Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 2, Issue 5, 2024

CYBERSECURITY AND ELECTRICAL SAFETY IN SMART GRIDS

Fawad Khan

Graduate, Department of Engineering & Technology, Sarhad University of Science & Information Technology, Peshawar, KP, Pakistan.

fawadkhank313@gmail.com

DOI:https://doi.org/10.5281/zenodo.17248217

Keywords
Smart grids; cybersecurity; electrical safety; SCADA systems; false data injection attacks; intrusion detection

Article History
Received: 08 October 2024
Accepted: 18 December 2024
Published: 31 December 2024

Corresponding Author: *
Fawad Khan

Abstract
The shift in the traditional power grids to smart grids has introduced the unprecedented opportunities in the field of efficiency, sustainability, and real-time control of energy. Smart grids combine physical and cyber space, with the help of digital communication, automation, and distributed energy resources, and enhance operational reliability. Nevertheless, convergence has also introduced new vulnerabilities on the nexus of electrical safety and cybersecurity. Protective mechanisms can be disrupted by cyberattacks like malware, ransomware, false data injection, and insider threats to compromise supervisory control and data acquisition (SCADA) systems and cause physical hazards like arc flashes, equipment damage, and cascading blackouts. The paper will look at smart grid architecture, identify the cybersecurity risks that compromise electrical safety, and look at how they can be applied in practice using the case of the Ukrainian grid attacks. It additionally discusses defense in depth techniques, intrusion detectors, encryption, artificial intelligence, and cross-training disciplines, and regulatory documents, such as the IEEE 2030, IEC 62443, and NERC CIP. In the future, new technologies such as blockchain-based trust management and digital twins-based predictive resilience coupled with human-centered solutions can be promising avenues of improving systemic protection. The research concludes that protection of smart grids is not only a matter of technology innovation but also regulation enforcement, cooperation at the international level, and cultural changes in the direction of collective responsibility. Making smart grids cyber-safe and resilient is thus of paramount importance to further the sustainable energy agenda and safeguard the well-being of the people, their economic stability, and national security.

INTRODUCTION

The world energy industry is in the process of significant change, with the growing need to obtain reliable, efficient, and sustainable electricity. The core of this change is the notion of the smart grid, and it is a radical break with the model of the traditional electricity grid. A smart grid may be described as an advanced electricity system, which combines the digital communication systems, automation, and distributed energy resources (DERs) to achieve more intelligent, adaptive, and resilient energy management (Amin and Wollenberg, 2005; Gunkgor et al., 2011). Smart grids, as opposed to traditional power grids, which are basically intended to provide one-way power flow through centralized

generation plants to the consumers, are based on the concept of two-way communication, allowing real-time monitoring, demand-side control, and integration of renewable energy sources (such as solar and wind) (Fang et al., 2012).

The enabling technologies, such as devices of the Internet of Things (IoT), sensors, advanced metering infrastructure (AMI) and supervisory control and data acquisition (SCADA), make this increased functionality possible (Gao et al., 2012). These parts combined enable the utilities to optimize the energy delivery, enhance fault detection and response, and minimize the transmission losses. Yet, as digitalization enhances the efficiency of operations, it also introduces some new vulnerabilities that were previously not present in the traditional grid infrastructures (Zhang et al., 2022).

Threats of smart grids are twofold in terms of both physical electrical dangers and information security-related threat. Physically, overcurrents, arc flash, short circuit, and equipment failures have continued to pose hazards that may lead to injury to maintenance personnel, damage to critical infrastructure, and massive interruption of services (Madani et al., 2016). On the online front, the integration of networked devices and communication interconnections opens the smart grids to cybercrimes, such as malware, ransomware, denial-of-service (DoS) attacks, and fake data injections (Liu et al., 2011; Conti et al., 2018). These attacks can not only interfere with grid operations, but also increase the hazards already present in electrical systems by paralyzing protective systems, changing relay settings, or even slowing down emergency response time.

