting the zero crossing of the grid. However, these methods are not as popular or well performing as phase-locked loop control, where filtering introduces feedback delays and zero crossing methods could be incorrectly triggered under the presence of noise (Liserre et al., 2010).

There are multiple proposed solutions to help improve power quality in the Gandoman et al. (2018) reviews the use of Flexible AC Transmission Systems (FACTSs) to improve multiple aspects, including power quality, of the SG. They examined that distributed FACTSs help to improve not only power quality, but also energy utilization, power factor, and ensuring energy efficiency. Ceaki et al. (2017) examines the issues of harmonic disturbances caused by solar power and electric vehicles on the grid and proposes a solution of connecting a passive filter in each of the two systems. They concluded that the harmonic spectrum decreased, and the voltage waveforms improved after including the passive filter.

6.6. Demand management

Provided the intrinsic irregular nature of renewable energy sources, maintaining an appropriate power supply requires a load demand management system (Shafiullah et al., 2010). This increases the overall efficiency and quality of the system, and can be achieved by scheduling, shifting, and/or reducing demand Ming et al. (2010), Shafiullah et al. (2010). In reducing demand, peak demand can be reduced, resulting in a smoother demand profile, as well as reduced costs and improved reliability.

Many of the methods of improving demand management focus on forecasting demand and incentivizing consumers to use during off-peak times. Gope and Sikdar (2019) proposes a scheme for forecasting power demand in SGs based on masking-based spatial data aggregation. The authors concluded that their scheme can ensure improved computational efficiency and privacy protection in comparison to existing solutions. Making use of deep Q-learning, Razzak et al. also develop a prediction model for consumer electricity prices and demand, outperforming current models through iterative and data-based learning (Razzak et al., 2024). Further load forecasting machine learning methods are also presented in Liu et al. (2024), Kumar et al. (2024). Kishore and Snyder (2010) proposed an optimization model for determining the amount of time an appliance is used for to take advantage of the lower rates occurring on off-peak periods. An enhanced energy

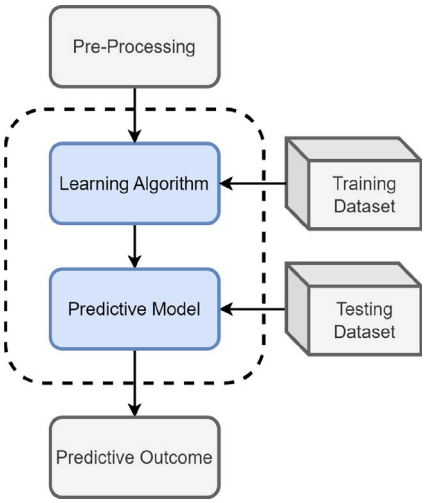

Fig. 6. Forecasting model training diagram (Bani Ahmad et al., 2023).

management controller (EMC) optimization model that accounts for the capacity constraints of potential electricity was also introduced. Bani Ahmad et al. proposed an alternative demand management optimization system based on machine learning, able to maintain efficiency in energy consumption and resiliency against malicious agents (Bani Ahmad et al., 2023). The forecasting models based on data generally are formulated using the training diagram presented below in Fig. 6.

6.7. Energy storage

Storage systems are designed to deliver short-term power which is used for frequency and voltage support, renewable generation variability, and power quality correction (Benzi et al., 2011). Energy storage systems are a fundamental part of incorporating renewable energy resources into SGs. The variability of such resources can be reduced since these systems store excess energy during off-peak periods and supply it during peak hours (Alotaibi et al., 2020).

Even though there are a large number of technologies available for storing energy in SGs, many are neither economical or efficient. Efficient storage technologies are necessary for the reliability of electric power systems, where researchers analyze the utility of energy storage with respect to peak shaving, frequency stability, voltage support, transmission upgrade deferral, and renewable firming (Salkuti, 2020). Other issues currently faced in this research include degradation, sizing and allocation, and feasibility (Tan et al., 2021). In their typically distributed installation, storage systems can additionally feature energy losses due to uncoordinated control and state of charge (SoC) imbalance. Real-time control strategies have been implemented to counteract this effect. Degradation in some storage systems (i.e., batteries) are also an issue, which have increasing losses overtime. Material research and control strategies are being investigated to mitigate degradation. The financial feasibility of energy storage systems is an emerging issue, where the attractive portions of SG implementation (e.g., environmental impact, energy savings by consumers and distributors) are not necessarily met if the storage systems are expensive to produce/maintain or use harmful/rare materials. There are also challenges faced in considering specific storage systems. For instance, thermochemical systems typically lack in effectiveness, where storage and mitigating heat losses are the result of scrupulous process monitoring and material selection (Tan et al., 2021).

Energy storage systems provide a method of delivering and storing energy to for when renewable energy sources are not able to be generated and ensuring a balance between supply and demand Hegazy (2012). They are also important in avoiding the wasting of the generated renewable energy (Worighi et al., 2019). Storage systems are able to supply power until a low SoC is reached, where the primary energy source then activates to charge the storage system (Hegazy, 2012). There are a variety of storage technologies which need to be chosen accordingly for particular applications, as examined in Department of Energy (2016).

Considering the perspective of REI, the main consideration is determining when energy should be co-located at generation sites or distributed across the grid (Bitar et al., 2011). Co-located storage devices allow for the possibility of real-time control, reducing the variability of the renewable energy output. It is therefore necessary to determine the minimum storage size that is needed to attain a certain extent of probability for satisfying the desired output power profile (Bitar et al., 2011).

Tan et al. (2021) extensively examines and reviews various energy storage technologies and their applications with REI, including electrochemical, mechanical, thermal, and electromagnetic systems. They examine the advantages, disadvantages, and applications of energy storage technologies, commenting on the future research and goals of the most promising considering renewable sources. Pang et al. (2012) discusses the advantages of using plug-in hybrid or battery-based electric vehicles as a means of energy storage for outage and demand side management. The energy storage method is dynamically configurable and dispersed, operating as a vehicle-to-building system (Pang et al., 2012).

6.7.1. Flywheel based energy storage systems

Stored as kinetic energy, flywheel technology efficiency is approximately 99% effective and ideal for large-scale regulation purposes, with standby losses ranging from only 0.2 to 2% (Dileep, 2020; Arghandeh et al., 2012). It has a rapid dynamic response, long life expectancy, and relatively high characteristics of self-discharge rate, energy density, power, cycling rate, and energy conversion efficiency (Salkuti, 2020). For short periods of time, the flywheel can administer peak power and fast responses used for balancing grid voltage sag correction and frequency oscillations (Samineni et al., 2006). Additionally, during grid disturbances, they provide highly reliable ride through for critical loads (Arghandeh et al., 2012). Some limitations remain however, where since they can only have these benefits on loads for short periods of time, they must be used in conjunction with other storage devices (Arghandeh et al., 2012). Additionally, they are difficult to install, and operation standards are limited (Arghandeh et al., 2012). Arghandeh et al. simulate flywheel storage methods for a facility microgrid, demonstrating the aforementioned benefits (Arghandeh et al., 2012).

6.7.2. Hydrogen based energy storage systems

In this system, the electricity is generated through reverse electrochemical reactions within fuel cells (Salkuti, 2020). Though having a low efficiency (around 50%), these types of storage systems have adequate dynamic response, can be used for long periods of time, and have no emissions since their only by-product is water (Salkuti, 2020). Research conducted by Chamandoust et al. are one such example of hydrogen storage implementation, proposing an optimization model with multiple objectives for SGs (Chamandoust et al., 2021). Using four case studies, results demonstrate the storage system's effectiveness in terms of operation cost and reliability, but energy consumption deviates from the desired value due to the charging mode (Chamandoust et al., 2021).

6.7.3. Thermal and electrical energy storage systems

Thermal energy is converted from electrical energy using their generation systems that generally consist of the storage heat exchanger, heating and cooling setups, and an air handling unit (Salkuti, 2020), but are generally categorized in terms of sensible, latent, and thermochemical storages (Enescu et al., 2020). The charging that is required for this type of system can be done centrally or locally, with load shifting also available (Abujubbeh et al., 2019). These systems typically feature frequency regulation, rapid response rate, high efficiency (close to 100%), and large storage capacities. Methods and case studies in this storage type are explored in Enescu et al. (2020).

Not widely adopted, magnetic coils, ultracapacitors, and super conductors are costly alternatives (Avancini et al., 2019). Considering electrical systems, ultracapacitors can be used to improve their reliability and performance, resulting in high power densities, and discharging/charging capacities (Panda and Das, 2021). They also provide additional power to the fuel cell plant during transient or peak periods (Uzunoglu and Alam, 2006). However, they cannot alone store significant amounts of energy (Uzunoglu and Alam, 2006), which is why they are typically used in hybrid structures, demonstrated in the following subsection. Shi and Crow (2008) outline mathematical, electric circuit, and non-electric circuit models, and compare their forms for equivalency.

6.7.4. Hybrids

Recently, researchers have begun proposing hybrid approaches, using multiple energy storage technologies together. A hybrid ultracapacitor and battery storage system was proposed by Kim et al. (2017b) in order to provide large scale regulation services. These services are vital in maintaining grid stability, correcting for discrepancies between power supply and demand Kim et al. (2017b). Their method intends to lessen the use of batteries while increasing the profitability of regulation services (Kim et al., 2017b). A model and optimization framework for this system was derived, concluding that their system could result in profit improvements at an order range of 1.16–5.44 (Kim et al., 2017b).

Akram and Khalid (2018) proposed a coordinated control scheme for operating hybrid systems composed of both batteries and ultracapacitors. This approach was proposed since replacing conventional generators with renewable energy generation sources could jeopardize grid stability (Akram and Khalid, 2018). Considering investment, operation/maintenance, and replacement costs, the authors concluded that their framework for the hybrid system ensures expected regulation of frequencies without information losses, again resulting in increased processes to regulation service providers (Akram and Khalid, 2018).

6.8. Energy efficiency

Minimizing energy losses in SG is an exceptionally important objective. Efficient power systems optimize transmission and distribution systems, and effectively manage consumption. Table 6, seen below, summarizes the papers examined in this section.

Aquino-Lugo and Overbye (2010) implemented decentralized control algorithms with agent-based technologies, aiming to minimize power losses across distribution grids. They presented two case studies for their optimal power flow (OPF) algorithm, analyzing their performance for distributed systems (Aquino-Lugo and Overbye, 2010). Their work concluded the validity of this control approach, but only with the presence of intelligent communication methods (Aquino-Lugo and Overbye, 2010).

Research from Ochoa and Harrison (2011) used a multi-period alternative current OPF for determining the optimal accommodation of renewable distributed generation (DG). Their method was aimed at minimizing energy losses, also investigating trade-offs between more generation capacity and energy losses. Their method was validated in terms of optimality and loss reduction, citing simple implementation in the majority of existing distribution networks (Ochoa and Harrison, 2011).

