Scan to know paper details and author's profile

Assessment of Cybersecurity Deployment to Power System Smart Grid

Adeloye A.A, Abood S.I, Annamalai A, Butler-Purry K & Chouikha M.F

A&M University, Texas

ABSTRACT

This comprehensive study delves into the multifaceted landscape of modern power systems, encompassing their intricate infrastructure, the integration of smart grid technology for optimized energy management, the critical significance of cybersecurity in safeguarding against a plethora of cyber threats, and the identification of gaps in the deployment of effective cybersecurity measures. The investigation delves into three primary deployment clusters, focusing on system operation continuity protection, network security, and data protection, each pivotal in ensuring smart grids' secure and seamless operation. Moreover, the study underscores the importance of frequency bias tie line control in maintaining stability within interconnected grids and addresses the evolving tactics of cyber attackers in exploiting vulnerabilities in power systems.

By assessing recent cyber-physical compromise incidents and their cascading consequences, the research highlights the urgency of robust defense strategies and the need for international collaboration in strengthening the resilience of power system smart grids.

Index terms: cybersecurity, cyber-threats, cyber- physical compromise, power system stability, critical infrastructure, smart grid.

Classification: LCC: QA76.9.A25

Language: English

Great Britain Journals Press

LJP Copyright ID: 392952
Print ISSN: 2631-8474
Online ISSN: 2631-8482

London Journal of Engineering Research

Volume 23 | Issue 4 | Compilation 1.0

Assessment of Cybersecurity Deployment to Power System Smart Grid

Adeloye A.A[α], Abood S.I[σ], Annamalai A[ρ], Butler-Purry K,[Ѡ] & Chouikha M.F[¥]

ABSTRACT

This comprehensive study delves into the multifaceted landscape of modern power systems, encompassing their intricate infrastructure, the integration of smart grid technology for optimized energy management, the critical significance of cybersecurity in safeguarding against a plethora of cyber threats, and the identification of gaps in the deployment of effective cybersecurity measures. The investigation delves into three primary deployment clusters, focusing on system operation continuity protection, network security, and data protection, each pivotal in ensuring smart grids' secure and seamless operation. Moreover, the study underscores the importance of frequency bias tie line control in maintaining stability within interconnected grids and addresses the evolving tactics of cyber attackers in exploiting vulnerabilities in power systems.

By assessing recent cyber-physical compromise incidents and their cascading consequences, the research highlights the urgency of robust defense strategies and the need for international collaboration in strengthening the resilience of power system smart grids. This comprehensive analysis culminates in a resounding call for fortified cybersecurity frameworks to safeguard the reliability of power supply in the face of evolving cyber threats.

Index terms: cybersecurity, cyber-threats, cyber-physical compromise, power system stability, critical infrastructure, smart grid.

Author α σ ρ Ѡ ¥*:* Department of Electrical and Computer Engineering, Prairie View A & M University, Texas.

Ѡ*:* Department of Electrical and Computer Engineering, Texas A & M University, Texas.

I. INTRODUCTION

1.1 Power Systems Architecture

The power system forms the electricity infrastructure backbone, enabling a reliable electricity supply to homes, businesses, and industries [1] [2].

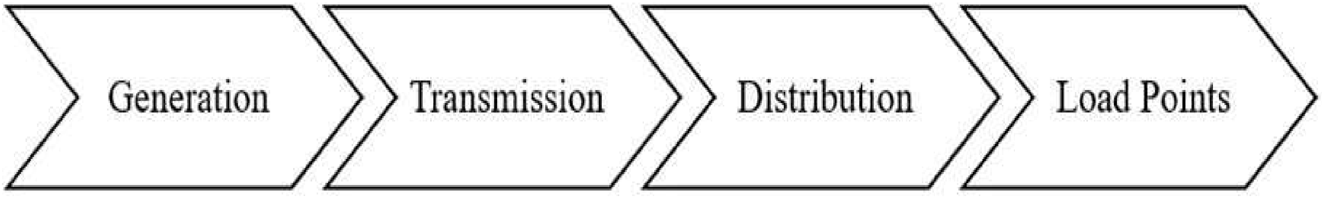

Figure 1: Block Diagram of a Basic Power System

The block diagram described in Figure 1 represents a complex power system network that delivers electricity from power plants to end-users. It comprises generation, transmission, and distribution infrastructure, which requires careful planning, operation, and maintenance for a reliable and resilient power supply [3]. High-voltage transmission lines interconnect different regions, efficiently transferring electricity. Substations step down the voltage for distribution through lower-voltage power lines to individual consumers [4].