The synergy of these hazards highlights the significance of resilience on contemporary energy systems. In this case, the term resilience is to be understood as the capacity of a smart grid to foresee, resist, and adapt to, as well as recover physical malfunctions and cyber attacks without the deterioration of its vital operations (Zhang et al., 2022). Maintaining resilience is not only a technical issue, but a social necessity. A smart-grid failure has a very extensive impact:Any inconveniences in electricity supply may impact hospitals, transportation, water supply, and financial systems, endangering the safety of the population, economic stability, and national security (Case, 2016; NERC, 2023). Consequently, the ways in which cybersecurity and electrical safety interrelate is an important issue that should be understood and resolved in order to implement smart grids successfully.

Therefore, understanding and addressing the interplay between cybersecurity and electrical safety is critical to the successful deployment of smart grids. This paper examines the architecture of smart grids, identifies their key vulnerabilities, explores the cybersecurity threats that impact electrical safety, and discusses strategies, standards, and future directions for building cyber-safe and resilient energy systems.

2. Smart Grid Architecture and Safety Concerns

Smart grids are amongst the most disruptive innovations in the present-day energy infrastructure, which combines the conventional electrical systems with the latest digital technologies to become more efficient, sustainable and reliable. In contrast to traditional power grids, which were basically created to allow one-way electricity flow between centralized generation facilities to consumers, smart grids allow bi-directional communication and control. This is implemented by incorporating smart equipment like smart meters, sensors, Internet of Things (IoT) gadgets, and advanced communication protocols which connect the physical objects to digital observation and decision making processes (Amin and Wollenberg, 2005; Güngor et al., 2011).

A smart grid architecture can be described as a multilayered architecture. At the physical level, the main components are transmission lines, substations, transformers and distribution networks which supply electricity to the final users. On top of this infrastructure is a digital layer comprising of IoT-based devices, phasor measurement units (PMUs) and supervisory control and data acquisition (SCADA) systems that enable real-time data collection and remote monitoring (Gao et al., 2012). More sophisticated protection relays and auto control systems also enable the utilities to identify an anomaly, address faults and load balancing. The smooth communication of physical and digital layers is to improve operational efficiency, minimize downtime and facilitate the incorporation of renewable energy sources like solar and wind energy.

Nevertheless, electrical safety risk has been transformed radically owing to the digitalization of power systems. Traditional grids had most safety mechanisms that were both mechanical and electromechanical. SCADA system protection through circuit breakers, protective relays, and manually monitored systems was developed to isolate faults, contain equipment faults, and avoid cascading outages (Madani et al., 2016). These mechanisms were not immune to failure, but were fairly inaccessible to cyber attacks due to the closed or semi closed nature of these environments. Conversely, the linkedness of smart grids creates new sources of vulnerability. Current safety systems have now been interlinked via digital communication systems, and they are also prone to attacks by computer criminals due to their dependence on software programs.

Indicatively, a device threat to a single IoT-enabled sensor may result in false data reporting, incorrect interpretation of system conditions by the grid operators. Equally, a compromised SCADA server may slow down the de-energizing of electrical faults or worst still, give unapproved instructions to protective relays. The result of such interconnectivity is that local risks can grow into system risks. According to Zhang et al. (2022), manipulated sensor data or hacked PMUs may give operators incorrect instructions, prompting them to make dangerous corrective actions, which may put the stability and reliability of the grid at risk. A hypothetical scenario would be an attacker who modifies voltage and frequency measurements to make the operators believe that the conditions are stable when in reality the system is on the point of overloading. This interference might cause delay in required interventions leading to massive outages or damages of equipment.

The crossing of the operational technology (OT) in physical grid operations and information technology (IT) in the digital communication and control has blurred the traditional divisions between engineering and cybersecurity. This hybridization implies that the problem of electrical safety can not be resolved simply by adhering to the conventional engineering approach anymore. Rather, it is necessary to install secure digital infrastructures as part of safety measures. Sharma and Sood (2011) argue that modern grid safety depends on a holistic approach that integrates both physical protection mechanisms and cybersecurity defenses, acknowledging that failures in one domain can have direct repercussions in the other. In short, smart grid safety is now inseparable from cybersecurity, and any comprehensive resilience framework must treat them as interdependent dimensions.

