Smart Grid Cyber-Attack Analysis and Countermeasures

Tan Duy Le[1,2,*], Huynh Phuong Thanh Nguyen[3], Kha-Tu Huynh[1,2], Razvan Beuran[3]
[1] *School of Computer Science and Engineering, International University, Ho Chi Minh City, Vietnam*
[2] *Vietnam National University, Ho Chi Minh City, Vietnam*
[3] *School of Information Science, Japan Advanced Institute of Science and Technology, Ishikawa, Japan*
ldtan@hcmiu.edu.vn

***Abstract*—The smart grid, a key component of Industry 4.0, is critical in promoting sustainable social and economic development. The traditional grid and computer technologies are integrated into this next-generation electrical power system to improve automation, connectivity, and communication. Testing on an existing system is risky and challenging due to the smart grid's complexity, which has two crucial components: electrical grid and network communication. Simulating and analyzing this system could be an effective solution for experimenting with smart grid cybersecurity. This research identified the necessity for practical cybersecurity experimentation for the smart grid, and a methodology was proposed to enable such investigation successfully. Furthermore, a general smart grid cybersecurity architecture that satisfies these requirements was designed and implemented in two systems named GridAttackSim and GridAttackAnalyzer. By employing these systems, countermeasures against cyber-attacks can be investigated, thus helping researchers determine the implications of various attack types and allowing for the early development and evaluation of new anomaly detection methods and mitigation strategies before deployment.**

***Index Terms*—smart grid, cyber-attack analysis, cyber-attack countermeasures, co-simulation, security training**

I. Introduction

Traditional power grids are characterized as central power stations that generate and supply electricity to consumers. Initially the distribution was conducted without much energy consumption management and monitoring. Technological advancements have improved the management process of loads and equipment designed to track specific parameters or run according to schedules. The smart grid is a new and smart power system that integrates information technology, two-way communication, and security into electrical grids.

Nowadays, the way that people live and work is changing as a result of disruptive technologies and trends, including the Internet of Things (IoT), robotics, virtual reality (VR), and artificial intelligence (AI), which form the term Industry 4.0. Smart grid is one of the critical components of the Industry 4.0 vision. In 2016, the Society 5.0 initiative [1] was established by the Japanese Cabinet to develop new economic and social development strategies, with the smart grid cited as one of the essential components. The smart grid is also described as a special vital infrastructure that supports essential services by the US Department of Homeland Security (DHS) [2]. However, there is a growing shortage of highly skilled technical cybersecurity experts. According to a recent report by the Center for Strategic and International Studies (CSIS), 82% of organizations in eight countries reported a lack of cybersecurity abilities, with 71% agreeing that this skill shortage has direct and determinable consequences for their institutions [3].

Cybersecurity has emerged as a key issue along with the advancement of smart grid systems. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported that almost one-third of the cybersecurity incidents in 2014 was targeted the energy sector [4]. In 2007, Iran's crucial nuclear power development was slowed significantly by an attack on its nuclear power plant [5]. The operations of the uranium enrichment chain could also be substantially reduced or interrupted. By 2014, more than 1000 energy firms [6] had been targeted by a professional hacker team called Dragonfly. The core system controls energy companies in North America, and Europe had broken successfully. Malware in emails, websites, and third-party programs was used to access these systems. On 25 December 2015, during the Ukrainian civil war in Donbass, 80,000 civilians were forced into the dark [7] due to a cyber-attack aimed at an electrical power station in Ivano-Frankvisk. These security incidents prove that cyber-attacks can happen and that actual, tangible consequences exist in the real world. Governments and organizations can launch attacks on smart grid networks, resulting in blackouts and possibly infrastructure destruction. Using attack simulation tools is a promising solution to these issues, and the most crucial element in enhancing cybersecurity training efficacy is the utilization of real-world event simulation technology.

Co-simulation technology is a potential approach to overcome the smart grid complexities. However, there is a limitation in this area. Very little effort has been put into investigating the potential damage of attacks and evaluating their impact on the system. A few works focus on smart grid attack analysis using GrSM and CVSS. So a new framework must be developed to support smart grid attack co-simulations fully.

This research aims to develop a methodology that can successfully enable realistic cybersecurity experiments for the smart grid as well as train IT experts and cybersecurity professionals. In particular, our realistic smart grid cyberse-

* Corresponding author.

978-1-6654-6166-5/22/$31.00 ©2022 IEEE

curity experimentation methodology was designed based on two approaches: co-simulation and analytical modeling. First, the co-simulation framework GridAttackSim was proposed to facilitate the modeling of the many specialized topologies for smart grid systems. Then GridAttackAnalyzer was also introduced as the first smart grid attack analysis framework. Furthermore, various cyber-attack scenarios were used to analyze and propose prevention models. The study also allows an early attack countermeasure to be conducted. Besides, this research also enables the assessment of detection of anomalies and even mitigation before deployment.

Background and related research, details on the the proposed approaches, and a discussion and conclusions will be presented in the following sections, respectively.

II. Background and Related research

The smart grid is defined as the core technology for sustainable economic and social development. Several cyberattacks have been attempted on smart grid systems in recent years around the world and caused serious consequences. Approaches to modeling hacker behaviors have been presented to visualize the system and analyze the attack paths.

EPOCHS (Electric Power and Communication Synchronizing Simulator) was one of the earliest simulation models for smart grid systems [8]. It includes a wide range of applications, such as large-area monitoring and management. The EPOCHS concept, however, does not include a cyberattack simulation feature. Real-time simulations of different smart grid-related applications can be conducted using the simulation framework known as SGsim [9]. It supports smart grid communication standards as well as common smart grid tools. Similar to EPOCHS, the cybersecurity attack simulation feature is omitted.