System operators manage and coordinate power system operations to maintain stability and address imbalances [5]. Increased demand for electricity, the integration of renewable energy sources, and the need for grid modernization are some of the complexities that have impacted the conventional power system architecture. and the need for real time operational monitoring and control. Consequently, there is a heightened need for real-time operational monitoring and control to address these challenges.

1.2 Smart Grid Overview

The smart grid integrates digital technologies into energy management, enabling real-time monitoring and control of electricity flows [6]. It facilitates two-way communication between power providers and consumers, optimizing energy demand and supply. The Advanced Metering Infrastructure (AMI) provides real-time energy usage data to consumers for informed decisions. Distribution automation enhances grid reliability by deploying sensors and intelligent switches [7] [8]. The smart grid prioritizes grid resilience and security through redundancy and cybersecurity measures. Demand-side management strategies encourage consumers to adjust energy consumption behaviors, reducing peak demand [9].

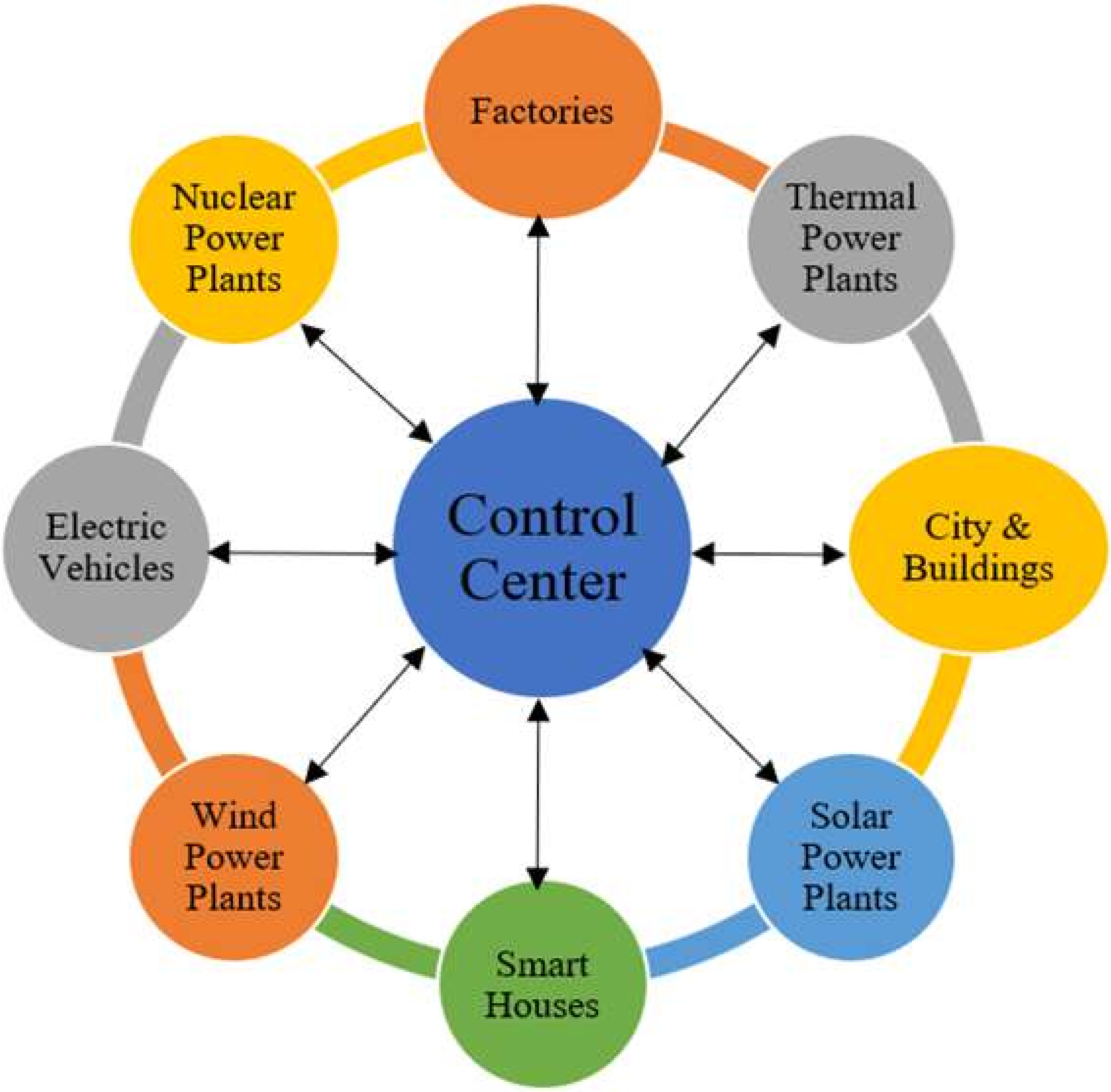

Figure 2: A Block Diagram of the Smart Grid Process Flow

Figure 2 illustrates a block diagram of a smart grid process flow. Electric vehicle (EV) integration employs smart charging infrastructure based on grid conditions and user preferences [10]. Smart grid analytics analyze sensor data, aiding optimization and predictive maintenance. Interoperability is maintained through common standards for seamless integration of devices and systems [11]. The smart grid supports renewable energy integration, microgrids, and storage, promoting sustainability, efficiency, and energy independence [4].

1.3 Significance of Cybersecurity to Smart Grid

Cybersecurity in power system smart grids encompasses various measures and technologies designed to protect critical infrastructure from cyber threats while ensuring a sustained grid operation [12]. One type of cybersecurity measure is network security, which involves securing communication networks and data transmission channels within the smart grid, and includes implementing firewalls, secure gateways, and virtual private networks (VPNs) to prevent unauthorized access and protect against network-based attacks [13]. Another important type is application security, which focuses on securing the software applications and control systems used in power system smart grids [14].

