EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 13, Issue 1, January-June, 2024, Available online at: www.eduzonejournal.com

Cyber Threats and Resilience in Power Grid Infrastructures: Assessing Vulnerabilities and Countermeasures

Sergey Parshivlyuk[1], Kirill Panchenko[2]

[1,2]Moscow State University, Russia

ABSTRACT

The power grid infrastructure stands as a critical backbone of modern society, ensuring the uninterrupted flow of electricity to support essential services and daily life. However, this vital system faces unprecedented challenges posed by evolving cyber threats. This paper conducts an in-depth examination of the vulnerabilities inherent in power grid infrastructures and explores effective countermeasures to enhance their resilience against cyber-attacks. The assessment begins by delineating the diverse spectrum of cyber threats targeting power grids, ranging from sophisticated ransom ware attacks and malware infiltration to coordinated hacking attempts. Understanding these threats involves analyzing their methodologies, potential impact on grid operations, and cascading effects on societal functions. Subsequently, this paper outlines the vulnerabilities within power grid systems, emphasizing their susceptibility to cyber intrusions due to interconnected networks, legacy systems, and inadequate security protocols. Addressing these vulnerabilities requires a multifaceted approach that encompasses technological advancements, policy frameworks, and human resource preparedness. In response to identified vulnerabilities, a comprehensive set of countermeasures is proposed to fortify the resilience of power grid infrastructures. These countermeasures include the implementation of robust encryption techniques, network segmentation, intrusion detection systems, and the integration of artificial intelligence for anomaly detection and rapid response.

Keywords: Power grid infrastructure, Cyber threats, Resilience, Vulnerabilities, Countermeasures, Cybersecurity

INTRODUCTION

The modern power grid infrastructure is essential for maintaining societal functions, yet it faces unprecedented cyber threats that compromise its reliability and security[1]. This paper conducts an extensive analysis of the vulnerabilities present in power grid systems and proposes effective countermeasures to bolster their resilience against cyber-attacks.Examining a spectrum of cyber threats targeting power grids, including ransom ware, malware, and hacking attempts, this study delves into their potential impact on grid operations and societal stability. The assessment identifies vulnerabilities within power grid systems stemming from interconnected networks, legacy infrastructure, and insufficient security protocols[2]. To mitigate these risks, a multifaceted approach is recommended, encompassing technological advancements, policy reinforcement, and human resource training. Proposed countermeasures include robust encryption, network segmentation, intrusion detection systems, and leveraging artificial intelligence for anomaly detection and rapid response[3]. Additionally, establishing stringent security standards through regulatory bodies and fostering a cybersecurity-centric culture within power grid organizations are crucial steps in fortifying defenses against evolving cyber threats[4].The power grid infrastructure is a critical component of modern society, playing a pivotal role in ensuring the delivery of electricity from power generation sources to end-users[5]. Its importance can be understood through various perspectives: Reliability and Continuity: A robust power grid ensures a steady and reliable supply of electricity to homes, businesses, industries, hospitals, and other essential services[6]. Interruptions or failures in the grid can lead to significant disruptions, impacting daily life, causing economic losses, and potentially jeopardizing public safety[7]. Economic Growth and Development: Industries and businesses heavily rely on a consistent and affordable supply of electricity[8]. A stable power grid is essential for economic growth, innovation, and the functioning of various sectors, including manufacturing, technology, healthcare, and agriculture[9]. Energy Security: A well-developed and interconnected power grid enhances energy security by diversifying energy sources and creating redundancy[10]. It allows for the efficient integration of various renewable energy sources, reducing dependency on fossil fuels and mitigating the risks associated with supply chain disruptions or geopolitical tensions[11]. Grid Modernization and Innovation: Advancements in technology, such as smart grid systems, digital monitoring, and control systems, enable grid operators to manage and optimize energy distribution more effectively[12]. These innovations enhance efficiency, reduce losses during transmission, and facilitate the integration of decentralized energy sources like solar and wind power[13]. Resilience to Natural Disasters and

Emergencies: A well-designed and resilient power grid can better withstand natural disasters such as hurricanes, earthquakes, or extreme weather events[14]. Additionally, it enables a more effective response and faster recovery during emergencies, ensuring essential services remain functional[15]. Overall, the power grid infrastructure forms the backbone of modern civilization, supporting economic activities, enhancing quality of life, promoting sustainability, and enabling the integration of new energy sources and technologies. Continued investment, innovation, and maintenance are vital to ensuring its resilience and adaptability to future challenges[16].

