Towards Developing an Asset-Criticality Identification Framework in Smart Grids

Yazeed Alrowaili
School of Computer Science & Informatics
Cardiff University
Cardiff, United Kingdom
alrowailiyf@cardiff.ac.uk

Neetesh Saxena
School of Computer Science & Informatics
Cardiff University
Cardiff, United Kingdom
saxenan4@cardiff.ac.uk

Pete Burnap
School of Computer Science & Informatics
Cardiff University
Cardiff, United Kingdom
burnapp@cardiff.ac.uk

***Abstract*—Smart Grids combine advanced communication technologies with traditional power systems, enhancing performance and reliability but also introducing cyber and physical vulnerabilities. This paper presents a comprehensive framework to identify and prioritize key assets within these interconnected layers. The proposed framework employs graph-based integration to create nodes for cyber hosts and vulnerabilities, as well as power system components, assigning specific attributes to each. The framework establishes clear connections between cyber assets and power system elements by prioritizing cyber vulnerabilities through impact scores and graph metrics like closeness centrality and identifying key power components using electric degree and betweenness centrality. Scenario simulations are utilized to evaluate the impacts of disruptions across layers, revealing potential attack pathways and assessing associated risks. This integrated approach offers a detailed analysis of interconnected vulnerabilities, aiding in the development of targeted mitigation strategies to enhance the security of the overall smart grids.**

I. INTRODUCTION

The increasing interconnection and automation of modern power systems through Information and Communication Technology (ICT) have transformed traditional power grids into Smart Grids (SGs). This integration enhances operational efficiency and reliability but also introduces new vulnerabilities [1], [2]. SGs consist of both cyber (ICT) and physical (power grid) components, forming complex, interconnected networks that require robust protection mechanisms against cybersecurity threats [3].

Understanding the interdependencies between cyber and physical layers is crucial. Several incidents highlight these risks, such as the Stuxnet worm causing physical damage to industrial systems, the BlackEnergy malware attack leading to power outages in Ukraine, and the SolarWinds attack demonstrating potential cascading failures [4]–[6]. These events underscore the need for a framework that identifies critical assets across both layers and maps potential attack paths. In 2022, a study showed how false data injection attacks could disrupt SCADA systems significantly [7]. The 2021 Colonial Pipeline ransomware attack disrupted fuel supply across the Eastern United States, highlighting infrastructure vulnerabilities [8]. Additionally, the 2021 Florida water treatment plant attack demonstrated the risks to public health from cyber threats [9]. These incidents highlight the need for an integrated approach to identify and mitigate risks in SG systems. Traditional risk assessment methods are often insufficient for such complex systems, relying on expert judgments or predefined conditions [10]. Instead, a data-driven framework is needed to accurately identify and assess critical assets, leveraging real-time information from the cyber and power system layers [11].

Detecting interdependencies between cyber and physical components is crucial for understanding cascading impacts when systems are compromised. Complex network analysis offers a strategy to study relationships and dependencies between cross-domain system components, revealing critical nodes and links whose failure could cause significant disruptions [12], [13]. Modern power systems, viewed as complex networks, represent components like generators and substations as nodes, and transmission lines as edges [10], [14]. In the ICT layer, network analysis, anomaly detection, intrusion detection, and vulnerability assessment can identify critical nodes [15]. Topological and flow-based metrics help prioritize security by identifying critical nodes. Analyzing interactions between cyber and physical components is essential for identifying vulnerabilities and developing security measures [16].

Therefore, this paper aims to build a comprehensive framework for physical and cyber layers in SGs. To the best of our knowledge, this is the first work that uses a graph-based model for the integration of cyber and physical layers to assess asset criticality. The key contributions of this paper are:

- Developed CPSs Graph-Based Model: The model helps to integrate component systems and identify critical paths and critical assets.
- Identification of Critical Assets (Physical Layer): Constructing a graph for physical layer and employing topological power metrics to identify critical power components.
- Identification of Critical Assets (Cyber Layer): Classifying assets in the cyber layer, assigning vulnerabilities, and mapping potential attack paths.
- Integrated Analysis: Combining the analyses of both layers into a single comprehensive view that highlights the critical interdependencies and vulnerabilities within the SG infrastructure.