Atwa et al. (2010) proposed a method for allocating different categories of renewable DG units optimally, minimizing the annual energy loss. This was applied to a common rural distribution system, including constraints applied to the maximum penetration limit, the feeders' capacity, voltage limits, and the discrete size of the available DG units (Atwa et al., 2010). The authors concluded that for all scenarios and renewable resource combinations studied, annual energy losses saw significant reductions without violating constraints (Atwa et al., 2010).

7. Industry applications

At various levels of industry, there have been numerous successful applications of SG across the globe. In this section, we examine how SG has been implemented by academic institutions and large companies, where small-scale prototypes or large-scale projects are constructed. These applications have utilized the majority of topics we have outlined in this survey, demonstrating the benefits of SG at the physical level, at varying scales. Efforts such as these are crucial to maintaining SG research endeavors where their increased efficiency and renewable energy integration can be psychically quantified. As such, SG projects are valuable to all levels of industry, enabling novel research. Projects led by larger companies are however more advantageous for communities since they are implemented at city-wide scales, where typically university led projects benefit the researchers and the institution. Without physical SG projects, research would not progress and traditional power grids will remain stagnant against growing energy demands and increased emissions. The impressive accomplishments of these projects will be examined.

7.1. University/small scale implementation

7.1.1. Research/academic papers

Many universities across the world have laboratories dedicated to researching SG, including Canadian Universities such as York University (York University Department of Electrical Engineering and Computer Science, 2024), Toronto Metropolitan University (Toronto Metropolitan University Centre for Urban Energy, 2024), and University of Waterloo (High Voltage Engineering Laboratory (HVEL), 2024), and the University of Melbourne in Australia (University of Melourne Department of Electrical and Electronic Engineering, 2024). These laboratories have conducted a significant amount of research and published numerous academic journals and surveys on various aspects of SG. As the demand for a more sustainable method of delivering energy increases, more research is dedicated to SG.

7.1.2. Prototypes

Alongside research and academic papers, prototypes of various aspects of SG, such as demand side management (Supriya et al., 2011) or remote monitoring (Natarajan and Bhagavath Singh, 2017), have been created to design and test components of the SG. Small scale grids are ideal for analysis and the testing of new technologies, where their results are scalable and their effects on city-wide scales can be extrapolated. More recently, larger scale, more complete prototypes have been created by a select number of universities and companies.

A significant milestone in SG prototyping is the award-winning Microgrid Energy Management System (MG-EMS) prototype. Located at the Laboratory for Clean Energy Research (LaCER), School of Electrical and Electric Engineering at Nanyang Technological University in Singapore, this prototype uses software applications for managing sensed data and performing generation and load management routines (Cheah, 2024). By using NI LabVIEW software, CompactRIO hardware featuring FPGA technology, and NI DAQ hardware, they extend the microgrid to a SG prototype (Cheah, 2024). A maximum power point tracking (MPPT) module of the PV system was created with this method, as

Table 6
Summary of REI challenges solution papers.

Year	Reference	Challenge Type	Method
2020	Hewage et al. (2021)	Accurate Weather Forecasting	A deep learning-based effective fine-grained weather forecasting model which utilized multiple layers that used surface weather parameters over a period of time.
2010	Liserre et al. (2010)	Synchronization	Zero crossing detection of the grid or using multiple filters paired with a nonlinear transformation
2018	Gandoman et al. (2018)	Power Quality	Flexible AC Transmission Systems (FACTSs)
2017	Ceaki et al. (2017)	Harmonic disturbances caused by solar and electric vehicles	Connecting a passive filter in solar systems and electric vehicle systems.
2019	Gope and Sikdar (2019)	Forecasting Power Demands	Private and lightweight masking-based spatial data aggregation scheme.
2010	Kishore and Snyder (2010)	Demand Management	Optimization model for determining the time of use of appliances and introduces an improved powerful energy management controller (EMC) optimization model that accounts for electric potential capacity constraints.
2021	Tan et al. (2021)	Energy Storage	Examines and reviews various energy storage technologies and their applications with renewable energy integration.
2012	Pang et al. (2012)	Energy Storage	Using plug-in hybrid and battery-based electric vehicles for storing energy, and strategy for adopting these uses in vehicle-to-building mode.
2017	Kim et al. (2017b)	Energy Storage	Hybrid ultracapacitor and battery storage system in order to provide large scale regulation.
2018	Akram and Khalid (2018)	Energy Storage	Coordinated control scheme to operate a hybrid system composed of both batteries and ultracapacitors.
2010	Aquino-Lugo and Overbye (2010)	Energy Efficiency	Agent based technologies for decentralized control algorithm implementations, minimizing power losses in the distribution grids.
2010	Atwa et al. (2010)	Energy Efficiency	Method applied to a common rural distribution system for allocating different types of renewable DG units optimally.
2011	Ochoa and Harrison (2011)	Energy Efficiency	Multi-period alternative current optimal power flow for determining the optimal accommodation of renewable distributed generation. Minimized energy losses and investigated trade-offs between those losses and increasing generation capacity.

well as a control scheme of the BESS to integrate energy management systems for buildings (HEMS, BEMS), solar PV technology, and energy storage with the existing microgrid prototype (Cheah, 2024).

Green Empowerment's SGs for Small Grids project aims to bring intelligent, open-source technology to engineers and technicians in remote communities. They work with regional partners to build renewable energy micro-grids with remote indigenous communities in South Asia (Green Empowerment, 2024). Green Empowerment also develops and builds prototypes for lab testing with real-world appliances, combines with simulated challenges. They work closely with their partners to assess financial sustainability. In 2022 and 2023, they had the opportunity to test their prototype appliance controllers and monitoring devices in Malaysia and the Philippines (Green Empowerment, 2024).

7.2. Country/continent implementations

Many countries around the world have also begun working on the SG, whether working on pilot projects or taking initiatives for testing and research. Governments of countries such as the United States, Australia, Britain, China, Japan, and South Korea have also considered SGs as a method of reducing carbon emissions and energy security (Majeed Butt et al., 2021).

NIST is also devoting research and attention to the cooperation of multiple countries for the development of international standards for the SG (Wang and Lu, 2013). Canada, Mexico, Brazil, Japan, South Korea, Australia, India, China are among the countries that have already or plan on investigating the substantial SG infrastructure (NIST, 2018), setting a baseline of energy standards that other countries will soon follow in. The countries and continents examined in the following section can be seen highlighted blue below in Fig. 7.

7.2.1. Australia

After a SG proposal in 2009, the Australian government was interested in investing $100 million. They were also interested in raising customer awareness of energy utilization and establishing generation management and distributed demand systems (Majeed Butt et al., 2021). In New South Wales, five sites were chosen for SG establishments and Energy Australia working with IBM, GE Energy, and Grid Net, were selected to work on the project. The idea was to build a Worldwide Interoperability for Microwave Access (WIMAX)-based SG that had capabilities of automatic substations, able to support up to 50,000 smart meter connections and to accommodate electric vehicles (Majeed Butt et al., 2021).

Most recently in 2021, the Australian Energy Security Board proposed an energy market redesign for 2025 (Energy Security Board, 2023). Built around the use of the SG and renewable energy sources, they suggested an assortment of reforms necessary for the transition to become the most decentralized power system in the world (Energy Security Board, 2023). With reforms established and enforced,

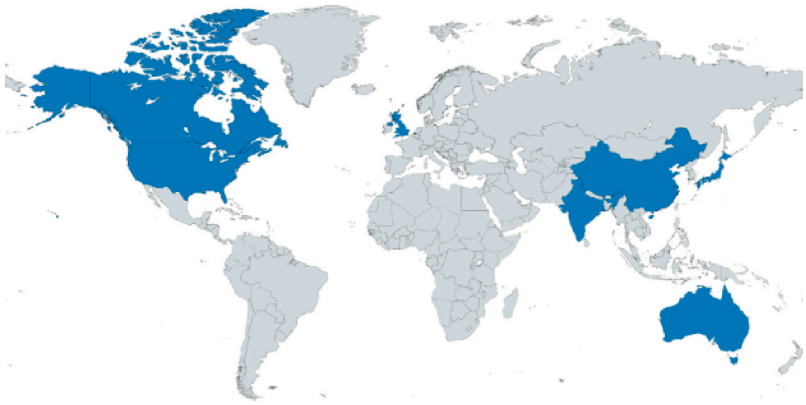

Fig. 7. Regions examined in Section 7.2.

the benefits will be targeted towards consumers, enabling flexibility, reliability, and affordability in Australia's power grid (Energy Security Board, 2023).

7.2.2. India

The Indian government has initiated nationwide SG projects, with the primary goal of identifying and discussing the deployment barriers and concerns, such as customer acceptance. Customers proved willing to adopt SG and a mini SG project was implemented by the Puducherry Electricity Department in Puducherry (National Smart Grid Mission, 2024). This project had proposed an area covering 34,000 consumers from a wide variety of monthly incomes and electricity usage, enabling each with advanced metering technologies (National Smart Grid Mission, 2024). Many projects have been proposed and implemented across India, in cities such as Ajmer, Tripura, Haryana, and Manesar (National Smart Grid Mission, 2024). There are currently 12 total SG pilot projects in power distribution sectors listed, which include the adoption of various functionalities, such as advanced metering technologies, load management, substation automation including SCADA, distribution transformer monitoring, distributed generation, outage management, power quality measuring, micro grid, electric vehicle charging infrastructure, home energy management center, and cybersecurity and training infrastructure (National Smart Grid Mission, 2024).

7.2.3. United Kingdom

The UK has actively been decreasing greenhouse gas and carbon dioxide emissions since 1990 (Cameron, 2022). Currently, the UK is in the process of adopting the SG on a country-wide scale, with a phased approach led by industry regulator Ofgem and the Department of Energy and Climate Change (DECC) (Cameron, 2022). In 2021 alone, 8 million smart meters were installed and connected to the Data Communications Company (DCC), who state their total 17 million units at the time help in reducing 500,000 tonnes of carbon dioxide per year (Cameron, 2022). Their goal is to implement 53 million smart meters by 2025 and as of 2022, they published a report proposing reforms for the energy market, digitizing the energy system and adopting novel smart technology (Cameron, 2022). Ofgem's proposed reforms aim to provide consumers increased energy consumption authority, as well as promoting net-zero green house gas emissions.

7.2.4. China

In September 2020, the Chinese government announced an objective of peak carbon dioxide emissions by 2030 and carbon neutrality by 2060 (Globe Newswire, 2022). Since then, they have been trying to build and improve their energy system (Globe Newswire, 2022). China is expected to lead in terms of advanced metering infrastructure deployment, as they have begun replacing their first generation of smart meters with more advanced systems (Nhede, 2021).

7.2.5. Canada

There are SG programs happening in several provinces and territories throughout Canada. The SG program, one of Natural Resource Canada's programs, funds $100M over four years (2019 to 2023) to progress the demonstration of SG technologies and the deployment of SG integrated systems (Government of Canada, 2023). During the four-year program, recipients reported on the initial deployment of the grid and its influence during their project up to 5 years following their project investment (Government of Canada, 2023). The information reported will be used by Natural Resource Canada to analyze grid impacts and program future lessons to inform of future programs and policy development. Currently, the SG program has funded 21 projects across Canada working on development projects, deployment projects, or hybrid projects, as seen in Fig. 8 (Government of Canada, 2023) below.