Understanding Cyber Threats to Power Grid Infrastructures

Cyber threats to power grid infrastructures pose significant risks due to their potential to disrupt essential services, cause economic damage, and threaten public safety[17]. Understanding these threats is crucial for implementing effective cybersecurity measures[18]. Here are some common cyber threats targeting power grid infrastructures: Ransomware Attacks: Ransomware is a type of malware that encrypts data or systems, rendering them inaccessible until a ransom is paid[19]. Power grid operators are susceptible to ransomware attacks that can disrupt operations, leading to service outages or loss of critical data[20]. Malware and Viruses: Malicious software and viruses can infect systems within the power grid, compromising their functionality, stealing sensitive information, or allowing unauthorized access to control systems[21].

Phishing and Social Engineering: Phishing attacks involve tricking individuals into revealing sensitive information or credentials through deceptive emails, messages, or phone calls. Social engineering tactics can manipulate employees into unwittingly providing access to critical systems or sensitive information. Insider Threats: Insider threats can come from employees, contractors, or individuals with privileged access to power grid systems[22, 23]. These threats may involve malicious actions or unintentional errors that compromise system security. Denial-of-Service (DoS) Attacks: DoS attacks flood networks or systems with traffic, overwhelming them and causing service disruption[24]. Distributed Denial-of-Service (DDoS) attacks involve multiple sources attacking simultaneously, making it difficult to mitigate[25]. Supply Chain Vulnerabilities: Components and software used in power grid infrastructure can have vulnerabilities introduced at any stage of the supply chain, potentially compromising the entire system if exploited[26]. Advanced Persistent Threats (APTs): APTs are sophisticated, prolonged attacks typically orchestrated by well-resourced threat actors, such as nation-states or organized cybercriminal groups[27]. These attacks aim to infiltrate and remain undetected within systems for an extended period, exfiltrating sensitive data or manipulating operations[28]. Zero-Day Exploits: Zero-day vulnerabilities are previously unknown vulnerabilities that hackers can exploit before a patch or fix becomes available. Exploiting these vulnerabilities can provide attackers with unauthorized access or control over systems[29].Physical Attacks Enabled by Cyber Means: Cyberattacks can also be used as a means to facilitate physical attacks on critical infrastructure, such as using compromised systems to manipulate or damage physical components of the power grid[30]. Addressing these threats requires a multi-layered approach to cybersecurity, including robust network monitoring, access controls, regular system updates and patches, employee training and awareness programs, encryption of sensitive data, incident response plans, and collaboration with cybersecurity experts and government agencies to share threat intelligence and best practices[31, 32].

Regular security assessments and audits are essential to identify and mitigate vulnerabilities before they are exploited[33].

In Figure 1, we discuss the Cyber resilience techniques according to NIST.

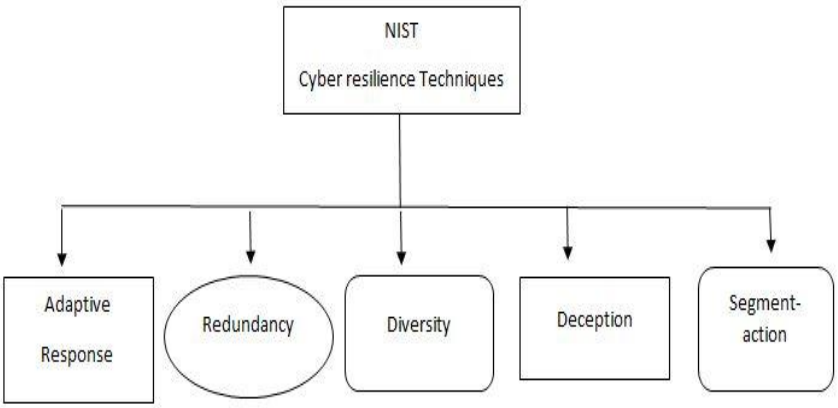

Figure 1: Cyber resilience techniques according to NIST

Figure 1 illustratesthatCyber resilience, as per NIST (National Institute of Standards and Technology), encompasses a strategic approach to managing potential cyber threats. It involves employing various techniques such as continuous monitoring, adaptive security measures, and rapid response capabilities. NIST emphasizes the importance of robust risk assessment and mitigation strategies, alongside the implementation of redundancies in systems and data backups.