II. Related work

Several existing frameworks for criticality assessments in Cyber-Physical Systems (CPSs) have been proposed. However, current research has not adequately addressed the open issues discussed earlier. Existing frameworks typically focus on identifying critical assets within a specific domain, such as electric systems or cyber assets, without considering the interdependencies between cross-domain assets linking the cyber and power layers. For instance, Aghabegloo et al. proposed a BIA-based quantitative framework for analyzing the criticality of built physical assets, focusing on sustainability and resilience [17]. While this framework effectively assesses physical assets, it does not account for the interconnected nature of cyber and physical systems in SG. Alvarez et al. introduced a conceptual model for asset management in electrical systems, emphasizing the management of physical infrastructure [18]. Although comprehensive in addressing electrical systems, this framework lacks the integration of cyber assets and the potential vulnerabilities arising from cyber-physical interdependencies. Rahman et al. presented a graph-theoretic approach for modeling and assessing cyber-security risks in manufacturing systems [19]. This approach highlights the importance of understanding cyber threats and vulnerabilities but does not extend its analysis to the physical impacts on interconnected components in an SG context. Le et al. conducted a CVSS-based attack analysis using a graphical security model, applying it to an SG case study [20]. While this work focuses on cyber threats within SGs, it primarily considers cyber assets and does not thoroughly examine the physical consequences of cyber incidents on the power infrastructure.

Many frameworks focus on business impact analysis, evaluating the functionality, health, and maintenance of physical assets. They often assess the economic outcomes of asset failures or the operational status of physical components. While important, these aspects do not address vulnerabilities arising from cyber-physical interdependencies.

Conversely, some frameworks exclusively address the criticality of compromised cyber assets by examining attack paths, identifying vulnerabilities, and considering potential attacks [21], [22]. These analyses are valuable for understanding cyber threats but fall short in evaluating the physical consequences of interconnected physical components.

A significant gap in existing research is the lack of a comprehensive framework that integrates both cyber and physical dimensions to assess the criticality of assets. Current methodologies do not sufficiently account for how cyber incidents can propagate through interconnected systems and affect physical infrastructure, highlighting the need for a new approach.

III. Proposed framework, Integrated Graph-Based Model and vulnerability analysis

A. Proposed Framework

The proposed framework integrates the cyber and power system layers to provide a holistic view of asset criticality within SGs. This integration is achieved through a series of steps involving data collection, graph construction, vulnerability assessment, and analysis of interdependencies as shown in Figure 1.

1) Pre-Processing and Information Gathering: Pre-processing and information gathering form the foundation of the proposed framework, providing essential data to model the SG's cyber and power infrastructure accurately.

Active Discovery: This step involves collecting detailed information about network hosts, including IP addresses, operating systems (OS), open ports, and services. Network scanning tools like Nmap [23] identify active devices, open ports, running services, and OS details. Service enumeration tools such as Metasploit and Nessus gather detailed information about running services and potential vulnerabilities [24]. **Passive Discovery:** This approach involves monitoring network traffic to identify communication links between hosts without actively probing the network, thus avoiding disruptions, especially in OT environments. Network traffic analysis tools like Wireshark and Zeek capture and analyze traffic, detect anomalies, and map communication patterns [24]. Flow monitoring techniques such as NetFlow and sFlow collect data from network devices, providing an overview of traffic patterns and identifying key communication paths and potential choke points [25]. **Power System Discovery:** This step involves identifying and collecting data from power system components such as buses, transmission lines, and transformers, including their power measurements. PowerWorld Simulator and its SimAuto API are used to extract this information, modeling these components as nodes and edges in the graph [26]. PowerWorld Simulator provides detailed insights into the electrical grid's behavior, helping to identify critical nodes (buses) and edges (transmission lines and transformers). The SimAuto API allows for automated extraction of data from PowerWorld simulation cases, including power measurements, bus information, and connectivity of transmission lines and transformers, which are then used to build the power system graph.