3. Cybersecurity Threats to Smart Grids

The growing use of smart grids as digital networks and interconnected devices has rendered them the easiest targets of cyberattacks. The vulnerabilities of smart grids are a range of cyber threats that take advantage of software defects, poor communication schemes, and human mistakes, unlike conventional power grids, the vulnerabilities of which are largely physical in nature. Such attacks are not only limited in stealing information or committing financial fraud but could also destabilize economies, compromise the major infrastructure and threaten the safety of the people.

A very notable group of cyber threat is that of malware and ransomware. Software viruses may penetrate the grid control systems, corrupt files and hinder normal operation. Ransom ware attacks are worse, since the operators are locked out of the control consoles until a ransom is paid. Such disruptions were demonstrated by the global WannaCry ransomware attack in 2017. Even though the healthcare systems were its main targets, multiple critical infrastructure sectors, such as energy, were impacted as well, which shows the weakness of utilities to large-scale ransomware attacks (Conti et al., 2018). In case of such malware specifically designed to target grid systems, it would be able to shut down monitoring stations, slow down emergency response, and even cause cascade failures.

The other significant risk is that of attacks on the SCADA systems and the programmable logic controllers (PLCs). The elements play crucial roles in the control of critical grid operations like regulating voltage, distribution of loads, and coordination of protective devices. Achieving control over the activity of SCADA servers or PLCs is one of the benefits through which the attacker may be directly involved in the work of the grid and provide unauthorized commands to it or even turn off the systems intended to protect it. Although the initial target of

the Stuxnet worm was nuclear plants, it showed the destructive power of malware that could exploit the vulnerabilities in PLCs (Khurana et al., 2010). Stuxnet physically damaged centrifuges by manipulating the operation parameters without making it apparent to the operators that centrifuges were sabotaged. Applied to smart grids, this type of attack would be able to shut down relays, overload transformers, or intentionally trip circuit breakers, which would disrupt operations in addition to causing physical damage.

Another malicious attack is false data injection attacks (FDIAs). FDIAs do not require operators to have control over systems, unlike direct intrusions, in which intruders gain control of systems. Attackers can manipulate measurement values in a way that deceives the operators to make unsafe decisions by intentionally manipulating current, voltage, or frequency measurements. In the case of a FDIA, an example is that a control center may be fooled by a false indication that a fault has been cleared, postponing protective measures and increasing the extent of damage. Liu, Ning, and Reiter (2011) showed that FDIAs are especially hard to identify since they are capable of circumventing the traditional anomaly detection techniques. In a large scale deployment, FDIAs may cause all the relays to miscoordinate, and power flow to be unstable.

Lastly, insider threats are a very specific category of weakness. In contrast to external hackers, insiders, such as employees, contractors, or maintenance staff already have a legitimate access to critical systems. Insiders can unintentionally or intentionally sabotage grid security whether through malicious intent, negligence or ignorance of cybersecurity. According to Patel et al. (2020), insider threat becomes particularly dangerous due to the ability to bypass perimeter controls (i.e., firewalls or intrusion detection systems). An angry employee who has access to SCADA servers, e.g., might turn off alarms or alter relay settings, posing a great safety hazard. To reduce insider threats, technical solutions, including access control and activity monitoring, are essential, but organizational policies, such as personnel screening, periodic training, and creation of an ethos of responsibility, can also be used.

The existence of these various types of cyber threats points out the necessity to stop viewing cybersecurity as a support issue. In the case of smart grids, cybersecurity has to be integrated into the design of the system, the working practices, and the maintenance process. The traditional safety engineering is not enough; the safety of the protection systems themselves can fall under the scam of the cyber-attack, and safeguards will become weapons of attack.

