ISP
Innovative Science Publishers

IESJ
Innovative Engineering Sciences Journal

Adapting to Change: Analyzing Dynamic System Variations and Cyber Security in Smart Grids

Hiroshi Tanaka
Rising Sun University, Japan

Abstract

This paper encompasses a multifaceted exploration of the intricate interplay between evolving system dynamics and the imperative of fortifying cyber defenses within smart grid infrastructures. In this abstract realm, researchers delve into the complexities of dynamic system variations, elucidating how these fluctuations influence the operational landscape of smart grids. Concurrently, the discourse extends to the critical domain of cyber security, where the constant evolution of threats necessitates agile strategies for safeguarding against potential vulnerabilities. Through a comprehensive analysis, this abstract seeks to illuminate the synergistic relationship between adaptive system resilience and robust cyber security protocols, offering invaluable insights crucial for the sustainable advancement of smart grid technologies.

Keywords: Adapting to Change, Dynamic System Variations, Cyber Security, Smart Grids, Energy Infrastructure

1. Introduction

Smart grids represent a transformative leap in energy management, promising enhanced efficiency, reliability, and sustainability[1]. However, with this innovation comes the challenge of adapting to the dynamic nature of energy systems and ensuring robust cyber security measures. This paper explores the critical nexus of dynamic system variations and cyber security in smart grids [2]. As the energy landscape evolves, understanding and managing dynamic system variations become paramount [3, 4]. From fluctuating energy demand to variable renewable energy sources, smart grids must dynamically adjust to maintain stability and efficiency. Concurrently, cyber threats pose significant risks to the integrity and reliability of smart grid operations [5]. As such, this paper delves into the complexities of adapting to change in smart grids, analyzing dynamic system variations and cyber security measures essential for the resilience and viability of modern energy infrastructure [6]. Through comprehensive examination and strategic insights, this paper aims to provide a framework for navigating the evolving landscape of smart grids, ensuring sustainable energy management in an era of constant change and digital interconnectedness [7].

Adaptation is paramount in smart grids due to the dynamic nature of energy systems and the evolving challenges they face. Several factors underscore the significance of adaptation [8]. Fluctuating Energy Demand: Smart grids must adapt to the unpredictable nature of energy demand, which varies based on factors like time of day, weather conditions, and societal patterns. By dynamically adjusting energy distribution and consumption, smart grids can optimize resource utilization and minimize wastage [9]. Variable Renewable Energy Sources: The increasing integration of renewable energy sources such as solar and wind introduces variability into the grid. Smart grids need to adapt to the intermittent nature of these sources by implementing forecasting tools, energy storage solutions, and grid management strategies to ensure stability and reliability [10, 11]. Grid Resilience: Smart grids face various threats, including natural disasters, cyber-attacks, and equipment failures. Adaptation involves implementing resilience measures such as redundancy, grid hardening, and rapid response protocols to mitigate disruptions and ensure continuity of service[12]. Technological Advancements: The rapid pace of technological innovation presents both opportunities and challenges for smart grids [13]. Adaptation involves staying abreast of emerging technologies such as artificial intelligence, the Internet of Things (IoT), and blockchain, and leveraging them to enhance grid efficiency, security, and flexibility. Regulatory and Policy Changes: Regulatory frameworks and policy directives evolve in response to changing societal needs, environmental concerns, and technological advancements [14]. Smart grids must adapt to these changes by complying with regulations, incorporating new standards, and advocating for supportive policies that foster innovation and sustainability. In summary, adaptation is essential for smart grids to effectively address the dynamic and multifaceted challenges inherent in modern energy systems [15, 16]. By embracing flexibility, innovation, and resilience, smart grids can optimize performance, enhance reliability, and contribute to a more sustainable and secure energy future [17].

Dynamic system variations and cyber security are of paramount significance in the context of smart grids due to their profound impact on grid stability, reliability, and resilience [18]. Dynamic System Variations: Dynamic variations in energy demand, supply, and grid conditions can jeopardize grid stability, leading to voltage fluctuations, frequency deviations, and even blackouts. Understanding and managing these variations are essential for ensuring the smooth operation of smart grids [19]. Resource Optimization: By analyzing dynamic system variations, smart grids can optimize the utilization of resources such as generation capacity, energy storage, and transmission infrastructure [20, 21]. This enables efficient allocation of resources in response to changing demand patterns and grid conditions [22]. Operational Efficiency: Adaptation to dynamic system variations enhances operational efficiency by minimizing energy losses, reducing peak demand, and improving load balancing [23]. This results in cost savings, improved grid performance, and enhanced customer satisfaction. Cyber Security: Smart grids are vulnerable to a wide range of cyber threats, including malware, ransomware, and insider attacks [24]. Cyber security is crucial for protecting critical infrastructure, safeguarding sensitive data, and ensuring the integrity and reliability of grid operations [25]. Smart grids generate vast amounts of data related to energy consumption, grid performance, and consumer behavior. Robust cyber security measures are essential for preserving data privacy, preventing unauthorized access, and maintaining consumer trust [26]. Resilience against Attacks: Cyber security measures such as encryption, intrusion detection systems, and incident response protocols enhance the resilience of smart grids against cyber-attacks. Timely detection and mitigation of threats are critical for minimizing the impact of cyber incidents and ensuring continuity of service [27]. In summary, dynamic system variations and cyber security are intricately linked and play a crucial role in shaping the reliability, resilience, and sustainability of smart grids [28]. By effectively analyzing dynamic system variations and implementing robust cybersecurity measures, smart grids can mitigate risks, optimize performance, and contribute to a more secure and efficient energy infrastructure [29].