Additionally, fostering a culture of awareness and training within an organization is key to enhancing cyber resilience, ensuring a proactive stance against evolving cyber threats.

Identifying Vulnerabilities in Power Grid Systems

Identifying vulnerabilities in power grid systems is crucial for ensuring their security and resilience against potential cyber threats and other risks[34]. Here are some key areas where vulnerabilities may exist: Legacy Systems: Older components or legacy systems within the power grid infrastructure might lack modern security features and could be more susceptible to cyberattacks due to outdated software, hardware, or protocols[35, 36]. Interconnected Networks: Increased interconnectivity between operational technology (OT) and information technology (IT) systems within power grids creates potential vulnerabilities[37]. Any connection points or interfaces between these systems can become entry points for attackers[38]. Software and Firmware Security: Vulnerabilities in software applications or firmware used in control systems, SCADA (Supervisory Control and Data Acquisition), or other critical infrastructure can be exploited by attackers to gain unauthorized access or manipulate system operations[39]. Inadequate Access Controls: Weak or inadequate access controls, such as weak passwords, default credentials, or insufficient authentication measures, can be exploited by attackers to gain unauthorized access to critical systems or networks[40]. Third-Party and Supply Chain Risks: Components, equipment, or software acquired from third-party vendors might introduce vulnerabilities[41]. Supply chain risks involve potential compromises in the manufacturing, distribution, or installation process of these components[42]. Human Factors and Insider Threats: Employees or personnel with access to critical systems may inadvertently introduce vulnerabilities through actions such as clicking on phishing emails, mishandling sensitive information, or falling victim to social engineering attacks[43]. Insider threats involve malicious actions or unauthorized activities by individuals with insider access[44].Insufficient Patching and Updates: Failure to regularly update and patch software or systems with the latest security updates can leave vulnerabilities unaddressed, making systems susceptible to exploitation through known vulnerabilities[45, 46]. Lack of Network Segmentation: Inadequate segmentation of networks within the power grid infrastructure may allow attackers to move laterally across systems once they gain initial access, increasing the potential impact of a breach[47]. Inadequate Incident Response Plans: Lack of comprehensive incident response plans and protocols to detect, respond to, and recover from cyberattacks or system breaches can exacerbate the consequences of an incident[48].

To identify vulnerabilities within power grid systems, utilities, grid operators, and cybersecurity professionals often conduct comprehensive security assessments, risk assessments, penetration testing, and audits. These assessments involve analyzing system architectures, conducting vulnerability scans, evaluating access controls, reviewing configurations, and testing security measures to identify weaknesses and potential entry points for attackers[49]. Regular security updates, staff training, and collaboration with cybersecurity experts also play essential roles in identifying and mitigating vulnerabilities in power grid systems[50].

Enhancing Power Grid Security: Innovations in Cyber Defense and Resilient System Architecture

Power grid security refers to the measures, protocols, technologies, and strategies implemented to safeguard the infrastructure, systems, and data associated with the generation, transmission, and distribution of electrical power[51]. It encompasses protection against physical, cyber, and natural threats that could disrupt the functioning, reliability, and stability of the power grid. The importance of power grid security cannot be overstated due to several critical reasons: Critical Infrastructure Protection: The power grid is considered critical infrastructure as it sustains numerous essential services, including healthcare, communications, transportation, and public safety[52]. Any disruption can lead to severe societal and economic consequences[53]. Economic Stability: Disruptions or attacks on the power grid can have significant economic impacts, causing financial losses for businesses, interrupting manufacturing processes, and disrupting supply chains. Public Safety: A secure power grid ensures the safety and well-being of individuals by providing electricity for heating, cooling, medical equipment, and emergency services[54]. Any compromise in the grid's security could jeopardize public safety.National Security: The power grid is a potential target for cyberattacks by malicious actors, including nation-states, seeking to disrupt a country's stability or gain strategic advantage[55]. Securing the grid is crucial for national security interests. Technological Dependence: With the advancement of technology and the integration of smart devices, IoT, and digital infrastructure into the grid, vulnerabilities increase. Ensuring security is essential to protect against cyber threats exploiting these technological advancements[56]. Resilience against Disasters: Power grid security measures also