2) Graph Modelling: Graph modelling is a crucial step in representing the interconnected components of the SG's cyber and power systems. This step involves constructing individual graphs for the cyber and power layers and then integrating them to analyze interdependencies.

In the **cyber layer**, nodes represent hosts (e.g., servers, routers, control systems) and vulnerabilities (e.g., specific software flaws or misconfigurations). Edges represent communication links between hosts (e.g., network connections) and the links between vulnerabilities and the hosts they affect. Each node and edge in the cyber graph can have attributes such as the type of host, the nature of the vulnerability, the protocol used for communication, and the likelihood of a vulnerability being exploited. In the **power system layer**, nodes represent power system components such as buses, substations, generators, and transformers. Edges represent physical connections such as transmission lines and transformers, with attributes including power flow, voltage levels, and line impedance.

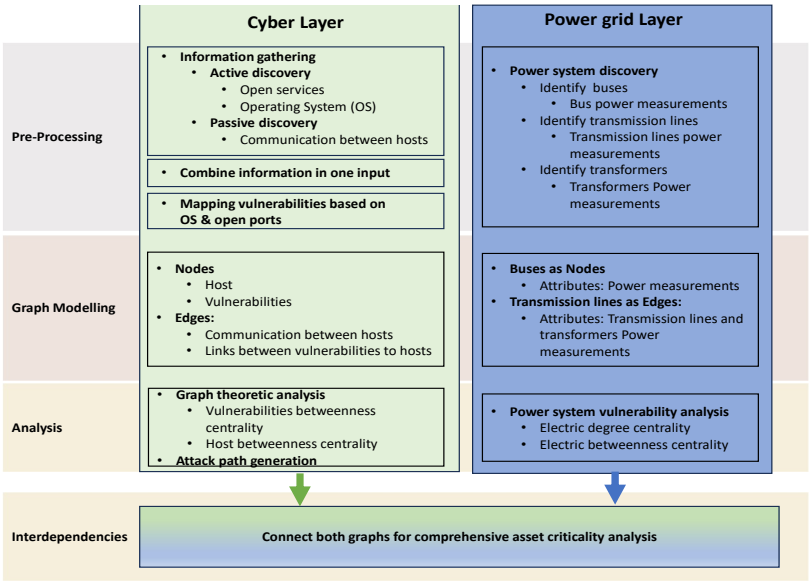

Fig. 1. The proposed framework of critical assets identification in cross-domain ICT and power systems.

Nodes and edges in the power layer are assigned attributes such as power measurements, operational status, and capacity.

3) Graph Analysis: Graph analysis involves applying various metrics to the constructed graphs to identify critical nodes and edges, understand network vulnerabilities, and assess potential attack paths. This analysis is crucial for understanding the resilience and robustness of the SG infrastructure.

Cyber Layer Analysis: Betweenness Centrality (BC) measures a node's importance by the frequency it appears on the shortest paths between other nodes [15]. Vulnerability BC identifies vulnerabilities existing on hosts that appear on many shortest paths in the network, indicating their critical role in communication. High BC for a vulnerability suggests its potential for widespread disruption if compromised. Host BC applies to network hosts, highlighting critical nodes for communication that, if compromised, could impact network integrity. Attack path mapping involves identifying possible routes for attackers using techniques like attack trees and Bayesian networks. Critical asset identification uses graph-theoretic metrics to identify high-impact assets, prioritizing them for security enhancements. **Power System Analysis:** Electric degree centrality measures the number of direct electrical connections a node has within the power system. Nodes with high electric degree centrality are vital for power distribution and their failure can cause significant disruptions. Electric BC evaluates the importance of nodes based on power flow. Nodes with high electric BC are crucial for maintaining grid stability, as they lie on many shortest paths for power flow. Their failure could result in widespread and cascading outages.