1.1. Background and History

The background and history of this paper reflect the evolution of energy infrastructure and the growing importance of cybersecurity in modern power systems [30, 31]. The concept of a smart grid emerged as a response to the need for modernizing traditional power grids to address emerging challenges such as increasing demand, integration of renewable energy sources, and improving overall efficiency [32]. Smart grids leverage advanced technologies, including digital communication, automation, and sensing, to enable more efficient, reliable, and sustainable energy delivery [33]. The development of smart grids can be traced back to the late 20th century, with early initiatives focused on improving grid monitoring and control [34, 35]. However, significant advancements in communication and computing technologies in the early 21st century propelled the smart grid concept forward, leading to widespread research and deployment efforts globally[36]. In the early stages, the emphasis was primarily on enhancing grid reliability, reducing energy losses, and facilitating the integration of renewable energy sources such as solar and wind power. As smart grid deployments expanded, so did concerns about cybersecurity [37]. The increasing digitization and interconnectedness of grid components introduced new vulnerabilities, making smart grids potential targets for cyber-attacks [38, 39].

The history of adapting to dynamic system variations and cybersecurity in smart grids is characterized by ongoing research, technological innovations, and regulatory efforts [40]. Researchers and industry practitioners have been actively investigating methods to analyze and adapt to dynamic variations in grid operation, including load fluctuations, renewable energy intermittency, and equipment failures [41]. Cybersecurity in smart grids has become a critical area of focus. Cyber-attacks targeting power systems can have severe consequences, including disruptions to energy supply, financial losses, and threats to public safety. Recognizing these risks, governments, regulatory bodies, and industry stakeholders have collaborated to develop standards, guidelines, and best practices for enhancing grid cybersecurity[42, 43]. The history of this paper likely involves a timeline of research and development efforts aimed at understanding and mitigating the impacts of dynamic variations and cyber threats on smart grid operation. This work likely builds upon previous studies in grid resilience, cybersecurity, and system analysis, offering insights and solutions tailored to the evolving challenges faced by modern power systems [44].

1.2. Related work

The Related works of this paper Cyber-Physical Security in Smart Grids: Survey and Challenges by Yasser M. Alginahi, Hussein T. Mouftah (2016): This paper provides an extensive survey of cyber-physical security challenges in smart grids and proposes various solutions to address them. Dynamic Security Assessment and Control of Smart Grids: Algorithms and Implementation by Reza Arghandeh, Hamed Mohsenian-Rad, Alberto Del Rosso, and Adam Wierman (2017): This work focuses on developing algorithms and methodologies for dynamic security assessment and control in smart grids to handle variations and cyber threats[45]. Adaptive Protection Strategies for Cyber-Physical Attacks on Power Grids by Aron Laszka, Yevgeniy Vorobeychik (2015): This paper investigates adaptive protection strategies against cyber-physical attacks in power grids, considering the dynamic nature of system variations and potential cyber threats. Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey by Siddharth Sridhar, Lingyu Wang, Sajal K. Das (2016): This survey paper provides an overview of cyber-physical attacks and defense mechanisms in smart grids, highlighting the need for adaptive strategies to cope with dynamic system variations. Resilient Control Systems: Next Generation Design Research for Adaptive Cyber-Physical Systems by Robert F. Jeffers, Todd R. Andel, et al. (2017): This work explores the concept of resilient control systems for adaptive cyber-physical systems, emphasizing the importance of resilience against cyber threats and system variations in smart grids [46]. These related works contribute to the understanding of adapting to change and addressing cyber security concerns in smart grids, providing insights into various methodologies, algorithms, and strategies to enhance the resilience and security of these systems.

2. Dynamic System Variations in Smart Grids

Dynamic System Variations in Smart Grids refer to the changes, fluctuations, and dynamic behaviors that occur within the components and operations of a smart grid over time. These variations encompass a range of factors, including fluctuations in energy demand, supply from renewable sources, grid conditions, and environmental factors[47]. In a smart grid context, dynamic system variations are influenced by factors such as changes in consumer behavior, weather patterns affecting renewable energy generation, and the integration of new technologies and distributed energy resources. Understanding and analyzing these variations is crucial for effectively managing and optimizing the performance, reliability, and efficiency of smart grid systems. Dynamic system variations introduce a host of challenges across various domains, complicating the management and optimization of complex systems [48]. One significant challenge lies in predictive modeling, where the inherent complexity and nonlinear dynamics of systems make accurate forecasting difficult. Variations in system behavior, influenced by a multitude of interconnected factors, often lead to uncertainty and unpredictability [49]. Developing robust predictive models that can effectively capture and account for these variations is essential but requires sophisticated mathematical techniques and computational resources to navigate the intricacies of dynamic systems accurately [50].

Figure 1 illustrates the Dynamic System Variation Performance Assessment Framework offers a structured approach to evaluating the effectiveness of strategies employed to manage dynamic variations within complex systems [51]. By analyzing system behavior over time, this framework provides insights into the system's adaptability, resilience, and performance under changing conditions [52]. Utilizing quantitative metrics and qualitative observations, the framework assesses the impact of dynamic variations on system stability, efficiency, and reliability [53]. Through comprehensive analysis, it identifies areas of improvement and informs decision-making processes aimed at enhancing system performance and mitigating risks associated with dynamic variations[54]. By incorporating feedback loops and iterative improvements, the framework enables continuous optimization of system responses to dynamic changes, fostering adaptive and robust system behavior [55].