Additionally, Canada's Energy Innovation Program and Smart Grid Demonstration provides funding to projects that demonstrate innovations in smart grid solutions or technologies (Government of Canada, 2024). Having just closed its call for proposals this year, the project promotes accelerating grid modernization, improving customer accessibility, addressing market gaps, and advancing diversity, inclusively, equity, and accessibility in this field (Government of Canada, 2024)

7.2.6. United States

The US DOE was provided with $4.5B from the Recovery Act for the modernization of the power grid (U.S. Department of Energy, 2024b; U.S. Department of Energy, 2024). The two largest initiatives are the SG Demonstration Program (SGDP) (U.S. Department of Energy, 2024a) and the SG Investment Grant (SGIG) (U.S. Department of Energy, 2024b; U.S. Department of Energy, 2024). The SGDP works on advanced SG and energy storage systems and evaluates performance for future applications. Overall consisting of 32 projects, 16 of those are dedicated to regional demonstrations to prove validity, quantify costs, and test scalable business models (U.S. Department of Energy, 2024a). The other 16 projects is for the energy storage system development, such as the ones discussed in the previous section. The SGIG focuses on the accelerating the deployment of existing SG techniques, tools, and technologies for improving modern grid performance, comprising approximately $8B from the Act. The program involves 99 projects, consisting of power supply companies, who upgrade their systems to test distribution and transmission systems (U.S. Department of Energy, 2024b). There are also other SG programs such as ones for work training, interoperability and cybersecurity, and renewable and distributed systems (U.S. Department of Energy, 2024).

7.2.7. Japan

In 2015, the Japanese government identified six portions vital to accelerating the development and deployment of SG in the country.

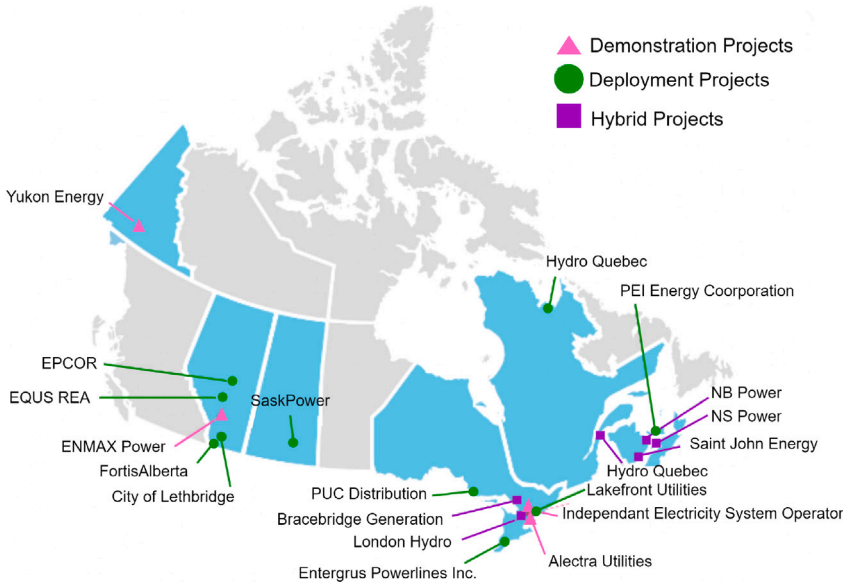

Fig. 8. SG projects throughout Canada.

These key portions included smart meters as the most vital, along with, communications technologies, solar PV, battery energy storage systems, energy management systems, and the deregulation of the electricity market (Nhede, 2021). The countries efforts towards SG were accelerated amid hosting the 2020 Olympic games as they aimed to ensure a secure energy supply. COVID-19 disruptions delayed the countries' SG plans, and so their efforts are projected to continue through 2030 (Nhede, 2021). A book from Ida et al. outlines the current economics of SGs in Japan, its developments, and the results of four field experiments conducted in different regions (Ida et al., 2024). The field experiments, performed in Kitakyushu city, Keihanna Science City, Toyota city, and Yokohama city, were designed to be "randomized control trials" on real power grids in residential areas (Ida et al., 2024). The validity of the experiments is upheld by this random aspect, as well as findings regarding behavioral economics and the use of large data sets (Ida et al., 2024).

7.3. Observed constraints

Cost is one of the foremost constraints challenging the further development and implementation of the SG (Young, 2017). There is a significant cost associated with the distribution and transmission systems, as well as the additional technologies and equipment, such as smart meters. This will be an especially challenging constraint for developing countries looking to implement the SG. A study done in 2017 by Young explored SG potential in these countries, calculating the expected cost of SG and the ratio of the nation's GDP to the cost of development. They compared factors of available resources, proximity to urban centers, the accessibility of education and training, political stability, and development cost with Kepner–Tregoe analyses (Young, 2017). This study showed a large distribution of ratios, with the lowest being 2 and the highest being 47, demonstrating the financial challenges of implementing SG and the determination of five developing nations most compatible for investment in SGs (Young, 2017).

8. Conclusions

In this work, we provide a comprehensive overview of SG technology, highlighting the current state of SG implementation through an examination of research conducted by a variety of industrial, governmental, and academic institutions. Emerging programs and standards are also considered, which contribute to the modern effort in global SG adoption. A new way of efficiently transmitting power, the SG offers enhanced resiliency, flexibility, and reliability in power systems, adapting self-healing grid infrastructure, improving power management, and better utilization of existing electricity assets. The SG is considerably more environmentally friendly than its alternative standardized power grid, providing a new solution to enable increased penetration of renewable energy generation, and reduce greenhouse gas emissions. Distributors and customers also benefit from this technology economically, where SG integration implies an increase in available energy sector employment and lower energy costs due to efficiency. From the surveyed literature, it was evident that the challenges faced in SG are numerous, requiring innovative solutions to reinforce its large-scale viability. Here, we specifically focus on what were determined to be the most critical issues, which are the challenges presented by cybersecurity, interoperability, and REI. These topics are examined thoroughly in this survey, where their associated difficulties and proposed solutions found in literature are discussed, serving as a reference to researchers in the field.

The first issue facing SG that we study is cybersecurity. Due to the close interaction of power distribution, consumption, generation, and transmission in these systems, there is a high degree of communication and therefore increased vulnerabilities to cyberattacks. Supervising massive amounts of data and energy, SG exposed to cyberattacks can have numerous consequences, including outages, infrastructure failures, compromised privacy, and dangers to human safety. In investigating cybersecurity, the benefit lies in attack mitigation to maintain essential functions. More sophisticated cyberattacks are being developed however, where one of them is the FDI class of attacks examined. One of the most prominent challenges in cybersecurity, more research, testing, and simulations should be conducted to ensure the proposed defense strategies provide high detection accuracy and resilience when integrated into SG. In research, the successes of data driven and deep learning methods for attack identification/rectification suggest that cybersecurity solutions involving such should be continued to be pursued.

Interoperability in SGs was considered next, referring to the ability to exchange and make use of information. A main feature of SG, it consists of the capacity of network technologies, sensors, and electrical devices to use interchanged information effectively. Interoperability between all systems is required for effective grid operation in this sense, ultimately resulting in improved reliability and operation protection through rapid dynamic and automatic communication.

Researching methods in improving interoperability for SG results in grid transmission efficiency and stability, benefiting the environment and transactional entities. Developing interoperability protocols and maintaining their universal adherence is a challenge itself, especially when considering SG on a national or international scale. Scalability is a topic relating to interoperability that must be studied further. Additionally, it is vital to develop improved interoperability testing, where these tests are required to ensure that components are capable of interoperability.

The third issue, renewable energy integration (REI), is of growing importance for SG, as the demand for more renewable and sustainable energy generation methods increases. SG allows for safe integration of renewable energy resources into the grid and supplementing the power supply with the power generated and stored by a consumer, reducing dependencies on fossil fuels. Integrating these resources into the SG will be necessary to meet the energy demand and environmental challenges of the 21st century, offering benefits in reduced cost and environmental impact. Utilizing these sources is challenging however, where its generation is incredibly variable, and the quantity of power generated is greatly impacted by the weather forecast. The physical implementation into SG is challenging as well, where considerations required include grid geography, generator design, and power movement type. Developing methods of controlling REI complications and investigating energy storage methods are crucial future research concerns. Energy storage is necessary to ensure load demand is met at all times, especially given the periodic and stochastic nature of renewable energy sources. New and innovative methods of storage, especially the emerging V2G (vehicle-to-grid) and V2X (vehicle-to-everything) methods should be further explored, considering the growth of electric vehicles.

An abundance of research has been dedicated to the development of SGs, either directly or indirectly. For instance, in the fields of renewable resources and cybersecurity, more powerful and accurate methods of generation and protection are constantly being developed, applicable to many other applications outside the scope of SG. As new technologies are developed, the problem of unifying them with the power grid or maximizing functionality will always exist. The cost of the prospective infrastructure reconfiguration is another one of the foremost constraints challenging the further development and implementation of the SG, making its adoption restrictive in developing countries.

Though existing portions of the SGs are well research and developed, the application of new research or modern problems must be considered under the same scope. Provided the current state of climate change and the digital age, areas that are likely to be explored more in the future include cybersecurity, improving accuracy of forecasting, micro-grid integration, and energy and demand management systems. Considering current research in these areas and anomaly mitigation and detection, it can be reasonably suggested that the utilization of deep learning/large data sets will play a pivotal role in overcoming the challenges of the future.

CRediT authorship contribution statement

Jadyn Powell: Writing – original draft, Visualization, Investigation, Formal analysis. **Alex McCafferty-Leroux:** Writing – review & editing, Visualization, Validation. **Waleed Hilal:** Writing – review & editing, Supervision. **S. Andrew Gadsden:** Writing – review & editing, Supervision, Project administration, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

This work was supported by the Natural Sciences and Engineering Research Council of Canada Discovery Grant (Gadsden).

References

Abdelhady, S., Osama, A., Shaban, A., Elbayoumi, M., 2020. A real-time optimization of reactive power for an intelligent system using genetic algorithm. IEEE Access 8, 11991–12000. http://dx.doi.org/10.1109/ACCESS.2020.2965321.

Abdelwahab, A., Lucia, W., Youssef, A., 2020. Set-theoretic control for active detection of replay attacks with applications to smart grid. In: 2020 IEEE Conference on Control Technology and Applications. CCTA, pp. 1004–1009. http://dx.doi.org/10.1109/CCTA41146.2020.9206373.

Abujubbeh, M., Al-Turjman, F., Fahrioglu, M., 2019. Software-defined wireless sensor networks in smart grids: An overview. Sustainable Cities Soc. 51, 101754. http://dx.doi.org/10.1016/j.scs.2019.101754.

Akhtar, F., Rehmani, M.H., 2015. Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review. Renew. Sustain. Energy Rev. 45, 769–784. http://dx.doi.org/10.1016/j.rser.2015.02.021.

