EPH - International Journal Of Science And Engineering

ISSN (Online): 2454-2016
Volume 09 Issue 03 September 2023

DOI:https://doi.org/10.53555/ephijse.v9i3.215

SAFEGUARDING STABILITY: STRATEGIES FOR ADDRESSING DYNAMIC SYSTEM VARIATIONS IN POWER GRID CYBERSECURITY

Guzman Erick[1*], Fatehi Navid[2]

[1*,2]*University of Toronto, Canada*

Corresponding Author:

Abstract

The power grid stands as a critical infrastructure supporting modern society, yet it remains susceptible to cyber threats that could compromise its stability and functionality. Addressing the dynamic variations and evolving challenges posed by cyber threats requires robust strategies in cybersecurity. This paper investigates methods to safeguard the stability of the power grid against cyber intrusions and system variations. This study delves into the multifaceted nature of cyber threats targeting the power grid and analyzes the dynamic variations within the system that could be exploited by malicious actors. This paper presents a comprehensive framework encompassing proactive and reactive cybersecurity measures. Reactive measures include incident response plans, rapid recovery protocols, and the integration of machine learning and artificial intelligence for real-time threat detection and mitigation. Moreover, considering the interconnected nature of the power grid, this study explores collaborative approaches among stakeholders, such as utility companies, government bodies, regulatory authorities, and cybersecurity experts, to foster information sharing, best practices, and standardized protocols. Ultimately, this paper serves as a guide for policymakers, grid operators, and cybersecurity professionals to develop robust strategies that safeguard the stability of the power grid in the face of evolving cyber threats and system dynamics. By implementing a holistic cybersecurity approach, the aim is to ensure resilience, reliability, and continuity in the delivery of electricity to society.

Keywords: *Power grid cybersecurity, Dynamic system variations, Cyber threats, Grid infrastructure vulnerabilities, Proactive cybersecurity measures*

1. INTRODUCTION

The power grid is the backbone of modern civilization, enabling the continuous flow of electricity to homes, businesses, and critical infrastructure[1]. However, this intricate network faces escalating threats from cyber adversaries seeking to exploit vulnerabilities in its infrastructure [2]. These threats, coupled with the inherent dynamic variations within the system, pose significant challenges to ensuring the stability and reliability of the power grid [3]. This paper aims to explore and analyze comprehensive strategies to safeguard the stability of the power grid amidst evolving cyber threats and dynamic system variations [4]. Understanding the intricate interdependencies within the grid infrastructure is crucial to comprehend the potential entry points for cyberattacks and the vulnerabilities that adversaries might exploit [5]. The cybersecurity landscape within the power grid domain is multifaceted, encompassing a range of threats including but not limited to malware, ransomware, phishing attacks, and sophisticated intrusions targeting control systems [6]. Moreover, the evolving nature of these threats necessitates a proactive approach that not only identifies vulnerabilities but also implements robust measures to prevent, detect, and respond to cyber incidents [7]. Dynamic system variations within the power grid, stemming from changes in demand patterns, network configuration, integration of renewable energy sources, and other operational factors, further complicate cybersecurity efforts [8, 9]. These variations can potentially create new points of weakness, making the grid susceptible to exploitation by cyber adversaries. This paper delineates a holistic framework that amalgamates proactive and reactive strategies to mitigate cyber threats and address the inherent system variations [10, 11]. In Figure 1 we discuss The power grid cyber-physical infrastructure comprising interconnected systems of hardware, software, and communication networks managing electricity generation, transmission, and distribution. It integrates physical components like transformers and power lines with digital systems, enabling real-time monitoring, control, and data analysis for efficient energy delivery. This infrastructure's complexity involves protecting against cyber threats while ensuring reliability, resilience, and responsiveness to evolving energy demand

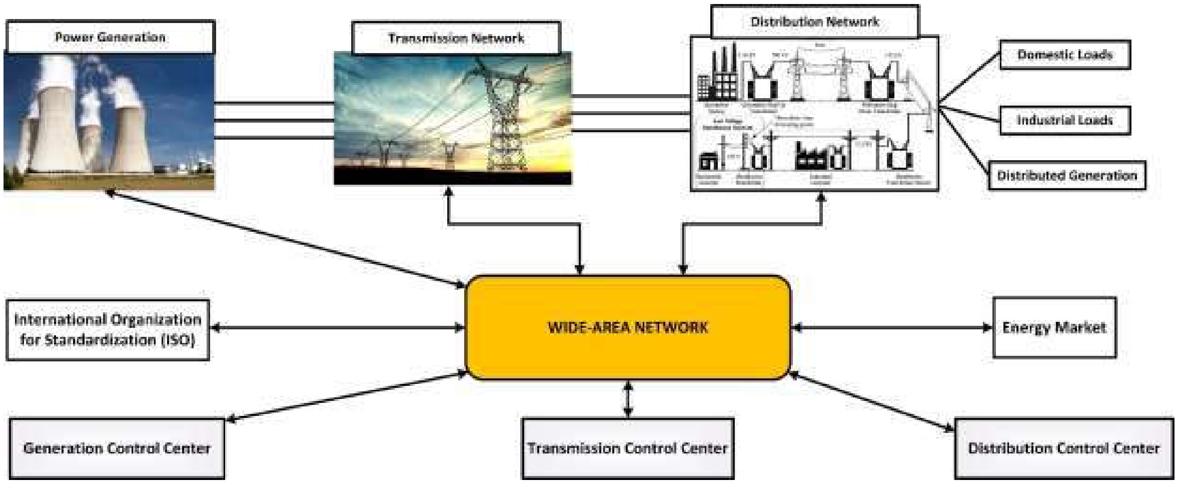

Figure 1: Power grid cyber-physical infrastructure

In Figure 1 We discuss the power grid cyber-physical infrastructure refers to the interconnected system that combines both physical components (such as power plants, transformers, transmission lines, substations, etc.) with digital technologies (such as control systems, communication networks, software, sensors, etc.) to generate, transmit, and distribute electrical power efficiently[12]. This infrastructure is the backbone of modern society, facilitating the delivery of electricity from generation sources to end-users [13]. However, with the integration of digital technologies, the power grid becomes susceptible to cyber threats and vulnerabilities, which can have severe consequences if exploited [14].
Key components of the power grid cyber-physical infrastructure include:

Generation Facilities: Power plants and renewable energy sources that generate electricity [15].
Transmission System: High-voltage lines that transport electricity over long distances from power plants to substations [16].
Substations: Facilities that convert electricity between different voltage levels for efficient transmission and distribution [17].
Distribution Networks: Lower voltage lines that deliver electricity from substations to homes, businesses, and other consumers [18, 19].
Control Systems: SCADA (Supervisory Control and Data Acquisition) and other control systems manage and monitor the grid's operations [20].
Communication Networks: Infrastructure used for data transmission between various components of the grid, enabling real-time monitoring and control.
Sensors and IoT Devices: Devices that collect data on grid performance, allowing for better management and maintenance.

However, the integration of digital systems into the power grid also introduces cybersecurity challenges[21]. Cyber threats like malware, hacking, ransomware, and other attacks can potentially disrupt grid operations, leading to power outages, data breaches, financial losses, and even threats to national security [22, 23].
To mitigate these risks, efforts are focused on enhancing cybersecurity measures, including:

Firewalls and Intrusion Detection Systems: Protecting critical systems from unauthorized access [24].

Encryption and Authentication: Safeguarding communication and data integrity.

Regular Updates and Patch Management: Ensuring systems are equipped with the latest security measures [25].

Training and Awareness Programs: Educating personnel to recognize and respond to cyber threats. Regulatory Standards and Compliance: Enforcing standards to ensure cybersecurity across the power grid infrastructure [26]. The goal is to maintain a balance between leveraging digital technologies for operational efficiency while safeguarding the grid against potential cyber threats to ensure reliability, resilience, and security in power supply [27].
Power grid cybersecurity refers to the comprehensive set of strategies, protocols, technologies, and practices implemented to protect the electric power grid infrastructure from cyber threats, attacks, and vulnerabilities [28, 29]. It involves safeguarding the various interconnected components and systems that form the backbone of electricity generation, transmission, distribution, and management against malicious activities that could disrupt operations, compromise data integrity, or threaten the reliability of power supply [30]. Key aspects and considerations within power grid cybersecurity include Critical Infrastructure Protection: Recognizing the power grid as critical infrastructure and establishing measures to ensure its resilience against cyber threats. Protecting essential components such as control systems, substations, generators, and transmission lines is paramount [31]. Threat Landscape Analysis: Constantly assessing and understanding the evolving threat landscape. This includes monitoring emerging cyber threats, vulnerabilities, and attack vectors that target power grid infrastructure, as well as studying historical cyber incidents for lessons learned [32]. Risk Assessment and Management: Conduct risk assessments to identify vulnerabilities, evaluate potential risks, and prioritize cybersecurity measures. Implementing risk management strategies to mitigate identified risks and enhance overall resilience [33]. Securing Communication Networks: Employing robust encryption, authentication mechanisms, and secure communication protocols to protect data transmission across the grid [34]. This includes securing SCADA (Supervisory Control and Data Acquisition) systems and other critical communication networks. Anomaly Detection and Monitoring: Implementing continuous monitoring systems and employing anomaly detection techniques to identify unusual behavior or potential cyber threats in real-time [35]. Monitoring for deviations from normal system operations helps in early threat detection. Incident Response and Recovery: Developing and regularly updating incident response plans to effectively respond to cyber incidents. Rapid recovery protocols are crucial for minimizing disruptions and restoring normal grid operations swiftly after an attack [36]. Regulatory Compliance: Adhering to industry-specific regulations, standards, and compliance requirements to ensure cybersecurity measures are in line with established guidelines and policies [37].