Application security involves implementing secure coding practices, conducting regular vulnerability assessments, and ensuring the integrity and authenticity of software updates [15]. The primary objective of this publication is to explore three primary deployment clusters of cybersecurity that directly impacts smart grids. The ultimate purpose for this is to identify successful technological measures for addressing vulnerabilities arising from specific types of cyberattacks on the smart grid.

II. LITERATURE REVIEW

2.1 Cybersecurity Deployment Clusters that are Smart Grid Focused

The deployment of cybersecurity measures spans various spheres to ensure comprehensive protection against cyber threats [16]. Three primary deployment categories directly impacting the smart grid's smooth operation were identified and briefly examined from twenty-three general cybersecurity protection measures examined. This was after the long list of measures was categorized into groups with primary focus areas as identified in Table 1:

Table 1: Cybersecurity Deployment Clusters

1	Target System Operation Assurance
2	Risk Management and Policy
3	Network Security
4	Software Application & Management
5	Data Protection
6	Human Capital Security Awareness & Collaboration

The first is the system operation continuity protection which upholds uninterrupted smart grid operation, safeguarding against cyber threats that could disrupt power delivery. Measures include redundancy in critical components, real-time monitoring, and incident response plans to ensure uninterrupted power supply [17] [5]. Network security which is the second, involves securing communication pathways between grid components to prevent unauthorized access and data maniPulation.

Techniques such as firewall deployment, intrusion detection systems, and encrypted communication protocols are used to shield against cyberattacks [15]. Data protection which is the third, ensures the confidentiality and integrity of sensitive information exchanged within smart grid systems [18]. Encryption mechanisms, access controls, and data loss prevention techniques are implemented to prevent unauthorized access and ensure critical data's safe transmission and storage [8]. Based on which of the three clusters might likely result in system fatality, a research decision was taken to focus on the impact of the system operation continuity protection.