4. Impact on Electrical Safety

The consequences of cyberattack of smart grids are much broader than the realm of the digital world because interruptions in such systems may directly affect physical infrastructure and put human lives in danger. In comparison with the traditional breaches of IT, where the outcome can be a loss of data or money, cyber-attacks into smart grids can cause electrical risks with disastrous physical implications. This physical-cyber risk convergence highlights the need to pay extra attention to smart grids as critical infrastructure. One of the safety issues of concern is arc flashes and equipment overloads. When protective equipment like relays or breakers are controlled through cyber intrusion, they might not trip when there is fault or they might faultlessly trip when the conditions are stable. As an example, an attacker might change relay settings to slow the clearing of faults so that too much current flows through conductors. This can result in overheating, arc flashes or fire which endangers field technicians and jeopardizes the safety of the people (Madani et al., 2016). Arc flashes, especially, can produce the high heat and pressure, which may result in serious injuries or death of the maintenance workers, particularly when they do not realize that the settings which were considered to be safe have been altered.

The other significant risk is that there will be overcurrent faults and cascading blackouts. Compromised SCADA systems would send false commands that would turn off important feeders unintentionally or block breakers during short circuits. These may cause ripple effects throughout the grid, as a single component failure imposes extra pressure on the others, causing massive outages everywhere. According to Zhang et al. (2022), cascading failures are also especially destructive since they interfere not only with the residential power system but also with other vital services, including

hospitals, the water treatment system, and the network. In severe situations, the long-term blackouts may undermine the national security, economic stability, and health of people.

There is also a risk of a long-term damage to equipment and loss of money because of cyberattacks. Attackers can destroy valuable assets such as transformers, generators, and distribution equipment by intentionally causing the malfunction of protective devices such as by prohibiting a breaker from tripping when in a sustained fault condition. The cost of repairing or replacing such components is tremendous, and in most cases, millions of dollars are incurred. Moreover, repair time magnifies the economic effect, since it interferes with the production and basic services in the industrial sector (Amin and Wollenberg, 2005). In addition to the financial aspect, damaged equipment extends the vulnerability of the grid until full functionality is restored, causing the grid to remain vulnerable to reoccurring attacks or physical breakdown.

Certainly, there is no evidence that cybersecurity and electrical safety are increasingly meeting quite as strongly than the evidence on real-life events. The cyberattacks on the Ukrainian power grid in 2015 and 2016 are examples of stark ones. These attacks were attributed to the black energy and Industroyer malware families and brought down SCADA systems and remotely disconnected substations leading to blackouts on a massive scale and affecting over 200,000 consumers (Case, 2016). The unusual feature of these cases was not only the magnitude of the disruption but also that the intrusions into the cyber became directly converted into massive physical disruptions. Automated protective mechanisms failed to ensure that grid operators and maintenance workers were put in dangerous spots, which is an example of how digital sabotage can cripple worker safety and community trust in major infrastructure.The experience in Ukraine reminds of the fact that smart grids cannot be perceived as a mere technological enhancement of the conventional one. The fact that they rely on digital infrastructures makes them cyber-physical systems, and any weaknesses in software and networks may become life-threatening risks. This underlines the pressing need of combined defense methods that will protect against cybersecurity and electrical safety at the same time. Securing smart grids is not only a data safety or continuation of service issue, but also a key element in the preservation of human life, infrastructure robustness, and stability of contemporary societies.

5. Strategies for Cyber-Safe Smart Grids

The growing sophistication of smart grids requires a security framework which is not merely reactive but fundamentally proactive and deals with vulnerabilities at a stage before they develop into crises. The high interdependence between the physical electrical infrastructure and digital technologies introduces the scenario in which the digital-based threats may have extreme physical impacts. Thus, the best method of making grids safe is to implement a defense-in-depth strategy. This is a multi-tiered defense model whereby should a single defensive measure be breached, there are still other defenses to protect against the domino effect. Such a method is one of prevention, detection, response and recovery, which results in a resilient and holistic system.