II. Components of Power Grid Cybersecurity

Critical Infrastructure Protection (CIP): Focuses on securing the vital components of the power grid, including generation plants, transmission lines, substations, and distribution networks, from cyber threats[38, 39]. This involves measures such as access controls, intrusion detection systems, and security protocols. Control Systems Security: Protects the operational technology (OT) and supervisory control and data acquisition (SCADA) systems that manage and monitor power grid operations [40]. Securing these control systems involves implementing firewalls, authentication mechanisms, encryption, and continuous monitoring to prevent unauthorized access and manipulation [41]. Risk Assessment and Management: Conducting thorough risk assessments to identify vulnerabilities and potential entry points for cyber attacks is crucial. Risk management strategies involve prioritizing threats, implementing mitigation measures, and establishing incident response plans to minimize the impact of cyber incidents [42]. Cybersecurity Standards and Regulations: Adherence to industry-specific cybersecurity standards and regulations, such as NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards in the United States, plays a significant role in ensuring a baseline level of security across the power grid infrastructure [43]. Challenges in Power Grid Cybersecurity Complexity and Interconnectedness: The power grid's extensive and interconnected nature increases its vulnerability to cyberattacks. A breach in one area can potentially affect the entire grid, leading to widespread outages or disruptions [44, 45]. Emerging Threat Landscape: Rapid technological advancements and the evolution of cyber threats present continuous challenges [46]. Threat actors are constantly devising new attack methods, making it essential for cybersecurity measures to adapt and evolve accordingly. Legacy Systems and Infrastructure: Many components within the power grid infrastructure, including control systems and equipment, often operate on legacy technologies that might lack robust cybersecurity features, making them more susceptible to attacks [47]. Strategies for Enhancing Power Grid Cybersecurity. Continuous Monitoring and Incident Response: Implementing real-time monitoring and rapid incident response mechanisms to detect and mitigate cyber threats promptly. Investment in Advanced Technologies: Embracing innovative cybersecurity technologies like artificial intelligence, machine learning, and behavioral analytics to identify and respond to threats [46] proactively. Collaboration and Information Sharing: Fostering collaboration among industry stakeholders, government agencies, and cybersecurity experts to share information, best practices, and threat intelligence for collective defense against cyber threats. Understanding these aspects provides a foundational framework for implementing robust cybersecurity measures within the power grid, ensuring its resilience against evolving cyber threats [48]. Variations within a power grid, including dynamic changes in demand, voltage, frequency, and system operations, can significantly impact power grid cybersecurity in several ways: Vulnerability Exploitation: Fluctuations in grid conditions may create windows of opportunity for cyber attackers to exploit vulnerabilities. Sudden changes in power flow, frequency, or system topology can be used to launch attacks or hide malicious activities within the noise of normal grid variations [49]. Disruption of Operations: Variations in grid parameters might be manipulated by cyber threats to disrupt or degrade normal grid operations. Attacks targeting control systems, such as SCADA (Supervisory Control and Data Acquisition) systems or other critical infrastructure, could lead to power outages or grid instability. Increased Complexity for Defense: The dynamic nature of grid variations adds complexity to cybersecurity defense strategies [50]. Rapid changes in grid conditions may make it harder to distinguish between normal variations and abnormal behavior caused by cyber threats, complicating threat detection and response efforts. Impact on Grid Stability: Cyberattacks exploiting variations in the power grid can impact its stability and resilience [51, 52]. For instance, unauthorized control over grid elements could lead to sudden frequency changes or overload conditions, potentially resulting in cascading failures or blackouts. Integrity and Data Security Concerns: Variations can also affect data integrity and communication within the grid. Attacks on data transmission or manipulation of operational data might result in incorrect decisions by control systems, impacting the overall grid reliability and safety [53].

III. Understanding Dynamic System Variations

Understanding dynamic system variations involves grasping a system's changes, fluctuations, or behaviors over time [54]. Dynamic systems refer to entities or processes that evolve or change continuously, and their variations are often influenced by internal and external factors. Here's an overview of key concepts related to understanding dynamic system variations: Dynamic Systems: These are systems that change or evolve. They can range from physical systems (like mechanical systems, and and biological systems) to abstract systems (such as economic systems, social systems, or mathematical models) [55]. Variables: Dynamic systems have variables that represent different aspects or quantities within the system. These variables can be dependent or independent and might change over time due to various factors [56]. States and State Space: A system's state is a set of values of all variables that fully describe its condition at a particular time. The state space represents all possible states of a system[57]. Time Evolution: Understanding how the system's variables change over time is crucial. This involves studying the system's dynamics or the rules that govern how the system evolves from one state to another [58]. Equilibrium and Stability: Systems may have equilibrium points where variables remain constant over time. Stability refers to the system's tendency to return to this equilibrium after being disturbed [59]. Feedback and Control: Feedback mechanisms within dynamic systems can influence the system's behavior. Control systems are designed to regulate or manage the system's behavior toward desired states. Nonlinear Dynamics: Systems with nonlinear relationships among variables can exhibit complex behaviors like chaos, bifurcations, or attractors. Understanding these dynamics often involves advanced mathematical modeling and analysis [60]. External Influences: Dynamic systems can be affected by external factors such as environmental changes, inputs, disturbances, or interactions with other systems [61]. Understanding these influences is crucial to predict and manage system behavior. Modeling and Simulation: Creating mathematical or computational models is often used to simulate and predict the behavior of dynamic systems. These models help in understanding variations and testing different scenarios without affecting the real system. Adaptation and Evolution: Some dynamic systems can adapt or evolve, changing their structure, behavior, or characteristics in response to internal or external stimuli. Understanding dynamic system variations requires a multidisciplinary approach, combining principles from mathematics, physics, engineering, biology, economics, and other fields. Analyzing these systems often involves a mix of theoretical understanding, empirical observations, and computational techniques to comprehend their behaviors and variations accurately [62, 63].

Certainly, here are some examples and case studies illustrating the impact of variations on power grid cybersecurity: Ukraine Power Grid Cyber Attack (2015 and subsequent years): In 2015, Ukraine experienced one of the first publicly acknowledged cyberattacks targeting its power grid. Hackers gained access to the grid's control systems and remotely manipulated them, leading to a widespread blackout affecting thousands of customers [64]. This attack showcased how variations in grid operations could be exploited by cyber threats to cause disruptions. Stuxnet Worm (2010): Although not directly related to power grid variations, the Stuxnet worm is a significant case demonstrating the potential impact of cyberattacks on critical infrastructure [65]. Stuxnet targeted Iran's nuclear facilities, specifically their centrifuges, by altering their control systems [66]. This highlighted the potential risks associated with cyber threats targeting critical infrastructure and control systems. Puerto Rico Power Grid (After Hurricane Maria, 2017): After Hurricane Maria devastated Puerto Rico's power grid, the system faced multiple variations and stress due to rebuilding efforts and changes in power demand patterns [67]. This scenario highlighted vulnerabilities during recovery periods, where cyber threats could exploit grid variations and infrastructure weaknesses [68]. North American Electric Reliability Corporation (NERC) CIP Standards Violations: Several instances have been reported where utilities have been found violating NERC's Critical Infrastructure Protection (CIP) standards. Variations in compliance measures or inadequate security protocols in response to dynamic changes in the grid's operations have exposed vulnerabilities to potential cyber threats [69]. These examples emphasize the vulnerability of power grids to cyber attacks, showcasing instances where variations in grid operations, either due to natural disasters, recovery efforts, or changing demand patterns, have created opportunities for cyber threats to exploit weaknesses in cybersecurity defenses [70]. These cases underscore the importance of robust cybersecurity measures to protect critical infrastructure and ensure grid resilience against cyber threats during dynamic operational variations [71].