4) Interdependencies Analysis: **Understanding Cross-Domain Impacts:** The analysis examines how vulnerabilities in the cyber layer can affect the power layer and vice versa. This involves understanding the interdependencies between the two layers and how an issue in one layer can propagate to the other. For example, a relay (cyber node) that controls a transmission line (physical edge) will have an edge representing this control relationship. The combined graph thus includes edges that connect cyber nodes, illustrating how cyber vulnerabilities can impact physical systems. Techniques such as dependency graphs and multi-layer network analysis are used to model these interdependencies. **Comprehensive Vulnerability Assessment:** The comprehensive graph provides a unified view of the SG's vulnerabilities, helping to identify critical assets that are vulnerable to attacks from multiple vectors. This holistic approach ensures that all potential vulnerabilities are considered, and the most critical assets are prioritized for protection.

The framework uses integrated data collection and graph modeling for seamless integration and sub-network analysis. Graph modeling handles large, complex networks effectively and can add attributes to each node for localized microgrid analysis, and dynamic configuration. This scalability makes the framework suitable for complex smart grids, microgrids, and advanced control systems.

B. Integrated Graph-Based and Vulnerability Analysis

A network can be presented as a connected graph $G\{V, E, W\}$, where $G(V)$ represents vertices (nodes) and $G(E)$ represents edges (connections) that link nodes together. Edges can include weights, represented as $G(W_{v1,v2})$ indicating the strength of the connection. Complex network analysis uses topological metrics to determine node criticality. **Node Degree Centrality** assigns importance based on the number of links a node has, with highly connected nodes deemed critical [10].

1) Power System Vulnerabilities Assessment In Integrated Graph-Based: Utilizing graph theory to assess power system

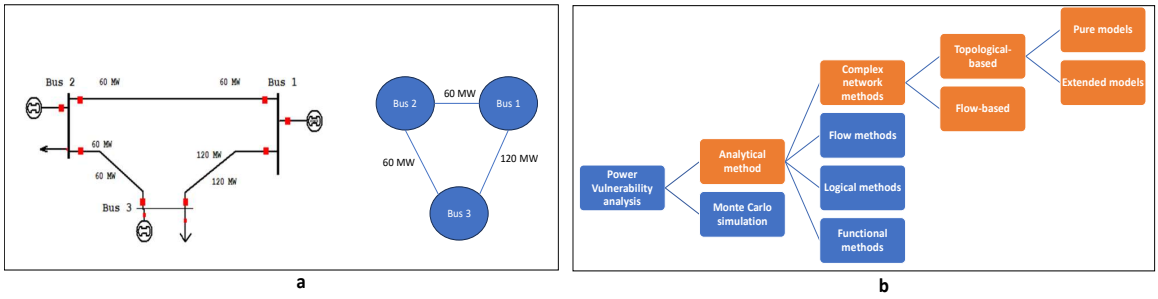

Fig. 2. Power system representation as graph-based with buses as nodes and transmission lines as edges **(a)**. Different methods for power vulnerability analysis **(b)**

vulnerabilities has gained importance recently [27]–[29]. This method identifies components likely to fail (e.g., transmission lines, substations) and provides scalable analysis for large networks. Figure 2 (b) illustrates the types of vulnerability assessments used.

In complex network vulnerability analysis, power components like substations, generators, and loads are nodes, while transmission lines and transformers are edges connecting power buses (Figure 2 (a)). Analysis can use pure topological methods or extended approaches including electrical attributes as network weights. However, this analysis often focuses on physical components, ignoring compromised cyber components linked to these systems.

2) ICT Vulnerabilities Assessment In Integrated Graph-Based: Vulnerability assessment in ICT can be performed using graph theory by modeling links between assets and associated vulnerabilities [30], [31]. This involves documenting ICT topology to represent nodes (e.g., hosts and their vulnerabilities) through network active identification, which includes information about hosts like IP addresses, OS, open ports, and services. Another method is identifying host connections by passively monitoring network traffic to establish edges (communication protocols) in the graph.

Identifying critical ICT components involves using graph theory topological metrics to find critical vulnerabilities, such as BC to locate vulnerabilities acting as bridges between assets. These vulnerabilities could lead to widespread exploitation if compromised. By examining assets connected to critical vulnerabilities, critical assets can be determined, as they are more vulnerable to potential attacks.