Intrusion detection and anomaly monitoring is rated among the most important pillars of this strategy. The operational data continually produced by a smart grid are enormous, including relay statuses and voltage and current measurements of various points in the system. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) is very important in processing this traffic to identify abnormal behavior that may be a sign of the breach. As an example, the SCADA commands are abnormally executed or the relay acts in a way that it is not expected, these can indicate that an intruder is trying to control the work of the systems. This layer is further reinforced by the use of machine learning, which assists in differentiating between real changes in grid activity, e.g. the ones induced by renewable energy intermittency, and malicious activities. Not only does this improve the accuracy of detection but it also decreases false alarms that will overwhelm human operators.

The other important element entails the protection of communications in the grid. The high dependence on the interconnected devices like IoT sensors, smart meters, and substations implies that sensitive data are being transferred all the time on networks. This information is securely transported by

encryption systems such as TLS and IPSec to ensure that it is not intercepted or otherwise manipulated by malicious parties. Simultaneously, secure authentication, such as multi-factor authentication, will be used to make sure that the system is only accessed by legitimate users or devices. In the absence of such measures, attackers might inject malicious code into control systems or steal working data which may be used in future attacks. Encryption and authentication offers a necessary defense against cyber intrusions by securing the content and the integrity of communication.

Machine learning and artificial intelligence are also increasingly important to smart grid security. These technologies are able to keep track of cybersecurity incidents and physical safety indications simultaneously thereby eliminating the gap between digital and electrical safety. As an example, AI algorithms trained on historical operational data can detect early warning of transformer overheating, failed breakers or cyber-motivated abnormalities like coordinated false data injection attacks. Utilities are also able to act proactively by identifying and monitoring the risks that might occur before they worsen. Such a predictive safety model minimizes the downtime, eliminates expensive damage and increases operational continuity and resilience. Human experience, nevertheless, also is a crucial element. The disciplinary divide between electrical engineering and cybersecurity is one of the long-standing problems in ensuring smart grids. Although electrical engineers are well aware of the complexities of power system systems, cybersecurity professionals concentrate on protecting digital systems. Cyber risks Cross-training programs can fill this gap, with engineers learning about cyber risks, and IT professionals learning how the power grid works. These hybrid professionals will make collaboration more effective and will make sure that neither of the domains is overemphasized at the cost of the other. Due to the changes in threats, the development of interdisciplinary skills in the workforce will have a vital role to play in grid protection.

6. Regulatory and Standardization Efforts

Technological innovation is fundamental, but it cannot give the stability that is necessary to implement smart grids at either country or international levels. The regulatory measures and standardization should play a key role in the implementation of security practices in the energy industry in an orderly manner. In the absence of a system of enforceable standards, the implementation of protection mechanisms tends to be uneven and leave certain parts of the grid vulnerable, which in turn jeopardizes the resilience of interdependent energy systems. There are several organizations that have contributed greatly in this area. Standards have been established by the Institute of Electrical and Electronics Engineers (IEEE) that describe secure communications protocols and best practices in integrating distributed energy resources within the grid such as IEEE 2030. The standards are especially applicable to a future where renewable energy and decentralized generation of power is becoming more common. In the same vein, the International Electrotechnical Commission (IEC) came up with the IEC 62443 framework, which concerns the security of industrial automation and control systems. Since the SCADA systems are under its coverage, the standard can be very relevant to utilities, offering structured methods of access control and system hardening, and overall risk management.

In North America, the North American Electric Reliability Corporation (NERC) has developed Critical Infrastructure Protection (CIP) standards that are an obligatory standard to bulk power system operators. These standards deal with broad scope issues like personnel security training, physical security of critical facilities and incident reporting. By rendering this requirements enforceable, NERC can make sure that those utilities that operate in the same interconnected system are following at least a minimum standard of security practices, and therefore minimizing vulnerabilities on a collective basis. Governments also are core drivers of regulatory environments. A large number of countries have officially accepted smart grids as vital infrastructure, which is directly connected to the national security agenda. The European Union has given orders to protect the crucial energy networks, and the United States has introduced the NIST Cybersecurity Framework specifically adapted to the energy systems. Nevertheless, the level of enforcement and compliance needs in different countries are different.