2. Adapting to Dynamic Challenges: Managing System Variations in Power Grid Cybersecurity

Adapting to dynamic challenges in managing system variations within power grid cybersecurity necessitates a comprehensive strategy that accounts for evolving threats [72]. The power grid, a foundational infrastructure, demands a proactive approach that integrates cutting-edge technologies like AI-driven threat detection, blockchain for secure transactions, and robust encryption methods [73]. Implementing a resilient framework involves continuous monitoring, threat intelligence analysis, and regular system updates to mitigate vulnerabilities. Moreover, fostering a culture of cybersecurity awareness among personnel and establishing collaborative partnerships across industry stakeholders are crucial components in safeguarding the power grid against emerging cyber threats[74]. This adaptive and holistic approach ensures the resilience and reliability of the power grid amidst a rapidly changing cybersecurity landscape [75].

I. Strategies for Safeguarding Stability Power Grid Cybersecurity

Safeguarding stability involves various strategies, and real-time monitoring, situational awareness, and adaptive, and resilient infrastructure design are crucial components in achieving this goal. Here's a breakdown of these strategies: Real-time Monitoring and Situational Awareness: Technology Integration: Implementing advanced monitoring technologies such as sensors, IoT devices, satellite imagery, and AI-driven analytics allows for real-time data collection and analysis. This helps in identifying potential risks, anomalies, or changes in the environment [76]. Early Warning Systems: Developing systems that can detect and alert about impending threats or disruptions allows for proactive measures to be taken, minimizing potential damages. Data Fusion and Analysis: Integrating diverse data sources and utilizing analytics for comprehensive insights enhances situational awareness, enabling better decision-making in times of crisis [77]. Adaptive Strategies: Flexibility in Planning: Creating adaptive strategies that can evolve in response to changing conditions is crucial. This involves having contingency plans that can be adjusted based on real-time information. Scenario Planning: Developing multiple scenarios and strategies for various potential disruptions helps in preparedness and quick adaptation when unexpected events occur. Agile Response Teams: Having teams trained and ready to respond to various situations helps in implementing adaptive strategies effectively [78]. Resilient Infrastructure Design: Redundancy and Backup Systems: Building redundancies into critical infrastructure and systems ensures that if one part fails, there are backups in place to maintain functionality [79]. Figure 2 discusses the Infrastructure layer attack resilience involves implementing robust security measures, including firewalls, encryption, and intrusion detection systems, to defend against cyber threats targeting network, hardware, and software components. It encompasses strategies such as redundancy, segmentation, and regular updates to mitigate and recover from potential attacks, ensuring continuous functionality and minimizing disruptions. Resilience also involves proactive monitoring, incident response planning, and collaboration among stakeholders to fortify the infrastructure against evolving threats and vulnerabilities.

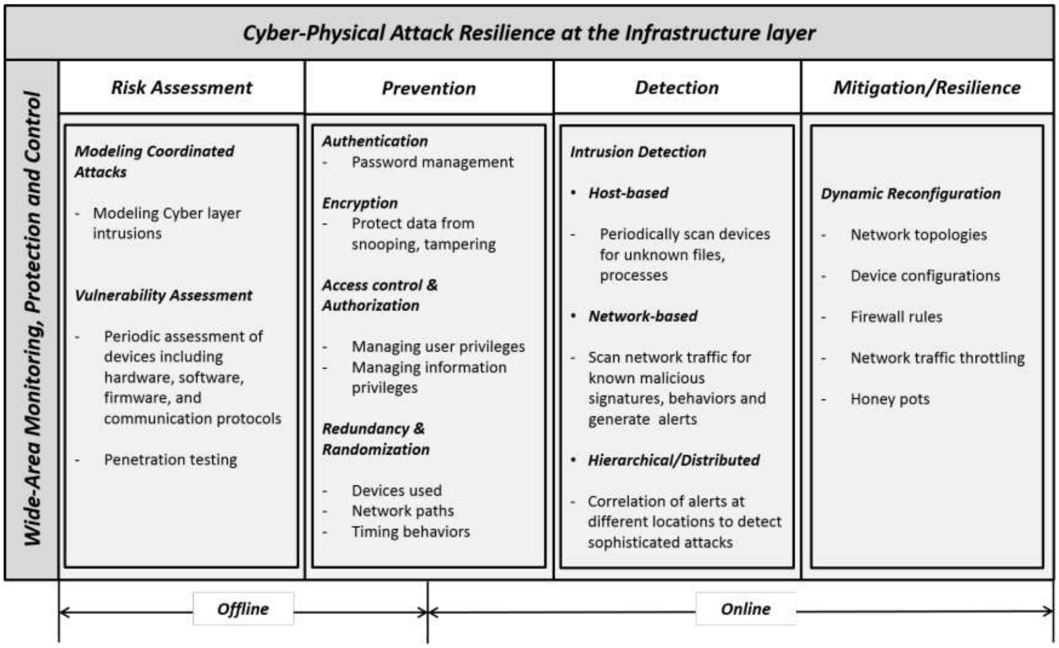
Cyber-Physical Attack Resilience at the Infrastructure layer
Wide-Area Monitoring, Protection and Control
Risk Assessment
Prevention
Detection
Mitigation/Resilience
Modeling Coordinated Attacks
- Modeling Cyber layer intrusions
Vulnerability Assessment
- Periodic assessment of devices including hardware, software, firmware, and communication protocols
- Penetration testing
Authentication
- Password management
Encryption
- Protect data from snooping, tampering
Access control & Authorization
- Managing user privileges
- Managing information privileges
Redundancy & Randomization
- Devices used
- Network paths
- Timing behaviors
Intrusion Detection
• Host-based
- Periodically scan devices for unknown files, processes
• Network-based
- Scan network traffic for known malicious signatures, behaviors and generate alerts
• Hierarchical/Distributed
- Correlation of alerts at different locations to detect sophisticated attacks
Dynamic Reconfiguration
- Network topologies
- Device configurations
- Firewall rules
- Network traffic throttling
- Honey pots
Offline
Online