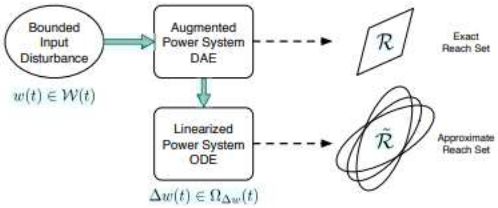

Figure 1: Dynamic System Variation performance assessment framework

Another critical challenge posed by dynamic system variations is risk management [56]. Fluctuations in system dynamics can introduce risks such as sudden disruptions, cascading failures, and emergent behaviors [57]. Identifying and mitigating these risks demands proactive risk management strategies that anticipate potential vulnerabilities and disturbances within the system. This necessitates the implementation of scenario analysis, stress testing, and contingency planning to prepare for various eventualities, ensuring the resilience and reliability of systems in the face of dynamic variations [58]. Resource allocation presents yet another challenge in the context of dynamic system variations. Variations in system demand, supply, and performance can significantly impact the allocation and utilization of resources [59, 60]. Balancing resource allocation to meet fluctuating demands while maintaining efficiency and reliability requires sophisticated optimization strategies [61]. Dynamic resource allocation mechanisms that can adapt to changing conditions in real time are crucial for optimizing system performance and minimizing waste, addressing the ongoing challenge of managing resources effectively amidst dynamic system variations [62].

2.1. Grid stability

Grid stability is a cornerstone of modern electrical power systems, ensuring the reliable and uninterrupted delivery of electricity to consumers [63]. It encompasses the ability of the grid to maintain equilibrium despite fluctuations in demand, supply, and other external factors. Achieving grid stability requires careful coordination of generation, transmission, and distribution assets, as well as advanced monitoring and control technologies to detect and respond to dynamic changes in real time [64]. Grid operators utilize automatic generation control (AGC) systems to adjust generator output in response to frequency variations, ensuring that generation matches demand and maintaining grid stability [65]. Additionally, voltage control mechanisms play a vital role in stabilizing the grid by maintaining voltage levels within acceptable limits. Voltage regulators, capacitors, and other devices are deployed strategically throughout the grid to manage voltage fluctuations and ensure the proper functioning of electrical equipment [66].

2.2. Cyber Security in Smart Grids

Cyber security in smart grids is paramount due to the increasing digitization and interconnectedness of critical infrastructure [67]. Smart grids leverage advanced communication and control technologies to enhance efficiency and reliability, but they also introduce new vulnerabilities and risks. Protecting smart grids from cyber threats is essential to ensure the integrity, reliability, and security of the energy infrastructure [68]. Cyber security in smart grids encompasses a range of measures aimed at safeguarding against unauthorized access, malicious attacks, and data breaches. Smart grid cyber security is the protection of grid control systems from cyber threats [69]. These systems, including Supervisory Control and Data Acquisition (SCADA) systems and Energy Management Systems (EMS), are responsible for monitoring and controlling grid operations. Securing these systems against cyber-attacks is critical to prevent unauthorized access, manipulation of operational data, or disruption of grid operations[70, 71]. Measures such as network segmentation, access controls, encryption, and intrusion detection systems are employed to mitigate the risk of cyber-attacks on grid control systems. Ensuring the security of communication networks and devices within the smart grid infrastructure is essential for cyber security [72]. Smart grids rely on communication networks to transmit data between grid components, sensors, and control systems. Securing these networks against cyber threats, such as eavesdropping, spoofing, or denial-of-service attacks, is crucial to maintaining the confidentiality, integrity, and availability of data and communications. Implementing secure communication protocols, network monitoring tools, and authentication mechanisms can help mitigate the risk of cyber-attacks on smart grid communication networks [73]. Cyber security in smart grids requires a multi-layered approach that addresses vulnerabilities at the system, network, and device levels to ensure the resilience and reliability of the energy infrastructure in the face of evolving cyber threats.

3. PROTOCOL VULNERABILITIES IN THE THREE STAGES OF A CYBER ATTACK

3.1. STAGE I: INTERCEPTION AND INVASION

During Stage I, the attacker's activities are designed to infiltrate the system or intercept data without disrupting the normal operation of the power grid [74]. The primary objective at this stage is to exploit vulnerabilities in communication protocols to gain unauthorized access or intercept signals from communicating devices within the cyber system[75]. Consequently, the most critical vulnerabilities in this phase are as follows.

- Authentication vulnerabilities arise due to weaknesses in the protocol's authentication mechanism, allowing attackers to establish an access channel without concealing their identity.
- Encryption vulnerabilities are significant as the communication messages lack sufficient protection against leakage within the protocol[76]. This means that if the communication signal is intercepted, attackers can extract data between communication devices without needing to decrypt the encrypted data[77].

3.2. STAGE II: PREPARING FOR AN ATTACK

After establishing an access channel, the attacker proceeds to orchestrate sabotage operations within the cyber system to fulfill malicious objectives. At this stage, specific protocol vulnerabilities become notably prominent[78].