2.2 Specific Aspects of Cybersecurity Protection in Smart Grid

A few cybersecurity protection aspects were closely studied regarding system operation continuity protection. A major factor that informed this cluster selection from the three closely studied is the importance of an uninterrupted smart grid operation in the event of a cybersecurity threat. Afterward, three specific cybersecurity protection aspects against system operation discontinuity were selected and closely examined.

The first was anomaly detection and behavioral analytics, which involves utilizing advanced technologies like machine learning to identify unusual behavioral patterns within the smart grid system that might indicate a cyber threat [14] [16]. Security measures to physically protect critical infrastructure components from unauthorized access or tampering, such as secured access points and surveillance systems, were studied [19]. The third was business continuity planning which entails developing strategies and plans to ensure the continued operation of the smart grid in the face of cyber incidents, aiming to minimize downtime and maintain power supply reliability [9].

III. METHODOLOGY

This study utilized a comprehensive approach to analyze each study section. Relevant sources [15] [17] were carefully identified, and important research events were closely observed, including recent publications relating to cybersecurity deployment to the smart grid [20] [10] [17]. This survey identified and closely studied three primary deployment clusters of cybersecurity crucial to the smart grid.

The publication then focused specifically on one within the examined group of clusters. Afterward, it delved into specific aspects of cybersecurity deployment to the smart grid, emphasizing the top three that may directly impact the power supply. The significance of frequency as a key power system stability parameter is emphasized, particularly regarding smart grid stability and protection. The content also involves analyzing recent cyber-physical compromise incidents in power systems' smart grids and addressing vulnerabilities in the deployment of cybersecurity for smart grids.

3.1 *Criticality of Frequency Bias Tie Line Control to Smart Grid Stability*

Among the vital power system stability parameters, a frequency common to the three closely examined aspects holds the utmost significance, aside from voltage magnitude and rotor angle [5]. Frequency bias tie line control is used in power systems to maintain stable frequency across interconnected grids by adjusting power flow between them in response to frequency deviations caused by load changes or disturbances [3]. Generators in one grid increase or decrease power output based on the frequency difference between interconnected grids, with adjustments proportional to a predetermined frequency bias coefficient [17].

This control mechanism helps restore frequency balance and stability, preventing cascading failures and blackouts. By coordinating power flow adjustments, frequency bias tie line control contributes to grid reliability and effective load management [5] [2]. This technique is essential to power systems operation, especially in interconnected smart grids where maintaining frequency stability is crucial for preventing widespread grid failures [17]. For a network of interconnected tie lines within a smart grid, active power P (W) varies linearly with frequency $f(Hz)$. The $P - f$ relationship is described by the expression in equation (1) [20].

$$\frac{\Delta P}{\Delta f} =- k \qquad (1)$$

Where k is a constant (frequency bias factor) dependent upon the system's load and governing characteristics in $\frac{MW}{Hz}$.

ΔP is the change in active power, Δf is the change in frequency and ΔP_{total} is the total active power change within an interconnected system [5]. For an isolated system, equation (2) holds true

$$\Delta P + k\Delta f = 0 \qquad (2)$$

However, for N interconnected system elements, equation (1) is expanded to equation (3)

$$\Delta P_{total} = \Delta P_1 + \Delta P_2 + ...\Delta P_N$$

$$= -\ k_1 \Delta f - k_2 \Delta f - \ldots k_N \Delta f$$

$$= \ -\ \left(k_N\right) \Delta f \qquad (3)$$

Equation (3) represents the system stiffness. This is the relationship between power change and frequency change in an interconnected system, with a stiffer system exhibiting smaller frequency changes for a given load change [20].

VI. DISCUSSION

4.1 Analysis of Recent Cyber-physical Compromise Incidents in Power Systems Smart Grid

Analysis of recent cyber-attacks on power system smart grids sheds light on the evolving landscape of cyber threats and their impact on critical infrastructure [20] [9]. Several high-profile cyber-attacks on power system smart grids, such as the Ukraine power grid attack in 2015 and the Not Petya malware attack in 2017, have demonstrated the potential consequences of successful cyber intrusions [17]. These attacks targeted the control systems and communication networks of power grids, causing widespread power outages, disruptions to critical services, and financial losses [21]. The methods employed in recent cyber-attacks on power system smart grids include phishing attacks, malware infections, exploitation of vulnerabilities in software and hardware, and supply chain attacks.