include provisions for resilience against natural disasters such as hurricanes, earthquakes, and solar storms. Protecting the grid ensures rapid recovery and minimizes the impact of such events[57]. Data Protection: The power grid generates vast amounts of data related to consumption patterns, operations, and infrastructure[58]. Security measures protect this data from unauthorized access, ensuring privacy and confidentiality. The power grid faces a range of cyber threats that pose significant risks to its security and functionality[59]. These threats can be broadly categorized into various types: Cyberattacks: Malware and Ransomware: Malicious software can infiltrate grid systems, causing disruptions, data theft, or ransomware attacks that encrypt critical systems until a ransom is paid[60, 61]. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): These attacks overwhelm grid systems with excessive traffic, rendering them inaccessible or causing service disruptions[62].

Analysis of Historical Cyber-Attacks on Power Grids

Cyber-attacks on power grids have been a significant concern due to their potential to cause widespread disruption and chaos[63]. Several historical cyber-attacks on power grids have highlighted vulnerabilities in critical infrastructure[64]. Here are some notable examples: Ukraine Power Grid Cyber-Attack (2015 and 2016): In December 2015 and December 2016, sophisticated cyber-attacks targeted the power grid in Ukraine[65]. These attacks, attributed to Russian threat actors, resulted in widespread power outages affecting hundreds of thousands of people[66, 67]. The attackers used malware to manipulate control systems, causing disruptions in the energy distribution process. Stuxnet (2010): Although not specifically targeting power grids, Stuxnet was a highly sophisticated computer worm discovered in 2010. It was designed to target Iran's nuclear program and infected industrial control systems, including those used in power plants[68]. Stuxnet demonstrated the capability of malware to manipulate critical infrastructure systems and highlighted the potential vulnerabilities in industrial control systems worldwide[69, 70]. BlackEnergy Attack (2015): The BlackEnergy malware was involved in the cyber-attack on Ukraine's power grid[71]. It was used to infiltrate the systems of energy companies and disrupt power distribution. The attack highlighted the potential risks posed by malware specifically crafted to target critical infrastructure. Dragonfly (2011-2014): This was a campaign targeting energy sector entities in the United States and Europe[72]. The attackers gained access to networks and systems of energy companies, raising concerns about the potential for future disruptions or espionage activities within critical infrastructure. Table 1,We discuss the Classification of Smart Grid Cyber-Attacks According to Network Layer[73].

Table 1: Classification of Smart Grid Cyber-Attacks According To Network Layer

Network Type	Attack Type
Application Layer	CPU Exhausting, LDoS, HTTP Flooding, Protocol, Stack Buffer Overflow, Data Injection Attacks
Transport Layer	IP Spoofing, Packet Sniffing, Wormhole, Data Injection, Traffic Flooding, Buffer Flooding, Buffer Overflow
MAC Layer	Traffic Analysis, Masquerading, ARP Spoofing, MITM, TSA, MAC DoS Attack, Flooding Attacks, Jamming
Physical Layer	Eavesdropping, Smart Meter Tampering Attacks TSA, Jamming Attacks

Layer Attacks and Solutions

MITM attacks aim to sniff and manipulate messages between the control center and field devices[74]. The attacker seems the right destination for both the source and target during the protocol session. MITM attacks may be performed in each layer, especially in layers 2 and 3, and also affect all of the CIA triad and accountability of a system[75]. The cyber-security solutions should include detailed packet analysis software, also robust authentication mechanisms can protect against MITM attacks[76].

Application layer attacks can easily flood a system that has limited computing resources. Confidentiality and integrity attacks are generally initiated in the application layer since they attempt to get or manipulate the data in the smart grid[77].

DoS attacks can be performed at different layers in smart grid applications. DoS attacks in the application layer aim to exhaust sources of a system, such as memory, CPU, or bandwidth by flooding with intense periods of requests[78]. As communication appliances in smart grids are equipped with limited computational capabilities, they may be potential targets of application layer DoS attacks. A lower-layer attack generally targets the bandwidth of communication channels[79].