Figure 2: Infrastructure layer attack resilience

Figure 2 discusses the Infrastructure layer attack resilience refers to the capability of critical infrastructure systems to withstand and recover from various types of attacks, disruptions, or failures [80]. This resilience is crucial in ensuring the continuous operation and functionality of essential services, such as power grids, transportation networks, communication systems, water supply, and more [81]. Key elements of infrastructure layer attack resilience include:

Redundancy and Diversity: Infrastructure systems incorporate redundant components and diverse pathways to ensure that if one part fails or is compromised, alternate resources or routes are available to maintain functionality [82, 83]. This redundancy helps in minimizing the impact of an attack or failure on the entire system.

Security Measures: Implementing robust security measures, such as encryption, firewalls, intrusion detection systems, access controls, and authentication protocols, to protect against cyber threats, unauthorized access, and attacks on critical infrastructure components [84].

Monitoring and Early Detection: Continuous monitoring of infrastructure systems for anomalies, unusual activities, or potential threats is crucial. Early detection allows for swift responses to mitigate potential damages and prevent widespread disruptions [85].

Resilient Design and Planning: Designing infrastructure systems with resilience in mind involves building them to withstand various stressors, including physical attacks, natural disasters, cyber threats, and operational failures. This includes designing for modularity, flexibility, and adaptability to rapidly recover from disruptions [86].

Backup and Recovery Procedures: Establishing effective backup and recovery plans for critical data, systems, and services is essential [87]. Regularly testing these procedures ensures that in the event of an attack or failure, systems can be restored quickly and efficiently.

Collaboration and Information Sharing: Encouraging collaboration among different stakeholders, including government agencies, private sector entities, and cybersecurity experts, promotes information sharing and coordination to enhance overall resilience against potential threats.

Training and Awareness: Educating personnel about potential threats, best practices in cybersecurity, and response protocols is critical [88]. Well-trained personnel are better equipped to detect, respond to, and recover from attacks effectively. By integrating these strategies, infrastructure layer attack resilience aims to minimize the impact of attacks or disruptions, maintain essential services, and enable rapid recovery to normal operations. It's an ongoing process that requires continuous assessment, improvement, and adaptation to evolving threats and technologies[89].
Artificial Intelligence (AI) and Machine Learning (ML) play significant roles in various fields, including mitigation efforts across different domains. When it comes to mitigating risks, addressing challenges, and managing crises, AI and ML offer several technological tools and applications. Here's how they contribute: Predictive Analytics: AI and ML algorithms can analyze large datasets to identify patterns and trends, enabling predictive modeling for potential risks and threats. For instance, in disaster management, these technologies can forecast natural disasters like hurricanes, earthquakes, or floods, allowing authorities to take proactive measures to mitigate their impact [90]. Risk Assessment and Management: AI and ML models can assess risks in various scenarios, including cybersecurity threats, financial risks, or environmental hazards. These tools can aid in evaluating vulnerabilities and suggest strategies to manage or minimize these risks. Early Warning Systems: Utilizing AI algorithms, early warning systems can be developed to detect anomalies or potential dangers [91]. These systems can be deployed in diverse settings, such as healthcare for disease outbreak detection or in infrastructure for identifying potential failures. Resource Optimization and Allocation: During crises or disasters, AI and ML help optimize resource allocation. For instance, in emergency response scenarios, these technologies can analyze real-time data to efficiently dispatch resources like medical supplies, manpower, or equipment to affected areas[92]. Natural Language Processing (NLP): NLP-driven AI systems can sift through vast amounts of textual data from social media, news outlets, or other sources to gather insights, assess public sentiment, and provide early indicators of potential issues or crises [93]. Adaptive Systems for Decision-Making: AI-powered decision support systems can assist decision-makers by processing and analyzing information rapidly, providing recommendations, and even learning from past decisions and outcomes to refine future suggestions [94]. Climate Change and Environmental Monitoring: AI and ML models can analyze environmental data to track changes, predict trends, and propose mitigation strategies for climate-related issues like deforestation, pollution, or biodiversity loss. Healthcare and Epidemic Management: AI and ML are crucial in analyzing medical data, tracking the spread of diseases, and developing models for disease prediction. They also aid in drug discovery, treatment optimization, and healthcare resource management during pandemics [95]. Automated Monitoring and Response Systems: AI-driven monitoring systems can continuously observe critical infrastructure, such as energy grids or transportation networks, to detect anomalies and respond quickly to prevent failures or accidents. Cybersecurity: AI and ML techniques are employed in cybersecurity to identify and respond to potential threats in real-time, detecting unusual patterns in network traffic, and enhancing systems' ability to defend against evolving cyber-attacks [96]. The role of AI and ML in mitigation efforts is expanding rapidly, providing innovative solutions and enhancing our capacity to predict, prevent, and manage various risks across multiple domains. However, ethical considerations, transparency, and accountability are essential while deploying these technologies to ensure their responsible and effective use [97].