Other states use legally binding requirements and penalties on non-adherence to suit, but others depend on voluntary implementation, which leads to unequal levels of protection.

7. Future Directions

As smart grids continue to evolve, future strategies for securing them are likely to emphasize proactive resilience, technological innovation, and a human-centered approach. Rather than focusing solely on reactive measures or static defenses, the goal is to build adaptive systems capable of anticipating threats and responding dynamically. Emerging technologies and evolving organizational practices are set to play key roles in this transformation.

One promising innovation is blockchain, which offers unique advantages for trust management and data security in decentralized energy systems. By recording transactions on a distributed ledger, blockchain ensures that records are immutable and tamper-proof. This is particularly beneficial in peer-to-peer energy trading platforms, where households equipped with solar panels can sell excess electricity directly to others. Blockchain prevents fraudulent transactions, ensures transparency, and enforces agreements automatically through smart contracts. However, challenges related to scalability and computational overhead remain significant obstacles. For blockchain to be integrated into large-scale grid operations, solutions must be developed to reduce energy consumption and optimize efficiency.

The other growing technology that has enormous potential is the digital twin. A digital twin is a computer simulation of the real physical grid infrastructure, which is updated in real time with measurements of IoT sensors and surveillance systems. Digital twins enable the operator to test a wide range of possibilities, such as cyberattacks, failures of equipment or any other environmental interruptions, in a safe simulated setting. An example of a false data injection attack can be simulated in the twin to determine how it may spread throughout substations so that operators can take preventive actions in the real grid. In addition to enhancing cybersecurity, digital twins offer such benefits as predictive maintenance scheduling, better load forecasting, and simulated training environments to staff. This technology is therefore efficient in terms of operations and preparedness of security.

Even with these technological developments, the most important aspect of the resilience of smart grids is the human factor. Human susceptibility to cyber attacks has been used in many of the most harmful cyber attacks, including phishing emails or inadequate password management. The work of a single negligent or sabotage attack can take down even advanced defenses. In order to overcome it, one needs to engage in a long-term workforce development process, conduct frequent awareness training, and create an organizational culture in which cybersecurity is viewed as a shared responsibility. This requires utilities to integrate cybersecurity in their daily operations by undertaking incident response exercises, open communication channels and continuous professional growth. The interactive networks that unite utilities, policymakers and academic researchers are also capable of creating adaptive strategies which change in response to the emerging threat environment.

The combination of blockchain-based trusts with digital twins simulations and human-oriented organizational practices is a paradigm shift in terms of the way smart grids will be secured in the future. These innovations depict that the emphasis has shifted to end-of-island technical solutions being less prioritized and the emphasis is on systemic resilience. With the adept integration of technology vision and human flexibility, the energy sector can be able to foresee threats and react better in case of disruptions. By doing so, the smart grid of the future will be more efficient, sustainable, as well as more secure and resilient to the continuously changing arsenal of cyber and physical attacks.

8. Conclusion

Smart grids are a new breakthrough in the world energy infrastructure, where efficiency, sustainability, and involvement of the consumer can be improved thanks to digitalization and automation. Nevertheless, the combination of the state-of-the-art communication networks and IoT gadgets presents uncharted threats at the intersection of electrical safety and cybersecurity. Cyber intrusion not only causes the disruption of digital processes but also physical threats, such as a massive blackout and

economic setbacks as well as damaged equipment and endangered human life. The paper has also outlined the fact that the protection of smart grids entails a complex process. Intrusion detectors, encryption, and AI-based surveillance are all technical solutions that constitute the core of cybersecurity protection. However, they have to be augmented by regulatory and standardization measures, such as frameworks, e.g., NERC CIP, IEC 62443, and IEEE 2030, where responsibility and uniformity is guaranteed on both national and international levels. The human aspect is also very important: engineers, IT experts, and operators should be provided with interdisciplinary training to counteract the lack of unity between electrical safety and cybersecurity, to have a comprehensive defense posture.