Transport layer attacks targeting availability aim to disturb end-to-end connections by consuming the sources, thereby causing the target device to not receive legitimate traffic after a while. TCP and UDP flooding attacks are some commonand vulnerability reporting, at least[80, 81]. A robust defense solution integrates various security techniques using artificial intelligence and machine learning, controlled wireless propagation, authentication, network segmentation, certification, proactive real-time IPS-IDS, and authorization[82].

Aanticipated Advancements in Cyber Threats and Challenges

As of my last update in January 2022, the field of cybersecurity is constantly evolving, with both defenders and attackers continuously innovating[83]. Here are some anticipated advancements, challenges, and trends in cyber threats: AI-Powered Attacks: Hackers are expected to leverage artificial intelligence and machine learning to develop more sophisticated attacks[84]. AI can automate tasks, allowing for more effective and adaptive attacks that can evade traditional security measures[85]. Ransomware Evolution: Ransomware attacks have been a significant threat, and they are expected to continue evolving. Attackers may employ more targeted and sophisticated methods, including double extortion tactics where sensitive data is not only encrypted but also stolen for additional leverage[86]Supply Chain Attacks: Cybercriminals increasingly target supply chains to exploit vulnerabilities in interconnected systems. Attacks on software supply chains and third-party vendors can have widespread and damaging consequences[87, 88]. IoT Vulnerabilities: The proliferation of Internet of Things (IoT) devices introduces new entry points for cyber threats[89]. Insecure IoT devices can be compromised and used as a gateway to access larger networks or launch attacks. Zero-Day Exploits: Zero-day vulnerabilities, which are unknown to the vendor and have no available patch, remain a significant concern[90]. Hackers will likely continue to exploit these vulnerabilities before they are discovered and patched, posing a serious threat to organizations[91]. Cloud Security Challenges: As businesses increasingly move their data and operations to the cloud, ensuring robust cloud security measures becomes crucial. Misconfigurations, unauthorized access, and data breaches in cloud environments are anticipated challenges[92]. Biometric Data Threats: With the increasing use of biometric authentication methods (such as fingerprints, and facial recognition), there are concerns about the security and potential exploitation of biometric data. Protecting this sensitive information will be a priority. Regulatory Compliance and Privacy Concerns: Keeping up with evolving regulations like GDPR, CCPA, and other regional data protection laws presents ongoing challenges for businesses. Ensuring compliance while managing and protecting sensitive data is a persistent issue[93, 94]. Social Engineering Attacks: Human manipulation remains a potent weapon for cybercriminals. Phishing, spear-phishing, and other social engineering techniques continue to evolve, exploiting human psychology and trust to gain unauthorized access[95, 96]. Quantum Computing Risks: While quantum computing offers incredible potential, it also poses a threat to current encryption methods[97, 98]. Quantum-resistant cryptographic solutions will be essential to safeguard against future quantum attacks. As cyber threats advance, organizations and cybersecurity professionals will need to adopt proactive measures, implement robust security practices, invest in training and technology, and remain vigilant to mitigate these evolving risks[99]. Collaboration, information sharing, and a proactive cybersecurity posture are critical in staying ahead of emerging threats[100].

CONCLUSION

Cyber threats pose a significant risk to power grid infrastructures, necessitating a comprehensive understanding of vulnerabilities and effective countermeasures to ensure resilience. Assessing vulnerabilities within power grids involves recognizing interconnected networks, legacy infrastructure weaknesses, and inadequacies in existing security protocols.

Various methods, including penetration testing, vulnerability scanning, risk assessments, and continuous monitoring, are crucial for identifying weaknesses. Case studies such as the Ukraine power grid cyber attacks and the Stuxnet incident underscore the potential impact of cyber threats on critical infrastructure. To bolster resilience, a multi-layered approach encompassing the modernization of legacy systems, robust security protocols, employee training, and compliance with industry standards is imperative.

Continual assessments, proactive measures, and collaboration between stakeholders are crucial in fortifying power grid infrastructures against evolving cyber threats, ensuring their reliability, security, and ability to withstand potential attacks.