II. Future Directions and Recommendations

AI and Machine Learning: Continued integration of AI and machine learning algorithms for predictive analysis, anomaly detection, and automated response systems. These technologies can assist in identifying threats and vulnerabilities in real time, enabling quicker and more accurate responses to potential cyber-attacks [98]. Blockchain Technology: Implementing blockchain for secure and transparent transaction logging, ensuring the integrity of data in the power grid.

It can help in securing communications and transactions between various components of the grid, reducing the risk of tampering or unauthorized access. Zero Trust Architecture: Moving towards a zero-trust model where no entity, inside or outside the network, is trusted by default. This approach requires strict authentication and verification for all users and devices accessing the grid's systems and data, minimizing the risk of insider threats and unauthorized access. Edge Computing and IoT Security: As the power grid becomes more interconnected with IoT devices and edge computing, there's a need for robust security measures at these endpoints [99]. Focus on securing these devices and networks to prevent potential entry points for cyber threats. Resilient Communication Networks: Developing and deploying resilient communication networks that can withstand cyber attacks or disruptions. Technologies like Software-Defined Networking (SDN) and Network Function Virtualization (NFV) can offer more agile, secure, and scalable communication infrastructures [100]. Cyber Threat Intelligence and Information Sharing: Encouraging collaboration among stakeholders to share threat intelligence and best practices in combating cyber threats. Establishing platforms for information exchange can help in early threat detection and response. Quantum-Safe Cryptography: Exploring and implementing quantum-resistant cryptographic algorithms to prepare for the advent of quantum computers, which could potentially break current encryption methods. Continuous Monitoring and Adaptive Security: Moving from static security measures to continuous monitoring and adaptive security mechanisms that can dynamically adjust to evolving cyber threats in real-time [101]. These emerging technologies and trends highlight the evolving landscape of power grid cybersecurity, emphasizing the need for proactive measures to address emerging threats and vulnerabilities. Integrating these technologies into cybersecurity strategies can significantly enhance the resilience of power grid systems against cyber-attacks. Interconnectedness and Complexity: The increasing interconnection of devices and systems in the power grid introduces complexity, making it more challenging to secure against cyber threats[102]. Ensuring the security of this interconnected infrastructure poses a significant challenge. Legacy Systems and Infrastructure: Many power grid systems still rely on legacy equipment and infrastructure, which might lack modern security features and could be more vulnerable to cyber-attacks. Human Factor: Insider threats, human errors, and lack of cybersecurity awareness among personnel remain significant challenges. Training and educating employees about cybersecurity practices are essential. Resource Constraints: Limited budgets and resources allocated for cybersecurity in power grid operations can restrict the implementation of robust security measures. Innovation and Technology Adoption: Embracing innovative technologies, such as AI, blockchain, and IoT, presents opportunities to bolster cybersecurity defenses and enhance resilience in the power grid. Collaboration and Information Sharing: Opportunities exist for increased collaboration between industry stakeholders, sharing threat intelligence, best practices, and lessons learned to improve overall cyber resilience. Regulatory Support: Regulatory bodies can play a crucial role in incentivizing and enforcing cybersecurity standards and practices across the power grid industry, encouraging a more resilient infrastructure. Risk Assessment and Management: Conduct comprehensive risk assessments regularly to identify vulnerabilities and prioritize cybersecurity investments based on potential threats. Investment in Modernization: Allocate resources for upgrading and modernizing legacy systems, integrating cybersecurity features, and implementing robust security protocols across the entire infrastructure. Employee Training and Awareness: Provide regular training programs to staff at all levels to enhance their understanding of cybersecurity threats and best practices for mitigating risks. Adopt a Defense-in-Depth Strategy: Implement multiple layers of security controls (firewalls, encryption, access controls, etc.) to create a defense-in-depth approach, reducing the likelihood of successful cyber attacks. Incident Response and Recovery Planning: Develop and test incident response plans to ensure a swift and efficient response to cyber incidents. This includes strategies for recovery and continuity of operations.

3. Conclusion

In conclusion, the future of power grid cybersecurity demands continuous adaptation and proactive measures. Embracing emerging technologies, fostering collaboration, and implementing robust cybersecurity strategies are imperative to safeguard against evolving cyber threats. The interconnectedness and complexity of power grid systems require a multifaceted approach that involves technological innovation, personnel training, regulatory support, and ongoing vigilance. By addressing these challenges and seizing opportunities, the resilience of power grid cybersecurity can be significantly enhanced, ensuring the continued stability and reliability of this critical infrastructure. Safeguarding stability within the power grid amidst dynamic system variations necessitates a holistic and adaptive cybersecurity approach. Recognizing the intricate interplay between evolving technologies and emerging threats is crucial. Strategies must prioritize continual risk assessment, the implementation of cutting-edge encryption and monitoring technologies, and the fostering of a collaborative ecosystem for information sharing among stakeholders. Embracing innovation, investing in robust training programs, and maintaining a proactive stance against cyber threats are pivotal in fortifying the power grid's resilience. Ultimately, a combination of proactive measures, technological advancements, and collective vigilance serves as the cornerstone in effectively addressing and mitigating the challenges posed by dynamic system variations in power grid cybersecurity.