Sophisticated threat actors, including state-sponsored groups and cybercriminal organizations, are responsible for orchestrating these cyber-attacks, highlighting the need for robust defense measures [22]. Cyber-attacks' impact on power system smart grids goes beyond financial losses, as they can have severe implications for public safety, national security, and economic stability [19]. These impacts on power grids can disrupt essential services, such as healthcare, transportation, and communication, leading to social and economic upheaval. The analysis of recent cyber-attacks highlights attackers' growing sophistication and persistence as they continually adapt their tactics to exploit vulnerabilities in power system smart grids [16]. The consequences of cyber-attacks on power grids extend to reputational damage for the affected organizations and erode public trust in the reliability of the power supply.

4.2 Existing Vulnerabilities in the Deployment of Cybersecurity for Smart Grid Protection

Incident response and recovery efforts in the aftermath of cyber-attacks on power system smart grids involve extensive forensic investigations, system restoration, and strengthening of security measures [23]. The recent cyber-attack analysis pinpoints current deficiencies in the deployment of cybersecurity for smart grid protection – beginning from the control and communication systems which were the identified targets [24].

Other gaps include the need for proactive defense strategies, continuous monitoring, threat intelligence sharing concerns, vulnerability assessments, differing priorities, regulatory complexities, limited resources, technological and cultural differences

Collaboration between government agencies, power utilities, and cybersecurity experts is also crucial in mitigating the effect of cyber-attacks and strengthening the resilience of power system smart grids [25]. Lessons from recent cyber-attacks inform the development of robust cybersecurity frameworks, regulations, and industry standards for power system smart grids.

The event also highlights the importance of educating personnel and end-users about cyber threats, promoting a security culture, and fostering resilience against potential attacks [26]. Technological advancements, such as integrating artificial intelligence and machine learning, can aid in early detection and response to cyber threats targeting power system smart grids. International cooperation and information-sharing platforms facilitate a coordinated response to cyber-attacks on power grids, enabling the exchange of best practices and threat intelligence [27].

V. CONCLUSION

The foundation of a robust electricity supply lies in a well-structured power system that caters to the energy needs of homes, businesses, and industries. As depicted in Figure 1, this intricate network involves multiple components working in tandem to ensure a seamless flow of electricity.

Integrating smart grid technology further optimizes this operation, allowing real-time monitoring, communication, and efficient energy management. Ensuring cybersecurity protection in smart grids is paramount, as demonstrated by the critical significance of frequency, voltage magnitude, and rotor angle in maintaining system stability. Completing comprehensive cybersecurity measures, focusing on system operation continuity protection, network security, and data protection, is a crucial defense against cyber threats in this modern energy landscape.

ACKNOWLEDGEMENT

The efforts of my supervisors, Prof. Annamalai. A, Prof. Chouikha M.F, Dr. Abood S.I, as well as the external collaborator on this project, Prof. Butler-Purry K. are acknowledged and greatly appreciated. Thank you for the painstaking reviews, useful research guidance and career counsel. My sincere appreciation is extended to the 2023 TAMU – PVAMU PRISE (Panther Research & Innovation for Scholarly Excellence) Grant Program for sponsoring this research endeavor.