Future Outlook:

The future outlook of cyber threats and resilience in power grid infrastructures is poised to navigate an evolving landscape characterized by both challenges and opportunities. As technology advances, the proliferation of interconnected systems and the integration of smart grid technologies introduce new dimensions of vulnerability. Emerging threats, including sophisticated malware, AI-driven attacks, and supply chain risks, necessitate a proactive approach to assess vulnerabilities and fortify defenses. The integration of Internet of Things (IoT) devices, edge computing, and increased reliance on cloud-based solutions further widen the attack surface, demanding robust security measures. However, alongside these challenges, innovations in artificial intelligence, machine learning, and advanced analytics offer potential solutions for threat detection, anomaly recognition, and real-time response. Collaborative efforts between industry stakeholders, government entities, and cybersecurity experts will be vital in shaping resilient power grid infrastructures, emphasizing continuous assessments, adaptive security measures, and a proactive stance against emerging cyber threats to safeguard critical infrastructure.

REFERENCES

[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] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566-575, 2014.
[3] 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.
[4] 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.
[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] 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.
[7] C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, "Smart grid cyber security: An overview of threats and countermeasures," *Journal of Energy and Power Engineering*, vol. 9, no. 7, pp. 632-647, 2015.
[8] S. Nazir, H. Hamdoun, and J. Alzubi, "Cyber attack challenges and resilience for smart grids," *European Journal of Scientific Research*, 2015.
[9] 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.
[10] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.
[11] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522-6530, 2019.
[12] H. Shahinzadeh, A. Mahmoudi, J. Moradi, H. Nafisi, E. Kabalci, and M. Benbouzid, "Anomaly detection and resilience-oriented countermeasures against cyberattacks in smart grids," in *2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS)*, 2021: IEEE, pp. 1-7.
[13] 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.
[14] 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.
[15] S. Hussain, J. H. Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *International Journal of Critical Infrastructure Protection*, vol. 33, p. 100406, 2021.
[16] 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.
[17] 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.
[18] 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.
[19] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *arXiv preprint arXiv:1401.3936*, 2014.

[20] J. Lázaro, A. Astarloa, M. Rodríguez, U. Bidarte, and J. Jiménez, "A Survey on Vulnerabilities and Countermeasures in the Communications of the Smart Grid," *Electronics*, vol. 10, no. 16, p. 1881, 2021.

[21] 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.

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

[23] T. Hecht, L. Langer, and P. Smith, "Cybersecurity risk assessment in smart grids," *Tagungsband ComForEn 2014*, vol. 39, 2014.

[24] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847-855, 2013.

[25] 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.

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

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

[28] 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.

[29] M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez Jr, and K. Perumalla, "Survey of cybersecurity governance, threats, and countermeasures for the power grid," *Energies*, vol. 15, no. 22, p. 8692, 2022.

[30] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, 2008.

[31] 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.

[32] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, p. 111642, 2021.

[33] 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.

[34] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4332-4341, 2018.

[35] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Generation Computer Systems*, vol. 136, pp. 358-377, 2022.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[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] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453-3495, 2018.

[42] Y. Wadhawan, A. AlMajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, no. 10, p. 249, 2018.

[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] L. Coppolino and L. Romano, "Exposing vulnerabilities in electric power grids: An experimental approach," *International Journal of Critical Infrastructure Protection,* vol. 7, no. 1, pp. 51-60, 2014.
[45] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology,* vol. 5, no. 3, pp. 468-483, 2018.
[46] 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.
[47] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem," *Journal of Computational Design and Engineering,* vol. 7, no. 3, pp. 352-366, 2020.
[48] 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.
[49] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid–Part–I: Background on CPPS and necessity of CPPS testbeds," *International Journal of Electrical Power & Energy Systems,* vol. 136, p. 107718, 2022.
[50] G. Dondossola and R. Terruggia, "Cyber security of smart grid communications: Risk analysis and experimental testing," in *Cyber-Physical Systems Approach to Smart Electric Power Grid*: Springer, 2015, pp. 169-193.
[51] 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.
[52] B. Karabacak, S. O. Yildirim, and N. Baykal, "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness," *International Journal of Critical Infrastructure Protection,* vol. 15, pp. 47-59, 2016.
[53] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid AC-based state estimation: Vulnerability analysis against cyber attacks," *IEEE Transactions on Automatic Control,* vol. 64, no. 5, pp. 1784-1799, 2018.
[54] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability,* vol. 13, no. 6, p. 3196, 2021.
[55] 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.
[56] A. Narayanan, J. W. Welburn, B. M. Miller, S. T. Li, and A. Clark-Ginsberg, "Deterring attacks against the power grid," *Santa Monica, CA: Rand Corporation,* 2020.
[57] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for SDN-enabled smart grids," *Computer Communications,* vol. 133, pp. 1-11, 2019.
[58] 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.
[59] Y. Mo *et al.,* "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 195-209, 2011.
[60] H. I. Kure, S. Islam, and M. A. Razzaque, "An integrated cyber security risk management approach for a cyber-physical system," *Applied Sciences,* vol. 8, no. 6, p. 898, 2018.
[61] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," *SoutheastCon 2015,* pp. 1-6, 2015.
[62] 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.
[63] A. Anzalchi and A. Sarwat, "A survey on security assessment of metering infrastructure in smart grid systems," in *SoutheastCon 2015*, 2015: IEEE, pp. 1-4.
[64] J. Xie, A. Stefanov, and C. C. Liu, "Physical and Cybersecurity in a Smart Grid Environment," *Advances in Energy Systems: The Large-scale Renewable Energy Integration Challenge,* pp. 85-109, 2019.
[65] 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.
[66] L. Langer, F. Skopik, P. Smith, and M. Kammerstetter, "From old to new: Assessing cybersecurity risks for an evolving smart grid," *computers & security,* vol. 62, pp. 165-176, 2016.
[67] J. Jarmakiewicz, K. Maślanka, and K. Parobczak, "Development of cyber security testbed for critical infrastructure," in *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, 2015: IEEE, pp. 1-10.
[68] 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.