- Authorization management vulnerabilities are significant, indicating that a communication protocol lacks robust supervision over visitor behavior within the system. By exploiting this weakness, attackers can extend their operations within the cyber system without encountering significant impediments [79].

3.3. STAGE III: LAUCHING AN ATTACK

From the perspective of the attack's impact, the potential intentions of the attacker can be categorized into three distinct objectives: compromising the integrity of the data received by the system, jeopardizing the availability of system equipment, or compromising the privacy of system data [80]. In this stage, protocol vulnerabilities associated with these three categories are as follows.

- Confidentiality protection vulnerabilities provide attackers with the means to access private information unlawfully and pilfer large volumes of data.
- Integrity protection vulnerabilities enable the transmission of packets containing falsified or incomplete data to and from the system via vulnerable protocols.
- Availability protection vulnerabilities empower attackers to manipulate parameters or other devices, leading to loss of control or malfunction of the affected devices.

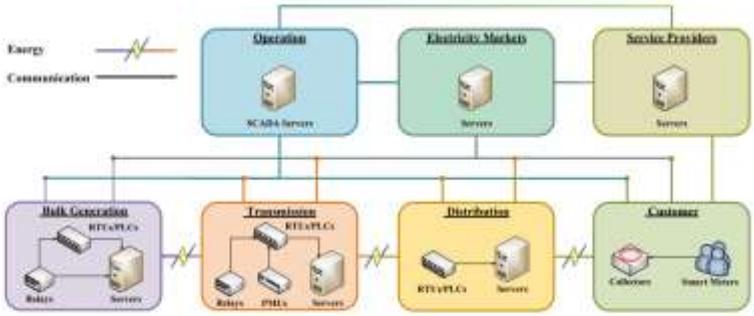

Figure 2: Potential affected components by cyber-attacks in a power grid.

4. Potential Affected Components by Cyber Attacks in Power Grid

Figure 2 provides an illustrative depiction of various common and representative points within the power grid susceptible to cyber-attacks, aiding in the identification of vulnerabilities [81, 82]. The figure illustrates the communication networks utilized for inter-subsystem communication across seven domains. Within these domains, several components are vulnerable to cyber-attacks:

- Protective relays, situated primarily within bulk generation systems and the transmission network, serve as secondary protection devices, controlling circuit operations by detecting changes in electrical signals. These relays rely on the IEC61850/Modbus communication protocol to receive real-time commands dictating their actions.
- Remote Terminal Units (RTUs) and Power Line Communication (PLC) devices are prevalent in power plants, transmission, and distribution networks, stationed at remote sites to monitor, measure, and control field devices[83]. These components utilize Modbus and DNP3 protocols for communication with other devices.
- Phasor Measurement Units (PMUs) conduct synchronous phasor measurements and dynamic recordings based on a standard clock signal within the transmission system. The communication standard IEEE 37.118 is instrumental in synchronizing data exchange processes among PMUs [84].

- Smart meters, serving as contemporary client-side information collection devices with bi-directional communication capabilities, rely heavily on the Modbus communication protocol.
- Servers within each domain interface with SCADA systems in operational and market contexts through a myriad of communication channels, including WANs, Internet, LAN, and FAN. This diverse array of communication pathways encompasses numerous complex protocols, adding to the intricacy of communication within the power grid infrastructure[85].

5. Vulnerabilities in Smart Grid Infrastructure:

Smart grid infrastructure is vulnerable to a range of cyber threats due to its reliance on interconnected technologies and communication networks. Identifying and understanding these vulnerabilities is crucial for implementing effective security measures to protect against potential cyber-attacks and breaches. Several key vulnerabilities in smart grid infrastructure include: Many smart grid components, such as SCADA systems and field devices, are built on legacy technologies that may lack built-in security features and are not easily upgradable [86]. These legacy systems often have known vulnerabilities that can be exploited by attackers to gain unauthorized access to critical infrastructure and disrupt grid operations. Insecure Communication Protocols: Smart grids rely on communication networks to transmit data between grid components, sensors, and control systems[87]. However, many of these communication protocols were not designed with security in mind and may be susceptible to interception, tampering, or manipulation by attackers. Insecure communication protocols can compromise the confidentiality, integrity, and availability of data within the smart grid infrastructure. Insufficient Authentication and Access Controls: Weak authentication mechanisms and inadequate access controls can make it easier for attackers to gain unauthorized access to smart grid infrastructure. For example, default or easily guessable passwords on network devices or control systems can provide attackers with a foothold to launch further attacks. Insufficient access controls may also allow attackers to escalate privileges and gain control over critical infrastructure components[88].

In Figure 3, the middle curve corresponds to the nominal trajectory obtained by setting a certain value for a parameter (rad/s) of $\omega(t_0)$ = rad /s, while all other states remain at their equilibrium values. This procedure was repeated for different parameter values, resulting in approximate trajectories. The calculated error points, depicted as stars, closely align with a quartic polynomial, indicating significant curvature compared to the previous case [89]. This suggests that the nominal trajectory is strongly influenced by nonlinearities, particularly as it passes closer to an unstable equilibrium point. The upper curve in Figure 3 represents a nominal trajectory for $\Delta\omega(t_0)$ taking values of $-0.5, -1.0, -1.5, \dots, -6.0$. with a different parameter value, again with all other states initially at their equilibrium values. Error points, represented as diamonds, also follow a quartic polynomial with increased curvature compared to the previous scenario. This trajectory also passes closer to the unstable equilibrium point, indicating heightened nonlinear effects. Despite relatively large perturbations, all three cases yield good approximations [90].