REFERENCES

1. I. Irene, "Cybersecurity Concerns on Real-time Monitoring in Electrical Transmission and Distribution Systems (SMART GRIDS)," 2020.
2. A. Michael, V. Venkatesh, and M. Richard, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," IEEE Access, Vol. 10, pp. 99875-99896, 2022.
3. S. Dhaou, "A Survey on Information Communication Technologies in Modern Demand-Side Management for Smart Grids: Challenges, Solutions and Opportunities.," IEEE Engineering Management Review, Vol. 51, No 1, pp. 76-107, 2023.
4. K. Tim, E. Raphael, K. Benedikt, H. Immanuel, and H. Martin, "Cybersecurity in Power Grids: Challenges and Opportunities," MDPI Sensors, pp. 2-19, 2021.
5. N. A. Ahmad, A.-K. Saif, and M. Qaraqe, "Anomaly Detection in Smart Grids: A Survey From Cybersecurity Perspective," International Conference on Smart Grid and Renewable Energy (SGRE), 2022.
6. M. Amira and G. Gibin, "Smart Grid - Evaluation and Review," International Conference on Smart Grid and Renewable Energy (SGRE), vol. 3, 2022.
7. E. M. C. Balduino, I. Loretta and P. Dan, "Cyber Security of Smart Grid Infrastructure," pp. 303-308, 2018.
8. H. Burhan and G. Manimaran, "A Novel Methodology for Cybersecurity Investment Optimization in Smart Grids Using Attack-Defense Trees and Game Theory," IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5, 2022.
9. P. Dimitrios, S. Panagiotis, L. Thomas and G. S. Antonios, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Communications Surveys & Tutorials, Vol. 22, No. 3, pp. 1942-1976, 2020.
10. M. Fazel, S. Mehrdad, A. Majid, and S. Bahram, "A Review of Cyber-Resilient Smart Grid," World Automation Congress (WAC), IEEE Xplore, pp. 11-15, 2022.
11. I. K. Asif and P. Deepak, "A Review of Cyber Securities in Smart Grid Technology," 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), vol. 2, pp. 151-156, 2021.
12. S. Salsabeel, Q. Fatma, A. Raafat, A. Fadi Aloul, and A. Ali, "Smart Grid Cyber Security: Challenges and Solutions," International Conference on Smart Grid and Clean Energy Technologies, pp. 170-175, 2015.
13. Z. Peng, Z. Talha, and L. Hao, "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," IEEE Transactions on Industrial Informatics, Vol. 17, No. 1, pp. 3-19, 2021.
14. Z. Zhiheng and C. Guo, "An Overview of Cyber Security for Smart Grid," pp. 1128-1131, 2018.

15. D.-G. Vasco, F. M. Joao, L. Celson and N. B. Paul, "Smart Grid Security Issues," pp. 534-538, 2015.
16. R. V. Taylor and V. Andrew, "Cybersecurity in the Blockchain Era," A Survey on Examining Critical Infrastructure Protection with Blockchain-Based Technology, pp. 107-112, 2020.
17. D. T. Nguyen, S. Q. Nguyen, B. L. Vo, V. T. Vu, and F. Goro, "A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy," IEEE Access (IEEE Power & Energy Society Section), pp. 35846-35875, 2022.
18. Y. Ye, Q. Yi, S. Hamid, and T. David, "A Survey on Cyber Security for Smart Grid Communication," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998-1010, 2012.
19. U. R. Poojith, S. Balwinder and S. Ranjana, "Cyber Security Enhancement of Smart Grids Via Machine Learning - A Review," 21st National Power Systems Conference (NPSC), no. 21, 2020.
20. R. Syed, S. Mark, M. Jimmy, and S. John, "Application of Artificial Intelligence to Network Forensics: SUrvey, Challenges, and Future Directions," IEEE Access, Vol 10, pp. 110362-110384, 2022.
21. D. Sourav and S. Ranjana, "A Simple Cyber Attack Detection Scheme for Smart Grid Cyber Security Enhancement," National Power System Conference (NPSC), vol. 21, 2020.
22. K. Vatan and C. P. Gupta, "Cyber Security Issue in Smart Grid," IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), pp. 1-9, 2021.
23. S. Shahriar, B. Sahba, A. Thnwa and M. Samantha, "Smart Grid and Cybersecurity Challenges," IEEE, vol. 5, pp. 1-8, 2020.
24. N. N. Tu, L. Bing-Hong, N. Nam P and C. Jung-Te, "Cyber Security of Smart Grid: Attacks and Defenses," 2020.
25. S. I. Abood, Power System Generation, Stability and Control, Australia: Central West Publishing, 2021.
26. F. John, P. Obiomon and S. I. Abood, Power System Operation, Utilization and Control, Florida: CRC Press, 2023.
27. S. I. Abood and M. H. Fayyadh, Philosophy of Power System Protection and Security, New York: Nova Science, 2021.

This page is intentionally left blank