[69] T. T. Khoei, H. O. Slimane, and N. Kaabouch, "A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions," *arXiv preprint arXiv:2207.07738*, 2022.

[70] Y. Chi, Y. Xu, C. Hu, and S. Feng, "A state-of-the-art literature survey of power distribution system resilience assessment," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, 2018: IEEE, pp. 1-5.

[71] S. Bologna, A. Fasani, and M. Martellini, "Cyber security and resilience of industrial control systems and critical infrastructures," in *Cyber security: Deterrence and IT protection for critical infrastructures*: Springer, 2013, pp. 57-72.

[72] F. A. Rahim, N. A. Ahmad, P. Magalingam, N. Jamil, Z. C. Cob, and L. Salahudin, "Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach," *International Journal of Sustainable Construction Engineering and Technology*, vol. 14, no. 3, pp. 210-220, 2023.

[73] 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.

[74] 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.

[75] J. Jasiūnas, P. D. Lund, and J. Mikkola, "Energy system resilience–A review," *Renewable and Sustainable Energy Reviews*, vol. 150, p. 111476, 2021.

[76] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011: IEEE, pp. 1-7.

[77] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1552-1564, 2020.

[78] 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.

[79] 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.

[80] T. Bragatto *et al.*, "Assessment and possible solution to increase resilience: Flooding threats in Terni distribution grid," *Energies*, vol. 12, no. 4, p. 744, 2019.

[81] 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.

[82] M. Alonso, J. Turanzas, H. Amaris, and A. T. Ledo, "Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks," *Sensors*, vol. 21, no. 17, p. 5826, 2021.

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

[84] 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.

[85] 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.

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

[87] M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in *2016 IEEE international conference on smart grid communications (SmartGridComm)*, 2016: IEEE, pp. 435-440.

[88] V. Demertzi, S. Demertzis, and K. Demertzis, "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities," *Applied Sciences*, vol. 13, no. 2, p. 790, 2023.

[89] 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.

[90] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modeling and security of cyber-physical systems in smart grids," *Energy Conversion and Economics*, vol. 2, no. 4, pp. 197-211, 2021.

[91] 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.

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

[93] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in PMU-based power network and countermeasures," *IEEE Access*, vol. 6, pp. 65594-65603, 2018.

[94] K. Mitsarakis, "Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures," 2023.

[95] 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.

[96] P. Chopade and M. Bikdash, "New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts," *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 29-45, 2016.

[97] C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the US electric sector," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.

[98] A. Teixeira, F. Kupzog, H. Sandberg, and K. H. Johansson, "Cyber-secure and resilient architectures for industrial control systems," in *Smart Grid Security*: Elsevier, 2015, pp. 149-183.

[99] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyzing vulnerability in power system," *Reliability Engineering& System Safety*, vol. 183, pp. 153-172, 2019.

[100] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions," *Energies*, vol. 15, no. 18, p. 6799, 2022.