Akram, U., Khalid, M., 2018. A coordinated frequency regulation framework based on hybrid battery-ultracapacitor energy storage technologies. IEEE Access 6, 7310–7320. http://dx.doi.org/10.1109/ACCESS.2017.2786283.

Alaerjan, A.S., 2021. Model-driven interoperability layer for normalized connectivity across smart grid domains. IEEE Access 9, 98639–98653. http://dx.doi.org/10.1109/ACCESS.2021.3096043.

Alaerjan, A., Kim, D.-K., Ming, H., Malik, K., 2018. Using DDS based on unified data model to improve interoperability of smart grids. In: 2018 IEEE International Conference on Smart Energy Grid Engineering. SEGE, pp. 110–114. http://dx.doi.org/10.1109/SEGE.2018.8499513.

Alenius, H., Luhtala, R., Messo, T., Roinila, T., 2020. Autonomous reactive power support for smart photovoltaic inverter based on real-time grid-impedance measurements of a weak grid. Electr. Power Syst. Res. 182, 106207. http://dx.doi.org/10.1016/j.epsr.2020.106207.

Alotaibi, I., Abido, M.A., Khalid, M., Savkin, A.V., 2020. A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. Energies 13 (23), http://dx.doi.org/10.3390/en13236269.

Aloul, F., Al-Ali, A., Al-Dalky, R., Al-Mardini, M., El-Hajj, W., 2012. Smart grid security: Threats, vulnerabilities and solutions. Int. J. Smart Grid Clean Energy 1 (1), 1–6.

Aquino-Lugo, A.A., Overbye, T., 2010. Agent technologies for control applications in the power grid. In: 2010 43rd Hawaii International Conference on System Sciences. pp. 1–10. http://dx.doi.org/10.1109/HICSS.2010.43.

Ardagna, C.A., Bellandi, V., Damiani, E., Bezzi, M., Hebert, C., 2021. Big data analytics-as-a-service: Bridging the gap between security experts and data scientists. Comput. Electr. Eng. 93, 107215. http://dx.doi.org/10.1016/j.compeleceng.2021.107215.

Arduini, F., Lanzrath, M., Ghosalkar, S., Nateghi, A., Fisahn, S., Schaarschmidt, M., 2023. Vulnerability of smart grid-enabled protection relays to IEMI. Adv. Radio Sci. 20, 131–139. http://dx.doi.org/10.5194/ars-20-131-2023.

Arghandeh, R., Pipattanasomporn, M., Rahman, S., 2012. Flywheel energy storage systems for ride-through applications in a facility microgrid. IEEE Trans. Smart Grid 3 (4), 1955–1962. http://dx.doi.org/10.1109/TSG.2012.2212468.

Atwa, Y.M., El-Saadany, E.F., Salama, M.M.A., Seethapathy, R., 2010. Optimal renewable resources mix for distribution system energy loss minimization. IEEE Trans. Power Syst. 25 (1), 360–370. http://dx.doi.org/10.1109/TPWRS.2009.2030276.

Avancini, D.B., Rodrigues, J.J., Martins, S.G., Rabêlo, R.A., Al-Muhtadi, J., Solic, P., 2019. Energy meters evolution in smart grids: A review. J. Clean. Prod. 217, 702–715. http://dx.doi.org/10.1016/j.jclepro.2019.01.229.

Ayadi, F., Colak, I., Bayindir, R., 2019. Interoperability in smart grid. In: 2019 7th International Conference on Smart Grid. IcSmartGrid, pp. 165–169. http://dx.doi.org/10.1109/icSmartGrid48354.2019.8990680.

Ayadi, F., Colak, I., Garip, I., Bulbul, H.I., 2020. Impacts of renewable energy resources in smart grid. In: 2020 8th International Conference on Smart Grid. IcSmartGrid, pp. 183–188. http://dx.doi.org/10.1109/icSmartGrid49881.2020.9144695.

Badar, H.M.S., Mahmood, K., Akram, W., Ghaffar, Z., Umar, M., Das, A.K., 2023. Secure authentication protocol for home area network in smart grid-based smart cities. Comput. Electr. Eng. 108, 108721. http://dx.doi.org/10.1016/j.compeleceng.2023.108721.

Baig, Z.A., Amoudi, A.-R., 2013. An analysis of smart grid attacks and countermeasures. J. Commun. 8 (8), 473–479. http://dx.doi.org/10.12720/jcm.8.8.473-479.

Bani Ahmad, A.Y.A., William, P., Uike, D., Murgai, A., Bajaj, K.K., Deepak, A., Shrivastava, A., 2023. Framework for sustainable energy management using smart grid panels integrated with machine learning and IOT based approach.. Int. J. Intell. Syst. Appl. Eng. 12 (2s), 581–590.

Bansal, G., Dua, A., Aujla, G.S., Singh, M., Kumar, N., 2019. SmartChain: A smart and scalable blockchain consortium for smart grid systems. In: 2019 IEEE International Conference on Communications Workshops. ICC Workshops, pp. 1–6. http://dx.doi.org/10.1109/ICCW.2019.8757069.

Bari, A., Jiang, J., Saad, W., Jaekel, A., 2014. Challenges in the smart grid applications: An overview. Int. J. Distrib. Sens. Netw. 10 (2), 974682. http://dx.doi.org/10.1155/2014/974682.

Bedi, G., Venayagamoorthy, G.K., Singh, R., Brooks, R.R., Wang, K.-C., 2018. Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet Things J. 5 (2), 847–870. http://dx.doi.org/10.1109/JIOT.2018.2802704.

Benzi, F., Anglani, N., Bassi, E., Frosini, L., 2011. Electricity smart meters interfacing the households. IEEE Trans. Ind. Electron. 58 (10), 4487–4494. http://dx.doi.org/10.1109/TIE.2011.2107713.

Bergmann, H., Mosiman, C., Saha, A., Haile, S., Livingood, W., Bushby, S., Fierro, G., Bender, J., Poplawski, M., Granderson, J., Pritoni, M., 2020. Semantic interoperability to enable smart, grid-interactive efficient buildings. Summer Study Energy Effic. Build. http://dx.doi.org/10.20357/B7S304.

Berl, A., Niedermeier, M., Meer, H., 2013. Smart grid considerations: Energy efficiency vs. Security. In: Green and Sustainable Computing: Part II. In: Advances in Computers, vol. 88, Elsevier, pp. 159–198. http://dx.doi.org/10.1016/B978-0-12-407725-6.00004-6.

Bitar, E., Khargonekar, P., Poolla, K., 2011. Systems and control opportunities in the integration of renewable energy into the smart grid. IFAC Proc. Vol. 44 (1), 4927–4932. http://dx.doi.org/10.3182/20110828-6-IT-1002.01244.

Blumsack, S., Fernandez, A., 2012. Ready or not, here comes the smart grid! Energy 7th Bienn. Int. Workshop Adv. Energy Stud. 37 (1), 61–68. http://dx.doi.org/10.1016/j.energy.2011.07.054.

Bossanyi, E., Saad-Saoud, Z., Jenkins, N., 1998. Prediction of flicker produced by wind turbines. Wind Energy 1 (1), 35–51. http://dx.doi.org/10.1002/(SICI)1099-1824(199809)1:1<35::AID-WE11>3.0.CO;2-J.

Camacho, E.F., Samad, T., Garcia-Sanz, M., Hiskens, I., 2011. Control for renewable energy and smart grids. Impact Control Technol. Control Syst. Soc. 4 (8), 69–88.

Cameron, A., 2022. The UK smart grid: How it started & how it's going. Fortra Available from: https://www.tripwire.com/state-of-security/uk-smart-grid-how-it-started-how-its-going#:~:text=In%20their%20extensive%20document%2C%20the,system%20for%20transporting%20electricity%20from.

Caribbean Renewable EnergyDevelopment Programme (CREDP), 2004. Wind-grid integration brief. Sol. Water Heat. Mark..

Cartwright, P., 2006. Connecting renewables: The challenge of integrating large offshore wind farms. Refocus 7 (1), 24–26. http://dx.doi.org/10.1016/S1471-0846(06)70513-3.

Cavalieri, S., 2021. Semantic interoperability between IEC 61850 and oneM2M for IoT-enabled smart grids. Sensors 21 (7), http://dx.doi.org/10.3390/s21072571.

Ceaki, O., Seritan, G., Vatu, R., Mancasi, M., 2017. Analysis of power quality improvement in smart grids. In: 2017 10th International Symposium on Advanced Topics in Electrical Engineering. ATEE, pp. 797–801. http://dx.doi.org/10.1109/ATEE.2017.7905104.

Chamandoust, H., Hashemi, A., Bahramara, S., 2021. Energy management of a smart autonomous electrical grid with a hydrogen storage system. Int. J. Hydrog. Energy 46 (34), 17608–17626. http://dx.doi.org/10.1016/j.ijhydene.2021.02.174.

Chandrasekaran, K., Selvaraj, J., Amaladoss, C.R., Veerapan, L., 2021. Hybrid renewable energy based smart grid system for reactive power management and voltage profile enhancement using artificial neural network. Energy Sources Part A Recovery Util. Environ. Eff. 43 (19), 2419–2442. http://dx.doi.org/10.1080/15567036.2021.1902430.

Cheah, P., 2024. Developing a functional smart grid prototype using NI LabVIEW, NI CompactRIO, and NI DAQ. Available from: https://www.ni.com/en-ca/innovations/case-studies/19/developing-a-functional-smart-grid-prototype.html.

Chen, N., 2013. Passive Interoperability Testing for Communication Protocols (Ph.D. thesis). (2013REN1S046), Université de Rennes, URL https://theses.hal.science/tel-00869819.

Chen, J., Mohamed, M.A., Dampage, U., Rezaei, M., Salmen, S.H., Obaid, S.A., Annuk, A., 2021. A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. Appl. Sci. 11 (21), http://dx.doi.org/10.3390/app11219972.

Chetan Khadse, A.A.P., Chaudhari, B.S., 2021. Electromagnetic field and artificial intelligence based fault detection and classification system for the transmission lines in smart grid. Energy Sources Part A Recovery Util. Environ. Eff. 1–15. http://dx.doi.org/10.1080/15567036.2021.1948637.

Chim, T., Yiu, S., Hui, L.C., Li, V.O., 2011. PASS: Privacy-preserving authentication scheme for smart grid network. In: 2011 IEEE International Conference on Smart Grid Communications. SmartGridComm, pp. 196–201. http://dx.doi.org/10.1109/SmartGridComm.2011.6102316.

Choi, T.-I., Lee, K.Y., Lee, D.R., Ahn, J.K., 2008. Communication system for distribution automation using CDMA. IEEE Trans. Power Deliv. 23 (2), 650–656. http://dx.doi.org/10.1109/TPWRD.2007.910991.

Colak, A.M., Kayisli, K., 2021. Reducing voltage and frequency fluctuations in power systems using smart power electronics technologies: A review. In: 2021 9th International Conference on Smart Grid. IcSmartGrid, pp. 197–200. http://dx.doi.org/10.1109/icSmartGrid52357.2021.9551248.

Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., Covrig, C.-F., 2016. A survey on the critical issues in smart grid technologies. Renew. Sustain. Energy Rev. 54 (C), 396–405. http://dx.doi.org/10.1016/j.rser.2015.10.03.

Colson, C.M., et al., 2012. Towards Real-Time Power Management of Microgrids for Power System Integration: a Decentralized Multi-Agent Based Approach (Ph.D. thesis). Montana State University-Bozeman, College of Engineering.

Commission, I.E., et al., 2012. Grid Integration of Large-Capacity Renewable Energy Sources and Use of Large-Capacity Electrical Energy Storage. International Electrotechnical Commission.

Cunjiang, Y., Huaxun, Z., Lei, Z., 2012. Architecture design for smart grid. Energy Procedia 2012 Int. Conf. Future Electr. Power Energy Syst. 17, 1524–1528. http://dx.doi.org/10.1016/j.egypro.2012.02.276.

DeCesaro, J., Porter, K., Milligan, M., 2009. Wind energy and power system operations: A review of wind integration studies to date. Electr. J. 22 (10), 34–43. http://dx.doi.org/10.1016/j.tej.2009.10.010.

Delgado-Gomes, V., Martins, J.F., Lima, C., Borza, P.N., 2015. Smart grid security issues. In: 2015 9th International Conference on Compatibility and Power Electronics. CPE, pp. 534–538. http://dx.doi.org/10.1109/CPE.2015.7231132.

Demertzis, K., Tsiknas, K., Taketzis, D., Skoutas, D.N., Skianis, C., Iliadis, L., Zoiros, K.E., 2021. Communication network standards for smart grid infrastructures. Network 1 (2), 132–145. http://dx.doi.org/10.3390/network1020009.

Department of Energy, 2016. Distribution Automation: Results from the Smart Grid Investment Grant Program. Tech. rep., United States Department of Energy.

Department of Energy and Climate Change, 2009. The UK Renewable Energy Strategy. Tech. rep., The HM Government, United Kingdom.

di Bisceglie, M., Galdi, C., Vaccaro, A., Villacci, D., 2009. Cooperative sensor networks for voltage quality monitoring in smart grids. In: 2009 IEEE Bucharest PowerTech. pp. 1–6. http://dx.doi.org/10.1109/PTC.2009.5282012.

Dileep, G., 2020. A survey on smart grid technologies and applications. Renew. Energy 146, 2589–2625. http://dx.doi.org/10.1016/j.renene.2019.08.092.

Durand, J., 2012. Conformance interoperability and portability testing: Proposed procedures and practices.

El-hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A., 2019. A survey of Internet of Things (IoT) authentication schemes. Sensors 19 (5), http://dx.doi.org/10.3390/s19051141, URL https://www.mdpi.com/1424-8220/19/5/1141.

El-Tamaly, H.H., Wahab, M.A., Kasem, A.H., 2007. Simulation of directly grid-connected wind turbines for voltage fluctuation evaluation. Int. J. Appl. Eng. Res. 2 (1), 15–30.

Electricity Advisory Committee, 2008a. Smart Grid: Enabler of the New Energy Economy. Tech. rep., United States Department of Energy, Washington, D.C.

Electricity Advisory Committee, 2008b. Smart Grid: An Introduction. Tech. rep., United States Department of Energy, Washington, D.C.

Eltigani, D., Masri, S., 2015. Challenges of integrating renewable energy sources to smart grids: A review. Renew. Sustain. Energy Rev. 52, 770–780. http://dx.doi.org/10.1016/j.rser.2015.07.140.

Energy, G., et al., 2010. Western Wind and Solar Integration Study. Tech. rep., National Renewable Energy Laboratory.

Energy Great Lakes Regional Wind, 2010. Eastern Wind Integration and Transmission Study. Technical Report, National Renewable Energy Laboratory (NREL).

Energy Sector Control Systems Working Group, 2011. Roadmap to Achieve Energy Delivery Systems Cybersecurity. Tech. rep., United States Department of Energy, Washington, D.C.

Energy Security Board, 2023. Post 2025 electricity market design. Available from: https://esb-post2025-market-design.aemc.gov.au/.

Enescu, D., Chicco, G., Porumb, R., Seritan, G., 2020. Thermal energy storage for grid applications: Current status and emerging trends. Energies 13 (2), http://dx.doi.org/10.3390/en13020340.

Fadaeenejad, M., Saberian, A., Fadaee, M., Radzi, M., Hizam, H., AbKadir, M., 2014. The present and future of smart power grid in developing countries. Renew. Sustain. Energy Rev. 29, 828–834. http://dx.doi.org/10.1016/j.rser.2013.08.072.

Faheem, M., Kuusniemi, H., Eltahawy, B., Bhutta, M.S., Raza, B., 2024. A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. IET Gener. Transm. Distrib. 18 (3), 625–638. http://dx.doi.org/10.1049/gtd2.13103.

Fang, X., Misra, S., Xue, G., Yang, D., 2012. Smart grid — The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. 14 (4), 944–980. http://dx.doi.org/10.1109/SURV.2011.101911.00087.

Faraji, H., Vahidi, B., Khorsandi, A., Hossein Hosseinian, S., 2024. Multiple control strategies for smart photovoltaic inverter under network voltage fluctuations and islanded operation. Int. J. Electr. Power Energy Syst. 156, 109723. http://dx.doi.org/10.1016/j.ijepes.2023.109723.

Farhangi, H., 2010. The path of the smart grid. IEEE Power Energy Mag. 8, 18–28. http://dx.doi.org/10.1109/MPE.2009.934876.

Farrokhabadi, M., Solanki, B.V., Canizares, C.A., Bhattacharya, K., Koenig, S., Sauter, P.S., Leibfried, T., Hohmann, S., 2017. Energy storage in microgrids: Compensating for generation and demand fluctuations while providing ancillary services. IEEE Power Energy Mag. 15 (5), 81–91. http://dx.doi.org/10.1109/MPE.2017.2708863.

Feng, S., Haykin, S., 2019. Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks. IEEE Trans. Veh. Technol. 68 (10), 9920–9934. http://dx.doi.org/10.1109/TVT.2019.2935999.

Feng, Z., Yuexia, Z., 2011. Study on smart grid communications system based on new generation wireless technology. In: 2011 International Conference on Electronics, Communications and Control. ICECC, pp. 1673–1678. http://dx.doi.org/10.1109/ICECC.2011.6066343.

Fouda, M.M., Fadlullah, Z.M., Kato, N., Lu, R., Shen, X.S., 2011. A lightweight message authentication scheme for smart grid communications. IEEE Trans. Smart Grid 2 (4), 675–685. http://dx.doi.org/10.1109/TSG.2011.2160661.

Gandoman, F.H., Ahmadi, A., Sharaf, A.M., Siano, P., Pou, J., Hredzak, B., Agelidis, V.G., 2018. Review of FACTS technologies and applications for power quality in smart grids with renewable energy systems. Renew. Sustain. Energy Rev. 82, 502–514. http://dx.doi.org/10.1016/j.rser.2017.09.062.

Gao, J., Asamoah, K.O., Sifah, E.B., Smahi, A., Xia, Q., Xia, H., Zhang, X., Dong, G., 2018. GridMonitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE Access 6, 9917–9925. http://dx.doi.org/10.1109/ACCESS.2018.2806303.

Gao, J., Zhang, X., Liang, H., Shen, X.S., 2014. Joint encryption and compressed sensing in smart grid data transmission. In: 2014 IEEE Global Communications Conference. pp. 662–667. http://dx.doi.org/10.1109/GLOCOM.2014.7036883.

Gaviano, A., Weber, K., Dirmeier, C., 2012. Challenges and integration of PV and wind energy facilities from a smart grid point of view. Energy Procedia 25, 118–125. http://dx.doi.org/10.1016/j.egypro.2012.07.016.

Gelazanskas, L., Gamage, K., 2013. Demand side management in smart grid: A review and proposals for future direction. Sustainable Cities Soc. 11, http://dx.doi.org/10.1016/j.scs.2013.11.001.

Ghaffari, A., Askarzadeh, A., Fadaeinedjad, R., Siano, P., 2024. Mitigation of total harmonic distortion and flicker emission in the presence of harmonic loads by optimal siting and sizing of wind turbines and energy storage systems. J. Energy Storage 86, 111312. http://dx.doi.org/10.1016/j.est.2024.111312.

Ginocchi, M., Ahmadifar, A., Ponci, F., Monti, A., 2020. Application of a smart grid interoperability testing methodology in a real-time hardware-in-the-loop testing environment. Energies 13 (7), http://dx.doi.org/10.3390/en13071648.

Globe Newswire, 2022. Global and China smart meters market report 2022–2027: Growing number of households spurs demand. Res. Mark. Available from: https://www.globenewswire.com/en/news-release/2022/08/02/2490054/28124/en/Global-and-China-Smart-Meters-Market-Report-2022-2027-_Growing-Number-of-Households-Spurs-Demand.html.

Goldstein, A., 2017. Advanced Electrical Power System Sensors Workshop Report. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, http://dx.doi.org/10.6028/NIST.SP.1500-11.

Gope, P., Sikdar, B., 2019. Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids. IEEE Trans. Inf. Forensics Secur. 14 (6), 1554–1566. http://dx.doi.org/10.1109/TIFS.2018.2881730.

Government of Canada, 2023. Smart grid program. Green Infrastruct. Programs URL https://natural-resources.canada.ca/climate-change/green-infrastructure-programs/smart-grids/19793.

Government of Canada, 2024. Energy innovation program smart grid demonstration call for proposals. https://natural-resources.canada.ca/science-and-data/funding-partnerships/opportunities/grants-incentives/energy-innovation-program/energy-innovation-program-smart-grid-demonstration-call-for-proposals/energy-innovation-program-smart. (Accessed 13 January 2024).

Green Empowerment, 2024. Smart grids for small grids. Available from: https://greenempowerment.org/technical-resources/smart-grid-for-small-grids/.

Gunduz, M.Z., Das, R., 2018. Internet of things (IoT): Evolution, components and applications fields. Pamukkale Eniversity J. Eng. Sci..

Gündüz, M., Das, R., 2018a. Analysis of cyber-attacks on smart grid applications. In: 2018 International Conference on Artificial Intelligence and Data Processing. IDAP, pp. 1–5. http://dx.doi.org/10.1109/IDAP.2018.8620728.

Gündüz, M.Z., Das, R., 2018b. A comparison of cyber-security oriented testbeds for IoT-based smart grids. In: 2018 6th International Symposium on Digital Forensic and Security. ISDFS, pp. 1–6. http://dx.doi.org/10.1109/ISDFS.2018.8355329.

Gunduz, M., Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 169 (C), http://dx.doi.org/10.1016/j.comnet.2019.107094.

Gungor, V.C., Lu, B., Hancke, G.P., 2010. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Ind. Electron. 57 (10), 3557–3564. http://dx.doi.org/10.1109/TIE.2009.2039455.