IV. Demonstration and Example of the Proposed Framework

The following section demonstrates the application of the proposed framework for critical asset identification in a SG, using the Ukraine cyber attack as a case study. The attack steps included initial access via spear-phishing and credential theft, remote access via VPN, lateral movement within the network, deployment of KillDisk malware on SCADA hosts, and manipulation of control systems to open breakers, causing widespread outages by disrupting communication between SCADA systems and RTUs/PLCs and impacting physical components like transformers and substations [32].

A. Pre-Processing and Information Gathering

In the cyber layer, information was gathered to mimic the cyber infrastructure similar to the Ukraine cyber attack scenario. In the power and OT assets layer, buses serve as main distribution points for electrical power, feeders distribute power from substations to consumers, and transformers and substations regulate voltage and power distribution.

B. Graph Modelling

1) Cyber Layer and Analysis: The cyber layer visualization (Figure 3) shows IP addresses representing hosts or devices in the power system infrastructure, each managing the grid. Detailed breakdown: 192.168.1.1 hosts SCADA1 and RTU1; 192.168.1.2 hosts SCADA2 and PLC1; 192.168.1.3 hosts RTU2 and PLC2; 192.168.1.4 hosts SCADA3; 192.168.1.5 hosts SCADA4 and RTU3; 192.168.1.6 hosts SCADA5; 192.168.1.7 hosts HMI1, VPN1, and UPS1. These IPs represent devices and systems similar to those in the Ukraine power grid cyber attack. Open ports are represented as nodes to illustrate potential entry points or vulnerabilities, highlighting services and their connectivity, which is crucial for understanding the network's attack surface.

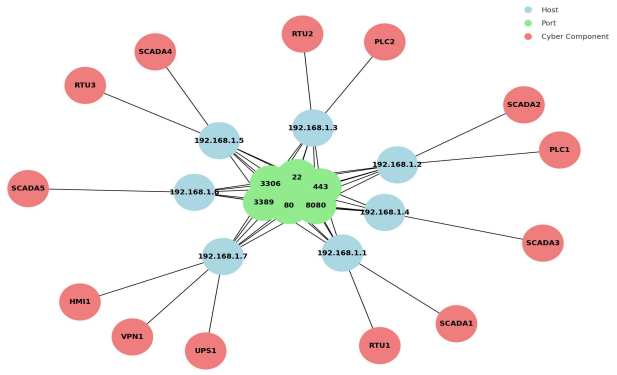

Fig. 3. Cyber layer graph

2) Power System Layer: The power system layer includes physical components as shown in Figure 4. In the Ukraine attack, once the attackers had control over the SCADA systems, they were able to manipulate these physical components, causing widespread outages.

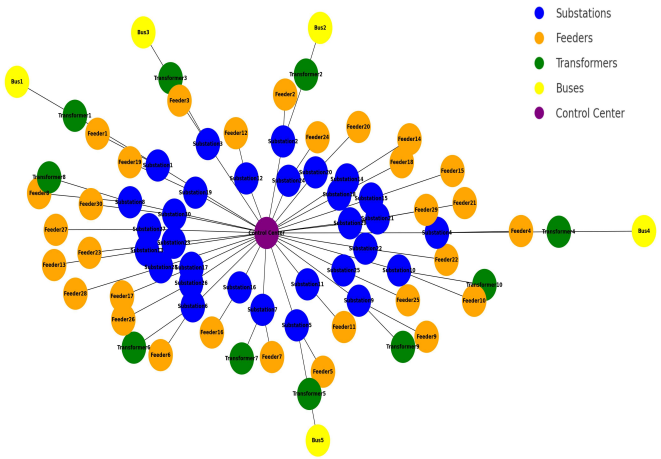

Fig. 4. Power system layer graph

3) Interdependencies and Cyber-Physical Graph: The combined graph (Figure 5) integrates the cyber and power system layers, highlighting interdependencies. The Ukraine cyber attack showed how cyber vulnerabilities can cause physical disruptions. Key interdependencies include SCADA systems to substations, communication networks to RTUs/PLCs, and VPN and remote access. The simulation considers interactions between cyber components (SCADA, RTUs, PLCs, HMIs, VPNs, UPS) and physical components (substations, feeders, transformers), showing how failures in the cyber layer can lead to cascading failures in the physical layer.