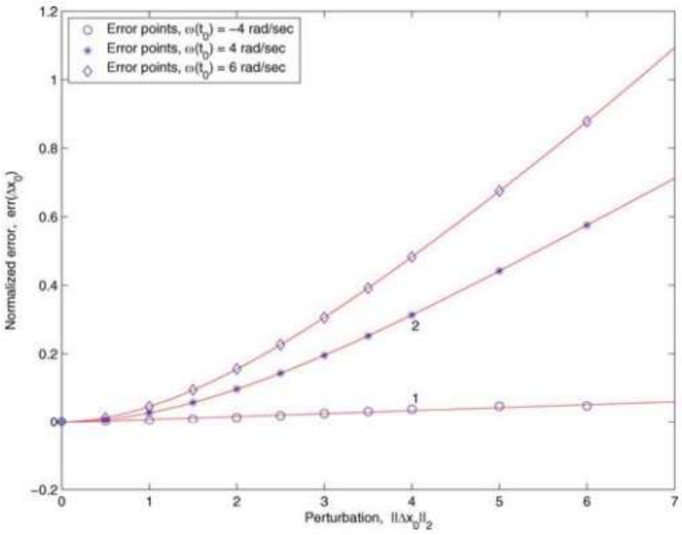

Figure 3: Error variation with perturbation size.

Figure 3 provides further insight. At point 1, most states are at equilibrium except for one, resulting in an almost constant trajectory [91]. A trajectory synthesized for this condition closely follows the nominal trajectory, indicating accurate approximation. At point 2, equilibrium conditions are again present, but the approximation to equilibrium is less accurate. However, the negated sensitivity term tracks the nominal trajectory closely, albeit with a slight phase shift, which induces the error observed in the approximate trajectory [92].

The supply chain for smart grid components, including hardware, software, and firmware, has vulnerabilities in the infrastructure [93]. Malicious actors may exploit vulnerabilities in third-party components or compromise the supply chain to introduce backdoors or malicious code into smart grid devices. Supply chain risks pose a significant challenge to ensuring the integrity and security of smart grid infrastructure. Smart grid infrastructure often consists of a diverse range of devices and software components from multiple vendors, making it challenging to ensure timely security updates and patches [94]. Failure to apply security updates and patches promptly leaves smart grid infrastructure vulnerable to known vulnerabilities that attackers can exploit to compromise system security [95]. Addressing these vulnerabilities requires a multi-layered approach to smart grid security, including implementing robust authentication and access controls, securing communication networks, regularly updating and patching systems, and conducting regular security assessments and audits. By addressing these vulnerabilities and implementing effective security measures, smart grid operators can enhance the resilience and reliability of the energy infrastructure in the face of evolving cyber threats [96].

Table 1 illustrates the vulnerabilities associated with protocols used in power grids. It highlights weaknesses such as inadequate authentication and encryption in Modbus and DNP3 protocols, leaving them susceptible to unauthorized access and data manipulation [97]. Additionally, the figure underscores the vulnerability of IEC 61850 due to weak encryption, potentially leading to unauthorized access and data interception. Furthermore, it addresses the susceptibility of wireless protocols like IEEE 802.11 (Wi-Fi) and Zigbee to various attacks, including network intrusion and compromise. Lastly, it mentions the vulnerabilities of TCP/IP, including its susceptibility to IP spoofing, which can result in denial of service attacks and data interception[98, 99].

Table 1: Protocol vulnerabilities in power grids

Protocol	**Vulnerability**	**Potential Impact**
Modbus	Lack of authentication and encryption	Unauthorized access, data manipulation
DNP3	Limited authentication mechanisms	Data spoofing, unauthorized control
IEC 61850	Weak encryption and authentication	Unauthorized access, data interception
IEEE 802.11 (Wi-Fi)	Vulnerable to attacks like KRACK, Rogue APs	Network intrusion, data interception
Zigbee	Lack of proper security measures	Network compromise, unauthorized access
TCP/IP	Vulnerable to various attacks like IP spoofing	Denial of service, data interception

6. Future Directions

The future direction for adapting to change, analyzing dynamic system variations, and enhancing cybersecurity in smart grids will involve a multidisciplinary approach encompassing advanced technologies and comprehensive risk management strategies. This approach will prioritize the development of adaptive control systems capable of autonomously adjusting to fluctuating grid conditions while maintaining resilience against cyber threats [100]. Integration of artificial intelligence and machine learning algorithms will play a pivotal role in enabling predictive analytics for proactive maintenance and anomaly detection. Moreover, future efforts will focus on implementing decentralized architectures and blockchain technologies to enhance data integrity and mitigate the impact of cyberattacks. Collaborative research initiatives between academia, industry, and government stakeholders will be crucial in addressing the evolving challenges and ensuring the reliability, security, and sustainability of smart grid infrastructures in the years to come.

7. Conclusion

In conclusion, this paper presents a holistic understanding of the challenges and opportunities inherent in modern energy infrastructure. Through a multifaceted exploration of dynamic system variations and cyber security measures, the paper underscores the critical importance of adaptability and resilience in ensuring the reliability and security of smart grid operations. By elucidating the synergistic relationship between evolving system dynamics and robust cyber defenses, the paper offers invaluable insights that are indispensable for navigating the complexities of smart grid technologies. Looking ahead, the paper advocates for a multidisciplinary approach that integrates advanced technologies and collaborative research initiatives to address the evolving challenges and ensure the sustainability of smart grid infrastructures. Ultimately, this paper serves as a comprehensive guide for stakeholders in the energy sector, providing strategic insights crucial for driving sustainable advancement and innovation in smart grid technologies.