He, Y., Mendis, G.J., Wei, J., 2017. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Trans. Smart Grid 8 (5), 2505–2516. http://dx.doi.org/10.1109/TSG.2017.2703842.

Hegazy, O., 2012. Advanced Power Electronics Interface and Optimization for Fuel Cell Hybrid Electric Vehicles Applications (Ph.D. thesis). Vrije Universiteit Brussel.

Hentea, M., 2021. Building an Effective Security Program for Distributed Energy Resources and Systems. John Wiley & Sons.

Hewage, P., Trovati, M., Pereira, E., Behera, A., 2021. Deep learning-based effective fine-grained weather forecasting model. Pattern Anal. Appl. 24 (1), 343–366. http://dx.doi.org/10.1007/s10044-020-00898-1.

High Voltage Engineering Laboratory (HVEL), 2024. Smart grid. https://uwaterloo.ca/high-voltage-engineering-laboratory/research/smart-grid. (Accessed 13 January 2024).

Hledik, R., 2009. How green is the smart grid? Electr. J. 22 (3), 29–41.

Ida, T., Tanaka, M., Ito, K., 2024. Smart Grid Economics: A Field Experimental Approach to Demand Response, vol. 32, Springer Nature.

IE.E.E. Standards Association, 2012. IEEE standard for electric power systems communications-distributed network protocol (DNP3). In: IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010). pp. 1–821. http://dx.doi.org/10.1109/IEEESTD.2012.6327578.

Jadidi, S., Badihi, H., Zhang, Y., 2023. Active fault-tolerant and attack-resilient control for a renewable microgrid against power-loss faults and data integrity attacks. IEEE Trans. Cybern. 1–16. http://dx.doi.org/10.1109/TCYB.2023.3305240.

Jin, D., Nicol, D.M., Yan, G., 2011. An event buffer flooding attack in DNP3 controlled SCADA systems. In: Proceedings of the 2011 Winter Simulation Conference. WSC, pp. 2614–2626. http://dx.doi.org/10.1109/WSC.2011.6147969.

Joga, S.R.K., Sinha, P., Paul, K., Sahoo, S., Pani, S.R., Dei, G., Ustun, T.S., 2024. Identification of harmonic sources in smart grid using systematic feature extraction from non-active powers. Front. Smart Grids 3, http://dx.doi.org/10.3389/frsgr.2024.1338774.

Jokar, P., Leung, V.C.M., 2018. Intrusion detection and prevention for ZigBee-based home area networks in smart grids. IEEE Trans. Smart Grid 9 (3), 1800–1811. http://dx.doi.org/10.1109/TSG.2016.2600585.

Judge, M.A., Khan, A., Manzoor, A., Khattak, H.A., 2022. Overview of smart grid implementation: Frameworks, impact, performance and challenges. J. Energy Storage 49, http://dx.doi.org/10.1016/j.est.2022.104056.

Kawoosa, A.I., Prashar, D., 2021. A review of cyber securities in smart grid technology. In: 2021 2nd International Conference on Computation, Automation and Knowledge Management. ICCAKM, pp. 151–156. http://dx.doi.org/10.1109/ICCAKM50778.2021.9357698.

Khadem, S.K., Basu, M., Conlon, M., 2010. Power quality in grid connected renewable energy systems: Role of custom power devices. In: International Conference on Renewable Energies and Power Quality. Granada.

Khelifa, B., Abla, S., 2015. Security concerns in smart grids: Threats, vulnerabilities and countermeasures. In: 2015 3rd International Renewable and Sustainable Energy Conference. IRSEC, pp. 1–6. http://dx.doi.org/10.1109/IRSEC.2015.7454963.

Khurana, H., Hadley, M., Lu, N., Frincke, D., 2010. Smart-grid security issues. IEEE Secur. Priv. 8, 81–85. http://dx.doi.org/10.1109/MSP.2010.49.

Kim, D.-K., Alaerjan, A., Lu, L., Yang, H., Jang, H., 2017a. Toward interoperability of smart grids. IEEE Commun. Mag. 55 (8), 204–210. http://dx.doi.org/10.1109/MCOM.2017.1600392.

Kim, H.J., Jeong, C.M., Sohn, J.-M., Joo, J.-Y., Donde, V., Ko, Y., Yoon, Y.T., 2020. A comprehensive review of practical issues for interoperability using the common information model in smart grids. Energies 13 (6), http://dx.doi.org/10.3390/en13061435.

Kim, Y., Raghunathan, V., Raghunathan, A., 2017b. Design and management of battery-supercapacitor hybrid electrical energy storage systems for regulation services. IEEE Trans. Multi-Scale Comput. Syst. 3 (1), 12–24. http://dx.doi.org/10.1109/TMSCS.2016.2627543.

King, T., 2018. Sensing & Measurement Research Activities. Department of Energy, Grid Moderization Laboratory Consortium, pp. 1–23.

Kishore, S., Snyder, L.V., 2010. Control mechanisms for residential electricity demand in SmartGrids. In: 2010 First IEEE International Conference on Smart Grid Communications. pp. 443–448. http://dx.doi.org/10.1109/SMARTGRID.2010.5622084.

Kitsios, A., Bousakas, K., Salame, T., Bogno, B., Papageorgas, P., Vokas, G., Mauffay, F., Petit, P., Aillerie, M., Charles, J.-P., 2017. Renewable energy sources, the internet of things and the third industrial revolution: Smart grid and contemporary information and communication technologies. In: Technologies and Materials for Renewable Energy, Environment and Sustainability. In: AIP Conference Proceedings, vol. 1814, 020070. http://dx.doi.org/10.1063/1.4976289.

Kumar, N.A., Daniel, R., Pasam, P.K., 2024. A novel electrical load forecasting model using a deep learning approach. In: The Internet of Energy: A Pragmatic Approach Towards Sustainable Development. CRC Press, p. 67.

Kumar, P., Kumar, R., Aljuhani, A., Javeed, D., Jolfaei, A., Islam, A.K.M.N., 2023. Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity. Sol. Energy 263, 111921. http://dx.doi.org/10.1016/j.solener.2023.111921.

Kumari, A., Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., 2020. When blockchain meets smart grid: Secure energy trading in demand response management. IEEE Netw. 34 (5), 299–305. http://dx.doi.org/10.1109/MNET.001.1900660.

Kuwałek, P., 2021. Selective identification and localization of voltage fluctuation sources in power grids. Energies 14 (20), http://dx.doi.org/10.3390/en14206585, URL https://www.mdpi.com/1996-1073/14/20/6585.

Larcom, J.A., Liu, H., 2013. Modeling and characterization of GPS spoofing. In: 2013 IEEE International Conference on Technologies for Homeland Security. HST, pp. 729–734. http://dx.doi.org/10.1109/THS.2013.6699094.

Lee, E.-K., Gerla, M., Oh, S.Y., 2012. Physical layer security in wireless smart grid. IEEE Commun. Mag. 50 (8), 46–52. http://dx.doi.org/10.1109/MCOM.2012.6257526.

Leon, R., Vittal, V., Manimaran, G., 2007. Application of sensor network for secure electric energy infrastructure. IEEE Trans. Power Deliv. 22 (2), 1021–1028. http://dx.doi.org/10.1109/TPWRD.2006.886797.

Li, H., Gong, S., Lai, L., Han, Z., Qiu, R.C., Yang, D., 2012. Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Trans. Smart Grid 3 (3), 1540–1551. http://dx.doi.org/10.1109/TSG.2012.2203156.

Linh, N.T., 2009. Power quality investigation of grid connected wind turbines. In: 2009 4th IEEE Conference on Industrial Electronics and Applications. pp. 2218–2222. http://dx.doi.org/10.1109/ICIEA.2009.5138593.

Liserre, M., Sauter, T., Hung, J.Y., 2010. Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics. IEEE Ind. Electron. Mag. 4 (1), 18–37. http://dx.doi.org/10.1109/MIE.2010.935861.

Liu, F., Dong, T., Liu, Q., Liu, Y., Li, S., 2024. Combining fuzzy clustering and improved long short-term memory neural networks for short-term load forecasting. Electr. Power Syst. Res. 226, 109967. http://dx.doi.org/10.1016/j.epsr.2023.109967.

Liu, H., Gu, T., Liu, Y., Song, J., Zeng, Z., 2020. Fault-tolerant privacy-preserving data aggregation for smart grid. Wirel. Commun. Mob. Comput. 2020, http://dx.doi.org/10.1155/2020/8810393.

Liu, Y., Ning, P., Dai, H., Liu, A., 2010. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In: 2010 Proceedings IEEE INFOCOM. pp. 1–9. http://dx.doi.org/10.1109/INFCOM.2010.5462156.

Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14 (1), http://dx.doi.org/10.1145/1952982.1952995.

Lu, Z., Wang, W., Wang, C., 2011. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. In: 2011 Proceedings IEEE INFOCOM. pp. 1871–1879. http://dx.doi.org/10.1109/INFCOM.2011.5934989.

Ma, R., Chen, H.-H., Huang, Y.-R., Meng, W., 2013. Smart grid communication: Its challenges and opportunities. IEEE Trans. Smart Grid 4 (1), 36–46. http://dx.doi.org/10.1109/TSG.2012.2225851.

Ma, L., Chu, Z., Yang, C., Wang, G., Dai, W., 2023. Recursive watermarking-based transient covert attack detection for the industrial CPS. IEEE Trans. Inf. Forensics Secur. 18, 1709–1719. http://dx.doi.org/10.1109/TIFS.2023.3251857.

Mahmood, A., Khan, A., Anjum, A., Maple, C., Jeon, G., 2023. An efficient and privacy-preserving blockchain-based secure data aggregation in smart grids. Sustain. Energy Technol. Assess. 60, 103414. http://dx.doi.org/10.1016/j.seta.2023.103414.

Majeed Butt, O., Zulqarnain, M., Majeed Butt, T., 2021. Recent advancement in smart grid technology: Future prospects in the electrical power network. Ain Shams Eng. J. 12 (1), 687–695. http://dx.doi.org/10.1016/j.asej.2020.05.004.

Mak, S.T., 2010. Sensor data output requirements for Smart Grid applications. In: IEEE PES General Meeting. pp. 1–3. http://dx.doi.org/10.1109/PES.2010.5589580.

Marcos, J., Marroyo, L., Lorenzo, E., Alvira, D., Izco, E., 2011. Power output fluctuations in large scale pv plants: One year observations with one second resolution and a derived analytic model. Prog. Photovolt., Res. Appl. 19 (2), 218–227. http://dx.doi.org/10.1002/pip.1016.

Markovic, D.S., Zivkovic, D., Branovic, I., Popovic, R., Cvetkovic, D., 2013. Smart power grid and cloud computing. Renew. Sustain. Energy Rev. 24, 566–577. http://dx.doi.org/10.1016/j.rser.2013.03.068.

Masoum, M.A., Fuchs, E.F., 2015. Introduction to power quality. In: Masoum, M.A., Fuchs, E.F. (Eds.), Power Quality in Power Systems and Electrical Machines, second ed. Academic Press, Boston, pp. 1–104. http://dx.doi.org/10.1016/B978-0-12-800782-2.00001-4, (Chapter 1).