4) Detailed Diagram of Cascading Failures : The cascading failures diagram (Figure 6) illustrates how the initial cyber attack propagated through interconnected layers, leading to widespread power outages. This visualization identifies critical points of failure and the impact of compromised cyber components on physical infrastructure. Initial points of compromise include VPN and open ports, propagation through SCADA systems leads to control over substations and transformers, and cascading failures result in widespread outages as feeders and buses are disrupted.

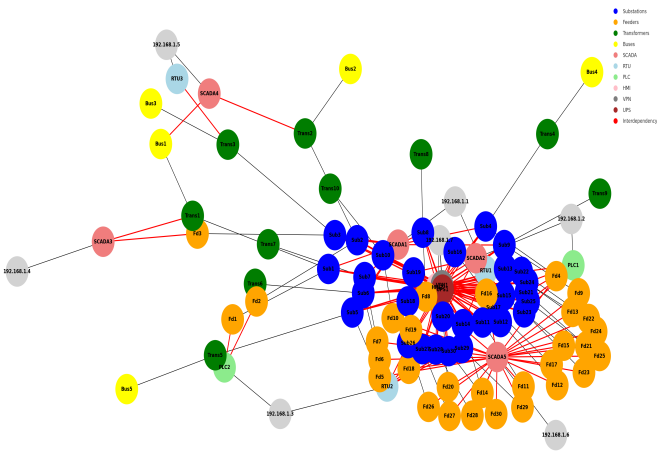

Fig. 5. Integrated Cyber-Physical graph

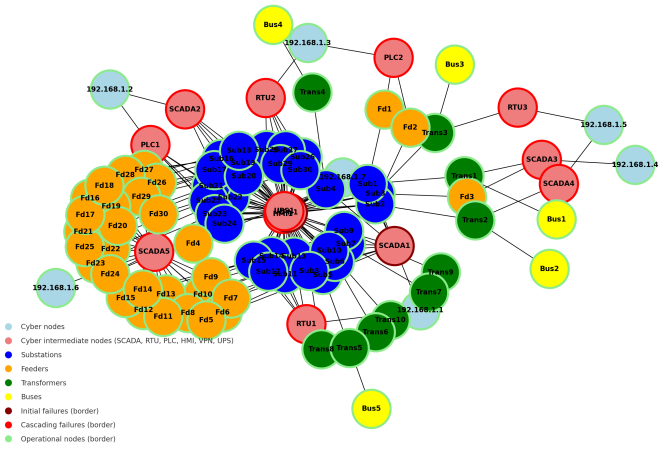

Fig. 6. Detailed diagram of cascading failures In Cyber-Physical graph

TABLE I
SUMMARY OF IDENTIFIED CRITICAL ASSETS

Type	Asset	Metric	Value
Vulnerable Cyber Assets	192.168.1.7	Vulnerabilities #	9
	192.168.1.1	Vulnerabilities #	8
	192.168.1.2	Vulnerabilities #	8
	192.168.1.3	Vulnerabilities #	8
	192.168.1.5	Vulnerabilities #	8
Critical Assets by Betweenness Centrality	192.168.1.7	BC	0.237
	192.168.1.1	BC	0.164
	192.168.1.3	BC	0.164
	192.168.1.5	BC	0.164
	192.168.1.2	BC	0.164
Critical Assets by Attack Path Frequency	VPN1	FAP	74
	Substation1	FAP	4
	Substation4	FAP	4
	Substation11	FAP	3
	Substation21	FAP	3

Table I summarizes the critical assets in the SG, categorized by their vulnerabilities, (BCs), and frequency in attack paths (FAPs). Vulnerable cyber assets, like 192.168.1.7 and 192.168.1.1, have the highest number of vulnerabilities, making them prime targets for cyber attacks. For instance, an attack path could start with initial access via VPN1, exploiting vulnerabilities in 192.168.1.7 to gain control of SCADA systems, and then manipulating RTUs/PLCs to disrupt Substation1 and Substation4, ultimately causing widespread outages. Critical assets with high BC, such as 192.168.1.7, are crucial for network communication and stability. Assets frequently appearing in attack paths, like VPN1 and key substations (Substation1, Substation4), indicate their high risk and criticality.