In the future, technologies such as blockchain, digital twins, and AI will be used to empower predictive and preventive, whereas human-centered approaches will help to build resilience by educating and regulating corporate culture. It is not only a technological, but a societal challenge: how to make sure that smart grids, which are considered critical infrastructure across the world, are reliable, secure, and safe. Finally, the security of smart grids is a social necessity because any problems in the electricity infrastructure will impact social security, economic stability, and national security. The development of resilient smart grids should thus be crucial not just in promoting the cause of sustainable energy but also in protecting the pillars of the new epoch.

REFERENCES

Amin, M., & Wollenberg, B. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine, 3*(5), 34–41. https://doi.org/10.1109/MPAE.2005.1507024

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Case, D. U. (2016). *Analysis of the cyber attack on the Ukrainian power grid*. SANS Industrial Control Systems. https://www.sans.org/white-papers/36297/

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials, 14*(4), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087

Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE Access, 8*, 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358

Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. L. P. (2012). A survey of communication/networking in smart grids. *Future Generation Computer Systems, 28*(2), 391–404. https://doi.org/10.1016/j.future.2011.04.014

Güngör, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics, 7*(4), 529–539. https://doi.org/10.1109/TII.2011.2166794

He, H., & Yan, J. (2016). Cyber-physical attacks and defenses in the smart grid: A survey. *IEEE Transactions on Smart Grid, 7*(1), 281–299. https://doi.org/10.1109/TSG.2015.2424856

IEC. (2018). *IEC 62443: Industrial communication networks – Network and system security*. International Electrotechnical Commission. https://webstore.iec.ch/publication/34421

IEEE. (2011). *IEEE 2030: Guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS)*. Institute of Electrical and Electronics Engineers. https://standards.ieee.org/standard/2030-2011.html

Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security & Privacy, 8*(1), 81–85. https://doi.org/10.1109/MSP.2010.49

Liu, Y., Ning, P., & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. ACM *Transactions on Information and System Security, 14*(1), 1–33. https://doi.org/10.1145/1952982.1952995

Madani, V., Novosel, D., & Bose, A. (2016). Smart grid protection issues. In J. Momoh (Ed.), *Smart grid: Fundamentals of design and analysis* (pp. 277–304). Wiley-IEEE Press. https://doi.org/10.1002/9781118491311.ch11

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

Mousavi, S. M., & Valenzuela, J. (2021). Machine learning for cybersecurity in smart grids: A comprehensive review. *Energies, 14*(17), 5465. https://doi.org/10.3390/en14175465

NERC. (2023). *Critical Infrastructure Protection (CIP) standards*. North American Electric Reliability Corporation. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Patel, S. C., Taghavi, M., & Bakhtiyari, K. (2020). Insider threat mitigation in smart grids: Challenges and opportunities. *Computers & Security, 96*, 101915. https://doi.org/10.1016/j.cose.2020.101915

Sharma, P. K., & Sood, S. K. (2011). A secure and efficient system for smart grid communication. *International Journal of Electrical Power & Energy Systems, 33*(10), 1721–1727. https://doi.org/10.1016/j.ijepes.2011.05.033

Zhang, H., Liu, J., & Xie, L. (2022). Cybersecurity and resilience in smart grids: A review of challenges and solutions. *IEEE Transactions on Smart Grid, 13*(1), 5–17. https://doi.org/10.1109/TSG.2021.3108335

Zhou, Q., Wang, S., Yang, F., & Liu, Y. (2020). Applications of artificial intelligence in power system operation and control. *CSEE Journal of Power and Energy Systems, 6*(2), 344–352. https://doi.org/10.17775/CSEEJPES.2019.02520