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., Weinhardt, C., 2018. A blockchain-based smart grid: towards sustainable local energy markets. Comput. Sci. Res. Dev. 33 (1), 207–214. http://dx.doi.org/10.1007/s00450-017-0360-9.

Metke, A.R., Ekl, R.L., 2010. Security technology for smart grid networks. IEEE Trans. Smart Grid 1 (1), 99–107. http://dx.doi.org/10.1109/TSG.2010.2046347.

Ming, Z., Lixin, H., Fan, Y., Danwei, J., 2010. Retracted article: Research of the problems of renewable energy orderly combined to the grid in smart grid. In: 2010 Asia-Pacific Power and Energy Engineering Conference. pp. 1–4. http://dx.doi.org/10.1109/APPEEC.2010.5448334.

Mirkovic, J., Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. SIGCOMM Comput. Commun. Rev. 34 (2), 39–53. http://dx.doi.org/10.1145/997150.997156.

Mohagheghi, S., Stoupis, J., Wang, Z., 2009. Communication protocols and networks for power systems-current status and future trends. In: 2009 IEEE/PES Power Systems Conference and Exposition. pp. 1–9. http://dx.doi.org/10.1109/PSCE.2009.4840174.

Mohamed, M.A., Eltamaly, A.M., Farh, H.M., Alolah, A.I., 2015. Energy management and renewable energy integration in smart grid system. In: 2015 IEEE International Conference on Smart Energy Grid Engineering. SEGE, pp. 1–6. http://dx.doi.org/10.1109/SEGE.2015.7324621.

Mollah, M.B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A.M.Y.M., Koh, L.H., Yang, L., 2021. Blockchain for future smart grid: A comprehensive survey. IEEE Internet Things J. 8 (1), 18–43. http://dx.doi.org/10.1109/JIOT.2020.2993601.

Moretti, M., Djomo, S.N., Azadi, H., May, K., De Vos, K., Van Passel, S., Witters, N., 2017. A systematic review of environmental and economic impacts of smart grids. Renew. Sustain. Energy Rev. 68, 888–898. http://dx.doi.org/10.1016/j.rser.2016.03.039.

Moura, J., 2009. Accommodating high levels of variable generation. In: The Canadian Wind Energy Association's 2009 Wind Matters Conference.

Mrabet, Z.E., Kaabouch, N., Ghazi, H.E., Ghazi, H.E., 2018. Cyber-security in smart grid: Survey and challenges. Comput. Electr. Eng. 67, 469–482. http://dx.doi.org/10.1016/j.compeleceng.2018.01.015.

Muthukumaran, E., Kalyani, S., 2021. Development of smart controller for demand side management in smart grid using reactive power optimization. Soft Comput. 25 (2), 1581–1594. http://dx.doi.org/10.1007/s00500-020-05246-3.

Natarajan, K.P., Bhagavath Singh, S., 2017. FPGA based remote monitoring system in smart grids. Indian J. Sci. Technol. 10, 1–5. http://dx.doi.org/10.17485/ijst/2017/v10i5/108829.

Nateghi, A., Schaarschmidt, M., Fisahn, S., Garbe, H., 2021. Vulnerability of wireless smart meter to electromagnetic interference sweep frequency jamming signals. In: 2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium. pp. 755–759. http://dx.doi.org/10.1109/EMC/SI/PI/EMCEurope52599.2021.9559200.

National Smart Grid Mission, 2024. SG projects. Ministry of Power, Government of India, 17 March 2023. Available from: https://www.nsgm.gov.in/en/sg-pilot.

Nhede, N., 2021. Smart grid's role in energy transition and the top five market leaders. Smart Energy Int. https://www.smart-energy.com/industry-sectors/smart-meters/smart-grids-role-in-energy-transition-and-the-top-five-market-leaders/.

NIST, 2010. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.

NIST, 2018. Smart grid international coordination. https://www.nist.gov/programs-projects/smart-grid-national-coordination/international-coordination. (Accessed 07 November 2023).

Ochoa, L.F., Harrison, G.P., 2011. Minimizing energy losses: Optimal accommodation and smart operation of renewable distributed generation. IEEE Trans. Power Syst. 26 (1), 198–205. http://dx.doi.org/10.1109/TPWRS.2010.2049036.

Office of Electric Transmission and Distribution, 2003. Grid 20230 - A National Vision for Electricity's Second 100 Years. Tech. rep., United States Department of Energy, Washington, D.C.

Oozeer, M.I., Haykin, S., 2019a. Cognitive dynamic system for control and cyber-attack detection in smart grid. IEEE Access 7, 78320–78335. http://dx.doi.org/10.1109/ACCESS.2019.2922410.

Oozeer, M.I., Haykin, S., 2019b. Cognitive risk control for mitigating cyber-attack in smart grid. IEEE Access 7, 125806–125826. http://dx.doi.org/10.1109/ACCESS.2019.2939089.

Ourahou, M., Ayrir, W., Hassouni, B.E., Haddi, A., 2020. Review on smart grid control and reliability in presence of renewable energies: Challenges and prospects. Math. Comput. Simulation 167, 19–31. http://dx.doi.org/10.1016/j.matcom.2018.11.009.

Panda, D.K., Das, S., 2021. Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. J. Clean. Prod. 301, 126877. http://dx.doi.org/10.1016/j.jclepro.2021.126877.

Pandey, R.K., Misra, M., 2016. Cyber security threats — Smart grid infrastructure. In: 2016 National Power Systems Conference. NPSC, pp. 1–6. http://dx.doi.org/10.1109/NPSC.2016.7858950.

Pang, C., Dutta, P., Kezunovic, M., 2012. BEVs/PHEVs as dispersed energy storage for V2B uses in the smart grid. IEEE Trans. Smart Grid 3 (1), 473–482. http://dx.doi.org/10.1109/TSG.2011.2172228.

Papaioannou, I., et al., 2018. Smart grid interoperability testing methodology. In: JRC Publications Repository. Publications Office of the European Union, Luxembourg (Luxembourg), http://dx.doi.org/10.2760/08049.

Paramo, G., Bretas, A., Meyn, S., 2022. Research trends and applications of PMUs. Energies 15 (15), http://dx.doi.org/10.3390/en15155329.

Paul, S., Rabbani, M., Kundu, R., Zaman, S., 2014. A review of smart technology (Smart Grid) and its features. In: Proceedings of 2014 1st International Conference on Non Conventional Energy. ICONCE 2014, pp. 200–203. http://dx.doi.org/10.1109/ICONCE.2014.6808719.

Pavithra, L., Rekha, D., 2021. Prevention of replay attack for isolated smart grid. In: Next Generation Information Processing System. Springer Singapore, Singapore, pp. 251–258.

Pendarakis, D., Shrivastava, N., Liu, Z., Ambrosio, R., 2007. Information aggregation and optimized actuation in sensor networks: Enabling smart electrical grids. In: IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications. pp. 2386–2390. http://dx.doi.org/10.1109/INFCOM.2007.286.

Peng, C., Sun, H., Yang, M., Wang, Y.-L., 2019. A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans. Syst. Man Cybern. Syst. 49 (8), 1554–1569. http://dx.doi.org/10.1109/TSMC.2018.2884952.

Popper, C., Strasser, M., Capkun, S., 2009. Jamming-resistant broadcast communication without shared keys. In: USENIX Security Symposium. pp. 231–248.

Premaratne, U.K., Samarabandu, J., Sidhu, T.S., Beresh, R., Tan, J.-C., 2010. An intrusion detection system for IEC61850 automated substations. IEEE Trans. Power Deliv. 25 (4), 2376–2383. http://dx.doi.org/10.1109/TPWRD.2010.2050076.

Rajesh, C., Meenalochini, P., Kannaiah, S.K., Bindu, A., 2024. A hybrid control topology for cascaded H-bridge multilevel inverter to improve the power quality of smart grid connected system: NBO-RERNN approach. Expert Syst. Appl. 238, 122054. http://dx.doi.org/10.1016/j.eswa.2023.122054.

Rajfallovska, A., 2016. Green telecommunications in smart grid. Int. At. Energy Agency.

Ranjan, S., Swaminathan, R., Uysal, M., Nucci, A., Knightly, E., 2009. DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Trans. Netw. 17 (1), 26–39. http://dx.doi.org/10.1109/TNET.2008.926503.

Rawat, D.B., Bajracharya, C., 2015. Cyber security for smart grid systems: Status, challenges, and perspectives. In: SoutheastCon 2015. pp. 1–6. http://dx.doi.org/10.1109/SECON.2015.7132891.

Razzak, A., Islam, M.T., Roy, P., Razzaque, M.A., Hassan, M.R., Hassan, M.M., 2024. Leveraging Deep Q-Learning to maximize consumer quality of experience in smart grid. Energy 290, 130165. http://dx.doi.org/10.1016/j.energy.2023.130165.

Rizzetti, T.A., Wessel, P., Rodrigues, A.S., Menezes Da Silva, B., Milbradt, R., Canha, L.N., 2015. Cyber security and communications network on SCADA systems in the context of smart grids. In: 2015 50th International Universities Power Engineering Conference. UPEC, pp. 1–6. http://dx.doi.org/10.1109/UPEC.2015.7339762.

Romero, M., Guédria, W., Panetto, H., Barafort, B., 2020. Towards a characterisation of smart systems: A systematic literature review. Comput. Ind. 120, 103224. http://dx.doi.org/10.1016/j.compind.2020.103224.

Romero Aquino, M., 2021. A Smart Assessment of Business Processes for Enterprises Decision Support (Ph.D. thesis). University of Lorraine.

Saadatmand, M., Ramezy, B., Mozafari, B., 2017. Review of communication technologies for smart grid applications. In: The National Conference on New Approaches in Power Industry. pp. 1–10.

Salkuti, S.R., 2020. Challenges, issues and opportunities for the development of smart grid. Int. J. Electr. Comput. Eng. (IJECE) 10 (2), 1179–1186. http://dx.doi.org/10.11591/ijece.v10i2.pp1179-1186.

Samineni, S., Johnson, B., Hess, H., Law, J., 2006. Modeling and analysis of a flywheel energy storage system for Voltage sag correction. IEEE Trans. Ind. Appl. 42 (1), 42–52. http://dx.doi.org/10.1109/TIA.2005.861366.

Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., Biswas, S., 2016. Smart grid security: Threats, challenges, and solutions. arXiv:1606.06992.

Saxena, N., Choi, B.J., Lu, R., 2016. Authentication and authorization scheme for various user roles and devices in smart grid. IEEE Trans. Inf. Forensics Secur. 11 (5), 907–921. http://dx.doi.org/10.1109/TIFS.2015.2512525.

Schuba, C., Krsul, I., Kuhn, M., Spafford, E., Sundaram, A., Zamboni, D., 1997. Analysis of a denial of service attack on TCP. In: Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097). pp. 208–223. http://dx.doi.org/10.1109/SECPRI.1997.601338.