Reference

[1] H. M. Khalid *et al.*, "WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Systems Journal,* 2023.

[2] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research,* vol. 215, p. 108975, 2023.

[3] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 303-314.

[4] M. Z. Gunduz and R. Das, "Cyber-security on the smart grid: Threats and potential solutions," *Computer networks,* vol. 169, p. 107094, 2020.

[5] H. Khalid, F. Flitti, M. Mahmoud, M. Hamdan, S. Muyeen, and Z. Dong, "WAMS Operations in Modern Power Grids: A Median Regression Function-Based State Estimation Approach Towards Cyber Attacks," *El-Sevier–Sustainable Energy, Grid, and Networks,* vol. 34, p. 101009, 2023.

[6] J. A. Momoh, *Smart grid: fundamentals of design and analysis*. John Wiley & Sons, 2012.

[7] T. Baumeister, "Literature review on smart grid cyber security," *Collaborative Software Development Laboratory at the University of Hawaii,* vol. 650, 2010.

[8] H. Khalid, S. Muyeen, and I. Kamwa, "Excitation Control for Multi-Area Power Systems: An Improved Decentralized Finite-Time Approach," *El-Sevier–Sustainable Energy, Grid, and Networks,* vol. 31, p. 100692, 2022.

[9] X. Yu and Y. Xue, "Smart grids: A cyber-physical systems perspective," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1058-1070, 2016.

[10] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid,* vol. 9, no. 4, pp. 2862-2872, 2016.

[11] Z. Shi *et al.*, "Artificial intelligence techniques for stability analysis and control in smart grids: Methodologies, applications, challenges, and future directions," *Applied Energy,* vol. 278, p. 115733, 2020.

[12] H. M. Khalid, F. Flitti, S. Muyeen, M. S. Elmoursi, O. S. Tha'er, and X. Yu, "Parameter estimation of vehicle batteries in V2G systems: An exogenous function-based approach," *IEEE Transactions on Industrial Electronics,* vol. 69, no. 9, pp. 9535-9546, 2021.

[13] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 1205-1215, 2016.

[14] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 782-795, 2011.

[15] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access,* vol. 8, pp. 87592-87608, 2020.

[16] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and prospects," *Electronics,* vol. 11, no. 9, p. 1502, 2022.

[17] M. Bollen, *The smart grid: Adapting the power system to new challenges*. Morgan & Claypool Publishers, 2011.

[18] A. V. Jha *et al.*, "Smart grid cyber-physical systems: communication technologies, standards, and challenges," *Wireless Networks,* vol. 27, no. 4, pp. 2595-2613, 2021.

[19] B. Schäfer, M. Matthiae, M. Timme, and D. Witthaut, "Decentral smart grid control," *New Journal of Physics,* vol. 17, no. 1, p. 015002, 2015.

[20] Z. Rafique, H. M. Khalid, S. Muyeen, and I. Kamwa, "Bibliographic review on power system oscillations damping: An era of conventional grids and renewable energy integration," *International Journal of Electrical Power & Energy Systems,* vol. 136, p. 107556, 2022.

[21] J. A. Momoh, "Smart grid design for efficient and flexible power networks operation and control," in *2009 IEEE/PES Power Systems Conference and Exposition*, 2009: IEEE, pp. 1-8.

[22] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *Ieee Access,* vol. 7, pp. 80778-80788, 2019.

[23] S. M. Amin, "Smart grid: Overview, issues and opportunities. advances and challenges in sensing, modeling, simulation, optimization, and control," *European Journal of Control,* vol. 17, no. 5-6, pp. 547-567, 2011.

[24] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways," *Sensors,* vol. 21, no. 19, p. 6415, 2021.

[25] S. Howell, Y. Rezgui, J.-L. Hippolyte, B. Jayan, and H. Li, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources," *Renewable and Sustainable Energy Reviews,* vol. 77, pp. 193-214, 2017.

[26] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid,* vol. 9, no. 1, pp. 163-178, 2016.

[27] H. Qi *et al.*, "A resilient real-time system design for a secure and reconfigurable power grid," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 770-781, 2011.

[28] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyber-physical infrastructures in power systems: architectures and vulnerabilities*. Academic Press, 2021.

[29] S. R. Salkuti and D. Gautam, "Advancements in the Integration of Renewable Energy and Energy Storage Technologies into Smart Grid."

[30] M. Q. Taha, "Advantages and recent advances of smart energy grid," *Bulletin of Electrical Engineering and Informatics,* vol. 9, no. 5, pp. 1739-1746, 2020.

[31] Z. Rafique, H. M. Khalid, and S. Muyeen, "Communication systems in distributed generation: A bibliographical review and frameworks," *IEEE Access,* vol. 8, pp. 207226-207239, 2020.

[32] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of IoT-based load altering attacks against power grids using the theory of second-order dynamical systems," *IEEE Transactions on Smart Grid,* vol. 12, no. 5, pp. 4415-4425, 2021.

[33] Z. A. Baig and A.-R. Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures," *J. Commun.,* vol. 8, no. 8, pp. 473-479, 2013.