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] 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.

[3] 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.

[4] K. Pan, P. Palensky, and P. M. Esfahani, "From static to dynamic anomaly detection with application to power system cyber security," *IEEE Transactions on Power Systems,* vol. 35, no. 2, pp. 1584-1596, 2019.

[5] 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.

[6] Z. Chu, S. Lakshminarayana, B. Chaudhuri, and F. Teng, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE Transactions on Smart Grid,* 2022.

[7] 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.

[8] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *International Journal of Information Security,* vol. 21, no. 5, pp. 1189-1210, 2022.

[9] A. M. Mohan, N. Meskin, and H. Mehrjerdi, "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems," *Energies,* vol. 13, no. 15, p. 3860, 2020.

[10] 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.

[11] A. Lakhani, "The Ultimate Guide to Cybersecurity," 2023, doi: 10.31219/osf.io/nupye.

[12] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal,* 2023.

[13] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1367-1388, 2017.

[14] D. Al Momani *et al.*, "Energy saving potential analysis applying factory scale energy audit–A case study of food production," *Heliyon,* vol. 9, no. 3, 2023.

[15] X. Huang, Z. Qin, and H. Liu, "A survey on power grid cyber security: From component-wise vulnerability assessment to system-wide impact analysis," *IEEE Access,* vol. 6, pp. 69023-69035, 2018.

[16] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010: IEEE, pp. 1-7.

[17] 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.

[18] 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.

[19] K. Aygul, M. Mohammadpourfard, M. Kesici, F. Kucuktezcan, and I. Genc, "Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks," *Internet of Things,* p. 101012, 2023.

[20] 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.

[21] A. Lakhani, "AI Revolutionizing Cyber security unlocking the Future of Digital Protection," 2023, doi: https://osf.io/cvqx3/.

[22] R. V. Yohanandhan *et al.*, "A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid," *International Journal of Electrical Power & Energy Systems,* vol. 136, p. 107720, 2022.

[23] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors,* vol. 21, no. 18, p. 6225, 2021.

[24] M. Rahim, H. M. Khalid, and M. Akram, "Sensor location optimization for fault diagnosis with a comparison to linear programming approaches," *The International Journal of Advanced Manufacturing Technology,* vol. 65, pp. 1055-1065, 2013.

[25] 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.

[26] J. Ruan *et al.*, "Deep learning for cybersecurity in smart grids: Review and perspectives," *Energy Conversion and Economics,* vol. 4, no. 4, pp. 233-251, 2023.

[27] 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.

[28] M. A. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, and C. Assi, "Protecting the future grid: An electric vehicle robust mitigation scheme against load altering attacks on power grids," *Applied Energy,* vol. 350, p. 121769, 2023.

[29] 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.

[30] M. Rahim, H. M. Khalid, and A. Khoukhi, "Nonlinear constrained optimal control problem: a PSO–GA-based discrete augmented Lagrangian approach," *The International Journal of Advanced Manufacturing Technology,* vol. 62, pp. 183-203, 2012.

[31] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering,* vol. 67, pp. 469-482, 2018.

[32] S. M. Amin, "Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems," in *IEEE PES General Meeting*, 2010: IEEE, pp. 1-5.

[33] 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 future prospects," *Electronics,* vol. 11, no. 9, p. 1502, 2022.

[34] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 5, pp. 1932-1941, 2017.

[35] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digital Communications and Networks,* vol. 8, no. 4, pp. 422-435, 2022.

[36] 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.

[37] 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.

[38] 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.

[39] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4405-4425, 2017.

[40] 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 normalized residual test," in *2015 IEEE Power and Energy Conference at Illinois (PECI)*, 2015: IEEE, pp. 1-5.

[41] S. Borenius, P. Gopalakrishnan, L. Bertling Tjernberg, and R. Kantola, "Expert-guided security risk assessment of evolving power grids," *Energies,* vol. 15, no. 9, p. 3237, 2022.

[42] 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.

[43] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 684-694, 2016.

[44] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electric power systems research,* vol. 163, pp. 396-412, 2018.

[45] M. Tuttle, M. Poshtan, T. Taufik, and J. Callenes, "Impact of cyber-attacks on power grids with distributed energy storage systems," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019: IEEE, pp. 1-6.

[46] R. W. Habash, V. Groza, and K. Burr, "Risk management framework for the power grid cyber-physical security," *British journal of applied science & technology,* vol. 3, no. 4, pp. 1070-1085, 2013.

[47] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyberphysical infrastructures in power systems: architectures and vulnerabilities*. Academic Press, 2021.

[48] 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.

[49] D. Zhang *et al.*, "A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems," *Renewable Energy,* vol. 189, pp. 1383-1406, 2022.

[50] 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.

[51] Z. Huang, S. Etigowni, L. Garcia, S. Mitra, and S. Zonouz, "Algorithmic attack synthesis using hybrid dynamics of power grid critical infrastructures," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018: IEEE, pp. 151-162.

[52] 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.

[53] 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.

[54] K. Demertzis, L. S. Iliadis, and V.-D. Anezakis, "An innovative soft computing system for smart energy grids cybersecurity," *Advances in Building Energy Research,* vol. 12, no. 1, pp. 3-24, 2018.

[55] B. Canaan, B. Colicchio, and D. Ould Abdeslam, "Microgrid cyber-security: Review and challenges toward resilience," *Applied Sciences,* vol. 10, no. 16, p. 5649, 2020.

[56] 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.

[57] A. Sulaiman *et al.*, "Artificial Intelligence-Based Secured Power Grid Protocol for Smart City," *Sensors,* vol. 23, no. 19, p. 8016, 2023.