Shadare, A.E., Sadiku, M.N., Musa, S.M., 2017. Electromagnetic compatibility issues in critical smart grid infrastructure. IEEE Electromagn. Compat. Mag. 6 (4), 63–70. http://dx.doi.org/10.1109/MEMC.0.8272283.

Shafiullah, G.M., Oo, A.M.T., Jarvis, D., Ali, A.B.M.S., Wolfs, P., 2010. Potential challenges: Integrating renewable energy with the smart grid. In: 2010 20th Australasian Universities Power Engineering Conference. pp. 1–6.

Shahinzadeh, H., Mirhedayati, A.-s., Shaneh, M., Nafisi, H., Gharehpetian, G.B., Moradi, J., 2020. Role of joint 5G-IoT framework for smart grid interoperability enhancement. In: 2020 15th International Conference on Protection and Automation of Power Systems. IPAPS, pp. 12–18. http://dx.doi.org/10.1109/IPAPS52181.2020.9375539.

Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., Al Ali, A.R., 2015. Smart grid cyber security: Challenges and solutions. In: 2015 International Conference on Smart Grid and Clean Energy Technologies. ICSGCE, pp. 170–175. http://dx.doi.org/10.1109/ICSGCE.2015.7454291.

Shi, L., Crow, M.L., 2008. Comparison of ultracapacitor electric circuit models. In: 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. pp. 1–6. http://dx.doi.org/10.1109/PES.2008.4596576.

Shi, H., Xie, L., Peng, L., 2021. Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method. Comput. Electr. Eng. 91, 107058. http://dx.doi.org/10.1016/j.compeleceng.2021.107058.

Song, E.Y., FitzPatrick, G.J., Lee, K.B., 2017a. Smart sensors and standard-based interoperability in smart grids. IEEE Sens. J. 17 (23), 7723–7730. http://dx.doi.org/10.1109/JSEN.2017.2729893.

Song, E.Y., FitzPatrick, G.J., Lee, K.B., Gopstein, A.M., Boynton, P.A., 2018. Interoperability testbed for smart sensors in smart grids. In: 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference. ISGT, pp. 1–5. http://dx.doi.org/10.1109/ISGT.2018.8403332.

Song, E.Y., FitzPatrick, G.J., Lee, K.B., Griffor, E., 2022. A methodology for modeling interoperability of smart sensors in smart grids. IEEE Trans. Smart Grid 13 (1), 555–563. http://dx.doi.org/10.1109/TSG.2021.3124490.

Song, E.Y., Lee, K.B., FitzPatrick, G.J., Zhang, Y., 2017b. Interoperability test for IEC 61850-9-2 standard-based merging units. In: 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference. ISGT, pp. 1–6. http://dx.doi.org/10.1109/ISGT.2017.8086084.

Stavrou, A., Keromytis, A.D., 2005. Countering DoS attacks with stateless multipath overlays. In: Proceedings of the 12th ACM Conference on Computer and Communications Security. CCS '05, Association for Computing Machinery, New York, NY, USA, pp. 249–259. http://dx.doi.org/10.1145/1102120.1102153.

Strasser, M., Popper, C., Capkun, S., Cagalj, M., 2008. Jamming-resistant key establishment using uncoordinated frequency hopping. In: 2008 IEEE Symposium on Security and Privacy. Sp 2008, pp. 64–78. http://dx.doi.org/10.1109/SP.2008.9.

Supriya, P., Nambiar, T., Charu, R., Tyagi, A., Nagadharni, V., Deepika, M., 2011. A laboratory prototype of a smart grid based demand side management. In: ISGT2011-India. pp. 28–31. http://dx.doi.org/10.1109/ISET-India.2011.6145343.

Syed, D., Refaat, S.S., Bouhali, O., 2020. Privacy preservation of data-driven models in smart grids using homomorphic encryption. Information 11 (7), http://dx.doi.org/10.3390/info11070357.

Tan, K.M., Babu, T.S., Ramachandaramurthy, V.K., Kasinathan, P., Solanki, S.G., Raveendran, S.K., 2021. Empowering smart grid: A comprehensive review of energy storage technology and application with renewable energy integration. J. Energy Storage 39, 102591. http://dx.doi.org/10.1016/j.est.2021.102591.

Tan, S., De, D., Song, W.-Z., Yang, J., Das, S.K., 2017. Survey of security advances in smart grid: A data driven approach. IEEE Commun. Surv. Tutor. 19 (1), 397–422. http://dx.doi.org/10.1109/COMST.2016.2616442.

Tian, M., Cui, M., Dong, Z., Wang, X., Yin, S., Zhao, L., 2019. Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid. IEEE Access 7, 9836–9847. http://dx.doi.org/10.1109/ACCESS.2018.2890604.

Toronto Metropolitan University Centre for Urban Energy, 2024. Schneider electric smart grid laboratory. https://www.torontomu.ca/cue/testing/schneider-electric-smart-grid-lab/. (Accessed 13 January 2024).

Tran, T.-T., Shin, O.-S., Lee, J.-H., 2013. Detection of replay attacks in smart grid systems. In: 2013 International Conference on Computing, Management and Telecommunications. ComManTel, pp. 298–302. http://dx.doi.org/10.1109/ComManTel.2013.6482409.

Ugale, B.A., Soni, P., Pema, T., Patil, A., 2011. Role of cloud computing for smart grid of India and its cyber security. In: 2011 Nirma University International Conference on Engineering. pp. 1–5. http://dx.doi.org/10.1109/NUiConE.2011.6153298.

University of Melourne Department of Electrical and Electronic Engineering, 2024. Smart grid lab. https://electrical.eng.unimelb.edu.au/power-energy/smart-grid-lab. (Accessed 13 January 2024).

U.S. Department of Energy, 2024. Recovery act smart grid program. SmartGrid.gov. URL https://www.smartgrid.gov/recovery_act/index.html.

U.S. Department of Energy, 2024a. Recovery act: Smart grid demonstration program. https://www.smartgrid.gov/archive/recovery_act/overview/smart_grid_demonstration_program.html. (Accessed 13 January 2024).

U.S. Department of Energy, 2024b. Recovery act: Smart grid investment grant program. https://www.smartgrid.gov/archive/recovery_act/overview/smart_grid_investment_grant_program. (Accessed 13 January 2024).

Uzunoglu, M., Alam, M., 2006. Dynamic modeling, design, and simulation of a combined PEM fuel cell and ultracapacitor system for stand-alone residential applications. IEEE Trans. Energy Convers. 21 (3), 767–775. http://dx.doi.org/10.1109/TEC.2006.875468.

Venayagamoorthy, G., 2009. Potentials and promises of computational intelligence for smart grids. In: 2009 IEEE Power and Energy Society General Meeting. PES '09, pp. 1–6. http://dx.doi.org/10.1109/PES.2009.5275224.

Visser, L., Schuurmans, E., AlSkaif, T., Fidder, H., van Voorden, A., van Sark, W., 2022. Regulation strategies for mitigating voltage fluctuations induced by photovoltaic solar systems in an urban low voltage grid. Int. J. Electr. Power Energy Syst. 137, 107695. http://dx.doi.org/10.1016/j.ijepes.2021.107695.

Wang, W., Lu, Z., 2013. Cyber security in the smart grid: Survey and challenges. Comput. Netw. 57, 1344–1371. http://dx.doi.org/10.1016/j.comnet.2012.12.017.

Wang, J., Niu, X., Zhang, L., Liu, Z., Huang, X., 2024. A wind speed forecasting system for the construction of a smart grid with two-stage data processing based on improved ELM and deep learning strategies. Expert Syst. Appl. 241, 122487. http://dx.doi.org/10.1016/j.eswa.2023.122487.

Wasiak, I., Hanzelka, Z., 2009. Integration of distributed energy sources with electrical power grid. Bull. Pol. Acad. Sci. Tech. Sci. 57 (4), 297–309. http://dx.doi.org/10.2478/v10175-010-0132-1.

Worighi, I., Maach, A., Hafid, A., Hegazy, O., Van Mierlo, J., 2019. Integrating renewable energy in smart grid system: Architecture, virtualization and analysis. Sustain. Energy Grids Netw. 18, 100226. http://dx.doi.org/10.1016/j.segan.2019.100226.

World Energy Outlook, 2016. Energy and Air Pollution. Tech. rep., International Energy Agency (IEA0), Paris, France.

Xie, L., Carvalho, P.M.S., Ferreira, L.A.F.M., Liu, J., Krogh, B.H., Popli, N., Ilić, M.D., 2011. Wind integration in power systems: Operational challenges and possible solutions. Proc. IEEE 99 (1), 214–232. http://dx.doi.org/10.1109/JPROC.2010.2070051.

Yaar, A., Perrig, A., Song, D., 2003. Pi: a path identification mechanism to defend against DDoS attacks. In: 2003 Symposium on Security and Privacy, 2003. pp. 93–107. http://dx.doi.org/10.1109/SECPRI.2003.1199330.

Yan, Y., Qian, Y., Sharif, H., Tipper, D., 2012. A survey on cyber security for smart grid communications. IEEE Commun. Surv. Tutor. 14 (4), 998–1010. http://dx.doi.org/10.1109/SURV.2012.010912.00035.

Yang, Y., Littler, T., Sezer, S., McLaughlin, K., Wang, H.F., 2011. Impact of cyber-security issues on smart grid. In: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies. pp. 1–7. http://dx.doi.org/10.1109/ISGTEurope.2011.6162722.

York University Department of Electrical Engineering and Computer Science, 2024. Smart grid research lab. https://smartgrid.eecs.yorku.ca/. (Accessed 13 January 2024).

Young, J., 2017. Smart grid technology in the developing world. Seattle Pacidic Library. URL https://digitalcommons.spu.edu/honorsprojects/68.

Yuan, Y., Li, Z., Ren, K., 2011. Modeling load redistribution attacks in power systems. IEEE Trans. Smart Grid 2 (2), 382–390. http://dx.doi.org/10.1109/TSG.2011.2123925.

Yurish, S.Y., 2010. Sensors: Smart vs. Intelligent. Sens. Transducers 114 (3), 6–I,II,III,IV,V,VI.

Zhang, Z., Gong, S., Dimitrovski, A.D., Li, H., 2013. Time synchronization attack in smart grid: Impact and analysis. IEEE Trans. Smart Grid 4 (1), 87–98. http://dx.doi.org/10.1109/TSG.2012.2227342.

Zhang, Z., Huang, S., Chen, Y., Li, B., Mei, S., 2022. Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game. IEEE Trans. Power Syst. 37 (1), 530–542. http://dx.doi.org/10.1109/TPWRS.2021.3091616.

Zhao, Y., Milanović, J.V., 2024. Prediction of harmonic distortion in sparsely monitored transmission networks with renewable generation. IEEE Trans. Power Deliv. 1–13. http://dx.doi.org/10.1109/TPWRD.2024.3373823.

Zhou, H.J., Guo, C.X., Qin, J., 2010. Efficient application of GPRS and CDMA networks in SCADA system. In: IEEE PES General Meeting. pp. 1–6. http://dx.doi.org/10.1109/PES.2010.5588206.