[34] S. Jahan and R. Habiba, "An analysis of smart grid communication infrastructure & cyber security in smart grid," in *2015 International Conference on Advances in Electrical Engineering (ICAEE)*, 2015: IEEE, pp. 190-193.

[35] O. A. Omitaomu and H. Niu, "Artificial intelligence techniques in smart grid: A survey," *Smart Cities,* vol. 4, no. 2, pp. 548-568, 2021.

[36] H. M. Khalid and J. C.-H. Peng, "Bidirectional charging in V2G systems: An in-cell variation analysis of vehicle batteries," *IEEE Systems Journal,* vol. 14, no. 3, pp. 3665-3675, 2020.

[37] M. Ceci, R. Corizzo, N. Japkowicz, P. Mignone, and G. Pio, "Echad: embedding-based change detection from multivariate time series in smart grids," *IEEE Access,* vol. 8, pp. 156053-156066, 2020.

[38] V. Arzamasov, K. Böhm, and P. Jochem, "Towards concise models of grid stability," in *2018 IEEE International Conference on Communications, control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018: IEEE, pp. 1-6.

[39] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat Analysis of black energy malware for synchrophasor based real-time control and monitoring in smart grid," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016*, 2016: BCS Learning & Development.

[40] H. M. Khalid, S. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Systems Journal,* vol. 14, no. 2, pp. 2054-2065, 2019.

[41] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications surveys & tutorials,* vol. 14, no. 4, pp. 981-997, 2012.

[42] F. Li *et al.*, "Smart transmission grid: Vision and framework," *IEEE Transactions on Smart Grid,* vol. 1, no. 2, pp. 168-177, 2010.

[43] A. S. Musleh, H. M. Khalid, S. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Systems Journal,* vol. 13, no. 1, pp. 710-719, 2017.

[44] U. Adhikari, T. H. Morris, and S. Pan, "Applying hoeffding adaptive trees for real-time cyber-power event and intrusion classification," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4049-4060, 2017.

[45] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 49, no. 8, pp. 1554-1569, 2019.

[46] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 210-224, 2011.

[47] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 697-707, 2015.

[48] H. Wang *et al.*, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 11, pp. 4766-4778, 2018.

[49] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big data analysis-based security situational awareness for smart grid," *IEEE Transactions on Big Data,* vol. 4, no. 3, pp. 408-417, 2016.

[50] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, pp. 2026-2037, 2016.

[51] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *Ieee Access,* vol. 7, pp. 13960-13988, 2019.

[52] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on the cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications,* vol. 209, p. 103540, 2023.

[53] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection, and control in a smart grid environment," *Journal of Advanced Research,* vol. 5, no. 4, pp. 481-489, 2014.

[54] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer networks,* vol. 55, no. 15, pp. 3604-3629, 2011.

[55] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks,* vol. 57, no. 5, pp. 1344-1371, 2013.

[56] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 1, pp. 200-210, 2016.

[57] H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Transactions on Power Systems,* vol. 30, no. 2, pp. 680-688, 2014.

[58] J. J. Moreno Escobar, O. Morales Matamoros, R. Tejeida Padilla, I. Lina Reyes, and H. Quintana Espinosa, "A comprehensive review on smart grids: Challenges and opportunities," *Sensors,* vol. 21, no. 21, p. 6978, 2021.

[59] S. Luthra, S. Kumar, R. Kharb, M. F. Ansari, and S. Shimmi, "Adoption of smart grid technologies: An analysis of interactions among barriers," *Renewable and Sustainable Energy Reviews,* vol. 33, pp. 554-565, 2014.

[60] C. Clastres, "Smart grids: Another step towards competition, energy security, and climate change objectives," *Energy Policy,* vol. 39, no. 9, pp. 5399-5408, 2011.

[61] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, 2019, vol. 1: IEEE, pp. 2958-2963.

[62] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity

attacks under concept drift," *International Journal of Electrical Power & Energy Systems,* vol. 119, p. 105947, 2020.

[63] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access,* vol. 8, pp. 151019-151064, 2020.

[64] A. S. Musleh, S. Muyeen, A. Al-Durra, and H. M. Khalid, "PMU based wide area voltage control of smart grid: A real-time implementation approach," in *2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia),* 2016: IEEE, pp. 365-370.

[65] W. Hoffman, "AI and the Future of Cyber Competition," *CSET Issue Brief,* pp. 1-35, 2021.

[66] J. Johnson, "The AI-cyber security nexus," in *Artificial intelligence and the future of warfare*: Manchester University Press, 2021, pp. 150-167.

[67] E. D. Knapp and R. Samani, *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes, 2013.

[68] A. Khoukhi and M. H. Khalid, "Hybrid computing techniques for fault detection and isolation, a review," *Computers & Electrical Engineering,* vol. 43, pp. 17-32, 2015.

[69] A. IBRAHIM, "AI Armory: Empowering Cybersecurity Through Machine Learning," 2019.

[70] I. Darwish, O. Igbe, and T. Saadawi, "Vulnerability assessment and experimentation of smart grid DNP3," *Journal of Cyber Security and Mobility,* pp. 23–54-23–54, 2016.

[71] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 195-209, 2011.

[72] M. S. Mahmoud and H. M. Khalid, "Model prediction-based approach to fault-tolerant control with applications," *Ima Journal of Mathematical Control and Information,* vol. 31, no. 2, pp. 217-244, 2014.