V. CONCLUSION

The proposed framework integrates the cyber and power grid layers, models interdependencies, and performs comprehensive asset criticality analysis. Applying this framework to the Ukraine cyber attack demonstrated its capability to identify and prioritize critical assets, enhancing grid resilience. The cyber layer includes hosts, services, and devices like SCADA systems, RTUs, PLCs, HMI, VPN, and UPS, with visualizations highlighting their relationships. The power grid layer consists of buses, transformers, and substations, showing

physical connections crucial for understanding cyber attack impacts. The combined graph illustrates layers interdependencies, showing how cyber layer failures propagate to the power grid, leading to cascading failures. The cascading failures diagram shows the attack's impact, marking failed nodes in red to identify critical points of failure and overall grid stability. Critical assets were identified using vulnerability analysis, BC, and FAPs. Vulnerable cyber assets (192.168.1.7, 192.168.1.1), were prime targets for cyber attacks. Assets with high BC (192.168.1.7), are crucial for network communication. VPN1 and key substations (e.g., Substation1, Substation4) frequently appeared in attack paths, indicating high risk. The Ukraine cyber attack simulation validated the framework's effectiveness, confirming that identified critical assets were most impacted, underscoring the framework's accuracy and reliability.

ACKNOWLEDGMENT

This work is supported by the RITICS Fellowship via NCSC, UK.

REFERENCES

[1] 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.

[2] A.-A. Bouramdane, "Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, 2023.

[3] 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.

[4] B. Bakić, M. Milić, I. Antović, D. Savić, and T. Stojanović, "10 years since stuxnet: What have we learned from this mysterious computer software worm?" in *2021 25th International Conference on Information Technology (IT)*. IEEE, 2021, pp. 1–4.

[5] O. Novikov, G. Vedmedenko, I. Stopochkina, and M. Ilin, "Cyber attacks cascading effects simulation for ukraine power grid." in *ITS*, 2021.

[6] L. Gjesvik and K. Szulecki, "Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 ukraine blackout," *European Security*, vol. 32, no. 1, pp. 104–124, 2023.

[7] E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, and S. Mekhilef, "Detection of false data injection attacks in cyber–physical systems using graph convolutional network," *Electric Power Systems Research*, vol. 217, p. 109118, 2023.

[8] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. IEEE, 2023, pp. 8–15.

[9] J. Cervini, A. Rubin, and L. Watkins, "Don't drink the cyber: Extrapolating the possibilities of oldsmar's water treatment cyberattack," in *International Conference on Cyber Warfare and Security*, vol. 17, no. 1. Academic Conferences International Limited, 2022, pp. 19–25.

[10] A. M. Amani and M. Jalili, "Power grids as complex networks: Resilience and reliability analysis," *IEEE Access*, vol. 9, 2021.

[11] X. Ma, H. Zhou, and Z. Li, "On the resilience of modern power systems: A complex network perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, p. 111646, 2021.

[12] X. Yuan, H. Wang, Y. Yuan, and S. Zhang, "Design of an intelligent decision model for power grid fault location and isolation based on topology analysis," *International Journal of Thermofluids*, vol. 21, p. 100536, 2024.

[13] 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.

[14] K. Demertzis, D. Taketzis, V. Demertzi, and C. Skianis, "An ensemble transfer learning spiking immune system for adaptive smart grid protection," *Energies*, vol. 15, no. 12, p. 4398, 2022.

[15] 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.

[16] A. Priyanka and A. Monti, "Towards risk assessment of smart grids with heterogeneous assets," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2022, pp. 1–6.