[58] D. K. Panda and S. Das, "Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy," *Journal of Cleaner Production,* vol. 301, p. 126877, 2021.

[59] P. Yang, F. Gao, and H. Zhang, "Multi-player evolutionary game of network attack and defense based on system dynamics," *Mathematics,* vol. 9, no. 23, p. 3014, 2021.

[60] L. R. Phillips *et al.*, "Analysis of operations and cyber security policies for a system of cooperating Flexible Alternating Current Transmission System (FACTS) devices," Sandia National Laboratories (SNL), Albuquerque, NM, and Livermore, CA …, 2005.

[61] 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.

[62] O. S. Nagesh, S. Tripathi, S. B. K. Prasad, P. Hariramakrishnan, A. Gehlot, and V. Tripathi, "Power System Monitoring, Control and Protection for Network, IOT and Cyber Security," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022: IEEE, pp. 1066-1070.

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

[64] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE communications surveys & tutorials,* vol. 14, no. 4, pp. 998-1010, 2012.

[65] T. Berghout, M. Benbouzid, and S. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *International Journal of Critical Infrastructure Protection,* p. 100547, 2022.

[66] 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.

[67] 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.

[68] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, "A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 2, pp. 880-890, 2021.

[69] B. B. Gupta and T. Akhtar, "A survey on smart power grid: frameworks, tools, security issues, and solutions," *Annals of Telecommunications,* vol. 72, pp. 517-549, 2017.

[70] 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.

[71] A. Stefanov and C.-C. Liu, "Cyber-physical system security and impact analysis," *IFAC Proceedings Volumes,* vol. 47, no. 3, pp. 11238-11243, 2014.

[72] I. L. Pearson, "Smart grid cyber security for Europe," *Energy Policy,* vol. 39, no. 9, pp. 5211-5218, 2011.

[73] I. Gandhi, L. Ravi, V. Vijayakumar, and V. Subramaniyaswamy, "Improving security for wind energy systems in smart grid applications using digital protection technique," *Sustainable Cities and Society,* vol. 60, p. 102265, 2020.

[74] 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.

[75] H. T. Reda, A. Anwar, A. N. Mahmood, and Z. Tari, "A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids," *ACM Computing Surveys,* vol. 55, no. 14s, pp. 1-37, 2023.

[76] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access,* vol. 9, pp. 29775-29818, 2021.

[77] 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.

[78] J. Ye *et al.*, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics,* vol. 9, no. 4, pp. 4639-4657, 2020.

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

[80] 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.

[81] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *2012 20th Mediterranean Conference on Control & Automation (MED)*, 2012: IEEE, pp. 716-721.

[82] X. Qin, K. Mai, N. Ortiz, K. Koneru, and A. A. Cardenas, "Cybersecurity and resilience for the power grid," *Resilient Control Architectures and Power Systems,* pp. 201-214, 2021.

[83] Y. Hu *et al.*, "CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack," *Computers & Security,* vol. 111, p. 102465, 2021.

[84] 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.

[85] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: A Review," *Authorea Preprints,* 2022.

[86] A. Gusrialdi and Z. Qu, "Smart grid security: Attacks and defenses," *Smart Grid Control: Overview and Research Opportunities,* pp. 199-223, 2019.

[87] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "A review of machine learning approaches to power system security and stability," *IEEE Access,* vol. 8, pp. 113512-113531, 2020.

[88] 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.

[89] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on 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.

[90] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: A review," *Current Sustainable/Renewable Energy Reports,* vol. 5, pp. 14-22, 2018.

[91] M. S. Mahmoud and H. M. Khalid, "Data-driven fault detection filter design for time-delay systems," *International Journal of Automation and Control,* vol. 8, no. 1, pp. 1-16, 2014.

[92] T. Kerdphol, I. Ngamroo, and T. Surinkaew, "Enhanced robust frequency stabilization of a microgrid against simultaneous cyber-attacks," *Electric Power Systems Research,* vol. 228, p. 110006, 2024.

[93] A. Ahmadi, Y. Asadi, A. M. Amani, M. Jalili, and X. Yu, "Resilient model predictive adaptive control of networked Z-source inverters using GMDH," *IEEE Transactions on Smart Grid,* vol. 13, no. 5, pp. 3723-3734, 2022.

[94] 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.

[95] B. W. Tuinema, J. L. Rueda Torres, A. I. Stefanov, F. M. Gonzalez-Longatt, and M. A. van der Meijden, "Cyber-physical system modeling for assessment and enhancement of power grid cyber security, resilience, and reliability," *Probabilistic Reliability Analysis of Power Systems: A Student's Introduction,* pp. 237-270, 2020.

[96] Y. Xiang, L. Wang, and Y. Zhang, "Adequacy evaluation of electric power grids considering substation cyber vulnerabilities," *International Journal of Electrical Power & Energy Systems,* vol. 96, pp. 368-379, 2018.

[97] M. S. Mahmoud and H. M. Khalid, "Expectation maximization approach to data-based fault diagnostics," *Information Sciences,* vol. 235, pp. 80-96, 2013.

[98] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International journal of critical infrastructure protection,* vol. 25, pp. 36-49, 2019.

[99] R. Khan *et al.*, "Energy sustainability–survey on technology and control of microgrid, smart grid and virtual power plant," *IEEE Access,* vol. 9, pp. 104663-104694, 2021.

[100] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs," *Renewable and Sustainable Energy Reviews,* vol. 168, p. 112794, 2022.

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

[102] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities," *IEEE Communications Surveys & Tutorials,* 2023.