[73] J. Liu, H. Hu, S. S. Yu, and H. Trinh, "Virtual Power Plant with Renewable Energy Sources and Energy Storage Systems for Sustainable Power Grid-Formation, Control Techniques, and Demand Response," *Energies,* vol. 16, no. 9, p. 3705, 2023.

[74] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *arXiv preprint arXiv:1401.3936,* 2014.

[75] M. Mahmoud and H. Khalid, "Bibliographic review on distributed Kalman filtering," *IET Control Theory Appl,* vol. 7, no. 4, pp. 483-501, 2013.

[76] S. Nazir, H. Hamdoun, and J. Alzubi, "Cyber attack challenges and resilience for smart grids," *European Journal of Scientific Research,* 2015.

[77] M. Rege and R. B. K. Mbah, "Machine learning for cyber defense and attack," *Data Analytics,* vol. 2018, p. 83, 2018.

[78] P. Boopathy *et al.*, "Deep learning for intelligent demand response and smart grids: A comprehensive survey," *Computer Science Review,* vol. 51, p. 100617, 2024.

[79] E. Onyema, A. Dinar, S. Ghouali, B. Merabet, R. Merzougui, and M. Feham, "Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications Systems," in *Security and Privacy in Cyberspace*: Springer, 2022, pp. 25-45.

[80] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1389-1407, 2017.

[81] G. Dondossola, F. Garrone, and J. Szanto, "Cyber risk assessment of power control systems—A metrics weighed by attack experiments," in *2011 IEEE Power and Energy Society General Meeting*, 2011: IEEE, pp. 1-9.

[82] A. Alamin, H. M. Khalid, and J. C.-H. Peng, "Power system state estimation based on Iterative Extended Kalman Filtering and bad data detection using the normalized residual test," in *2015 IEEE Power and Energy Conference at Illinois (PECI)*, 2015: IEEE, pp. 1-5.

[83] S. Dutta, S. K. Sahu, S. Dutta, and B. Dey, "Leveraging a micro synchrophasor for fault detection in a renewable-based smart grid—a machine-learned sustainable solution with cyber-attack resiliency," *e-Prime-advances in electrical engineering, electronics and energy,* vol. 2, p. 100090, 2022.

[84] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids," *Energies,* vol. 14, no. 16, p. 4941, 2021.

[85] M. Z. Jahromi, A. A. Jahromi, S. Sanner, D. Kundur, and M. Kassouf, "Cybersecurity enhancement of transformer differential protection using machine learning," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, 2020: IEEE, pp. 1-5.

[86] N. Shah, A. Haque, S. Mateen, M. Amir, A. Hussain, and H. M. Khalid, "Comparative Analysis of Control Algorithms in Isolated Dual Active Bridge for Ultra Fast Charging of Electric Vehicles," in *2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST),* 2024: IEEE, pp. 35-40.

[87] J. Johansson, "Countermeasures Against Coordinated Cyber-Attacks Towards Power Grid Systems: A systematic literature study," 2019.

[88] U. Inayat, M. F. Zia, S. Mahmood, T. Berghout, and M. Benbouzid, "Cybersecurity enhancement of smart grid: Attacks, methods, and prospects," *Electronics,* vol. 11, no. 23, p. 3854, 2022.

[89] A. E. L. Rivas and T. Abrao, "Faults in smart grid systems: Monitoring, detection and classification," *Electric Power Systems Research,* vol. 189, p. 106602, 2020.

[90] M. Z. Khan, A. Haque, A. Malik, M. Amir, F. S. Zahgeer, and H. M. Khalid, "A Critical Review on Control Techniques for Parallel Operated Inverters in Grid Connected and Standalone Mode," in *2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, 2024: IEEE, pp. 66-71.

[91] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica,* vol. 8, no. 2, pp. 319-333, 2021.

[92] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber-physical system testbed for power system security and control," *International Journal of Electrical Power & Energy Systems,* vol. 90, pp. 124-133, 2017.

[93] R. Akella, H. Tang, and B. M. McMillin, "Analysis of information flow security in cyber-physical systems," *International Journal of Critical Infrastructure Protection,* vol. 3, no. 3-4, pp. 157-173, 2010.

[94] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Communications Surveys & tutorials,* vol. 14, no. 4, pp. 944-980, 2011.

[95] H. M. Khalid, A. Khoukhi, and F. M. Al-Sunni, "Fault detection and classification using Kalman filter and genetic neuro-fuzzy systems," in *2011 Annual Meeting of the North American Fuzzy Information Processing Society*, 2011: IEEE, pp. 1-6.

[96] D. B. Avancini, J. J. Rodrigues, S. G. Martins, R. A. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *Journal of cleaner production,* vol. 217, pp. 702-715, 2019.

[97] C. W. Gellings, *The smart grid: enabling energy efficiency and demand response*. River Publishers, 2020.

[98] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *Ieee Access,* vol. 7, pp. 46595-46620, 2019.

[99] A. M. Annaswamy and M. Amin, "Smart Grid Research: Control Systems-IEEE Vision for Smart Grid Controls: 2030 and Beyond," *IEEE Vision for Smart Grid Controls: 2030 and Beyond,* pp. 1-168, 2013.

[100] H. M. Khalid and J. C.-H. Peng, "Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach," *IEEE Transactions on Power Systems,* vol. 31, no. 3, pp. 1799-1808, 2015.