[17] M. Aghabegloo, K. Rezaie, S. A. Torabi, and S. M. Khalili, "A bia-based quantitative framework for built physical asset criticality analysis under sustainability and resilience," *Buildings*, vol. 13, no. 1, p. 264, 2023.

[18] D. L. Alvarez, L. S. Rosero, S. R. Rivera, and A. A. Romero, "A framework for asset management in electrical systems, part i: Conceptual model," in *2019 IEEE Workshop on Power Electronics and Power Quality Applications (PEPQA)*. IEEE, 2019, pp. 1–6.

[19] M. H. Rahman, E. Y. Hamedani, Y.-J. Son, and M. Shafae, "Graph-theoretic approach for manufacturing cybersecurity risk modeling and assessment," *arXiv preprint arXiv:2301.07305*, 2023.

[20] T. Duy Le, M. Ge, P. The Duy, H. Do Hoang, A. Anwar, S. W. Loke, R. Beuran, and Y. Tan, "Cvss based attack analysis using a graphical security model: Review and smart grid case study," in *Smart Grid and Internet of Things: 4th EAI International Conference, SGIoT 2020, TaiChung, Taiwan, December 5–6, 2020, Proceedings*. Springer, 2021, pp. 116–134.

[21] S. Kaliappan, V. Paranthaman, M. R. Kamal, and V. Veeramsetty, "Enhancing the resilience of industrial cyber-physical systems against external threats," in *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*. IEEE, 2023, pp. 1–6.

[22] C. Deloglos, C. Elks, and A. Tantawy, "An attacker modeling framework for the assessment of cyber-physical systems security," in *Computer Safety, Reliability, and Security: 39th International Conference, SAFECOMP 2020, Lisbon, Portugal, September 16–18, 2020, Proceedings 39*. Springer, 2020, pp. 150–163.

[23] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA, USA: Insecure, 2009.

[24] A. Kumar, "Penetration testing tools and techniques," in *Perspectives on Ethical Hacking and Penetration Testing*. IGI Global, 2023, pp. 280–306.

[25] R. Islam, V. V. Patamsetti, A. Gadhi, R. M. Gondu, C. M. Bandaru, S. C. Kesani, and O. Abiona, "Design and analysis of a network traffic analysis tool: Netflow analyzer," *International Journal of Communications, Network and System Sciences*, vol. 16, no. 2, pp. 21–29, 2023.

[26] B. L. Thayer, Z. Mao, Y. Liu, K. Davis, and T. Overbye, "Easy simauto (esa): A python package that simplifies interacting with powerworld simulator," *Journal of Open Source Software*, vol. 5, no. 50, p. 2289, 2020.

[27] Y. Liu, A. Song, X. Shan, Y. Xue, and J. Jin, "Identifying critical nodes in power networks: A group-driven framework," *Expert Systems with Applications*, vol. 196, p. 116557, 2022.

[28] S. R. Pani, R. K. Samal, and P. K. Bera, "A graph-theoretic approach to assess the power grid vulnerabilities to transmission line outages," in *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*. IEEE, 2022, pp. 1–6.

[29] J. Beyza, V. M. Bravo, E. Garcia-Paricio, J. M. Yusta, and J. S. Artal-Sevil, "Vulnerability and resilience assessment of power systems: From deterioration to recovery via a topological model based on graph theory," in *2020 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*, vol. 4. IEEE, 2020, pp. 1–6.

[30] A. Ur-Rehman, I. Gondal, J. Kamruzzuman, and A. Jolfaei, "Vulnerability modelling for hybrid it systems," in *2019 IEEE international conference on industrial technology (ICIT)*. IEEE, 2019.

[31] J. Zeng, S. Wu, Y. Chen, R. Zeng, and C. Wu, "Survey of attack graph analysis methods from the perspective of data and knowledge processing," *Security and Communication Networks*, vol. 2019, no. 1, p. 2031063, 2019.

[32] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual conference for protective relay engineers (CPRE)*. IEEE, 2017, pp. 1–8.