The Attack Simulation Toolset for Smart Grid Infrastructure (ASTORIA) [10] is a framework for smart grid attack simulation and evaluation. Ns-3 and PY-POWER were used as network and power flow simulators. It allows for the injection of attacks as well as the examination of their outcomes. Attack Profiles, which are generally formatted configuration files, are used to launch these attacks. They enable multiple attack parameters, such as attack schedule, attack type, and intensity or frequency, to be configured. Denial of Service (DoS) and malicious software infection attacks were simulated. However, no explicit security evaluation metrics are identified in the study. Only the vulnerabilities are highlighted in the system by presenting sampled data.

Although both electric grid and communication network simulations are capable of these simulation techniques, they are often used in small, constrained networks that are difficult to extend. Furthermore, the current architecture for co-simulation is extremely complicated to implement and utilize. Our previous research [11] argued that it is possible to co-simulate with ns-3, DNCS, and GridLAB-D. Unfortunately, few studies have evaluated the effects of cyberattacks on the smart grid system based on this combination. Consequently, we conducted research to cover the FNCS study gap by developing a comprehensive and extendable attack pattern library that includes an attack schedule and a result visualization tool.

Liu et al. [12] proposed a methodology for agent-oriented software engineering and requirements analysis based on $i*$, which is an agent-oriented request modeling language [13]. Internal attackers, rather than external attackers, were the focus of this study. A similar approach was presented by Mouratidis [14]. Dangerous scenarios were utilized in this article to examine the nature of security threats that may arise with software development. In addition, this study used a simple attack model in which hackers must fulfill sub-targeted tasks in order to reach the main goal. Another study [4] evaluated attack scenarios during the development of service applications. Asnar [5] extended the framework of this study based on i^* by adding risks associated with the system's goals. Unfortunately, the detail of the sources of risks was not argued in this study.

A structured methodology was introduced by Beckers et al. [15] to analyze the threats related to constructing an attack tree to specific system faults that were presented in the attack graph. This method gathers system information at a low level in order to examine high-level probabilistic features. The attack tree and attack graph were used in the research to map the attacker's goals to actions. This study also demonstrated that it was possible to construct part of a complex graph related to a specific target in the attack tree. Furthermore, the research findings revealed that the attack graph analysis complexity had been significantly reduced. In addition, an algorithm to estimate the attacker's probability of overall succeeding in achieving the goal was proposed in this paper.

III. General Architecture for Smart Grid Cybersecurity Experimentation

A. Design Requirements

Network communication and power grid are defined as two significant aspects of the smart grid that make its construction complex. It is necessary for researchers to take into account the relationship between these components for system investigation and enhancement in the future. Unfortunately, it is usually impossible to implement a real smart grid system for the cybersecurity experiment and validation process because of its potentially dangerous consequences. Accordingly, system-level modeling and simulation tools are necessary for a smart grid cybersecurity experimentation system. Therefore, a cybersecurity experimentation system for smart grid should meet the following specifications, which are summarized in Figure 1:

- *Power grid component*: the experimentation system should be able to reproduce the behavior of a power grid network and the interaction between its components.
- *Network component*: the experimentation system should be able to reproduce a smart grid network's behavior by calculating and simulating interactions between various network entities.
- *Security component*: the experimentation system should be able to simulate, emulate, and analyze various types of

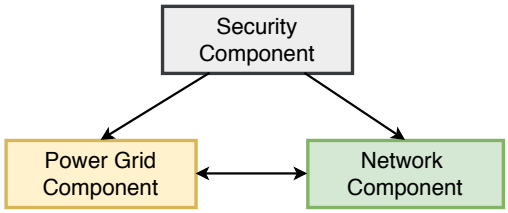

Fig. 1: Smart grid cybersecurity experimentation components

attacks on the smart grid system. The security component is a set of databases and configurations to start an attack on the system.

B. Concerns Regarding Smart Grid Cybersecurity Research

These prerequisites must be met in order to conduct realistic cybersecurity experiments on smart grids. Due to its structure being complex, it is inefficient to design a single smart grid cybersecurity experimentation system that meets all of the requirements above. Therefore, to simplify the system but still accomplish our goal, the smart grid cybersecurity experimentation is divided into two parts: the simulation technique and the analytical modeling approach.

The intention of simulation and analytical modeling approaches is to enhance understanding of the system's performance under various conditions.

On the one hand, an analytical model is a mathematical abstraction that might be generalized to deal with various working conditions through specific assumptions about how a process advances. In some circumstances, a solution can be identified, and a result can be achieved in a wide range of situations. The analytical model's advantage is that it offers a promising alternative to employ a mathematical formulation to derive performance outcomes in a variety of situations. The model's accuracy must be taken into account through the validity of the assumption that the mathematical formula is derived. Some uncertainties can be addressed with a stochastic model to estimate the modeling and measurement model.

Moreover, a simulation model also makes assumptions about the model and the behavior of the process that it is simulating. A simulation model is applied when it is impossible to derive the result using an analytical formulation since the model is too large or the exact solution cannot be obtained. This is only useful for specific applications and should be executed multiple times to compensate for the influence of numerical calculations. The simulation should be re-executed for several application scenarios to confirm the findings. A simulation model can be helpful when it has been shown to operate under numerous circumstances and is not dependent on a single case study.

The analytical approach should be preferred when the two methods are available, and simulation can be applied to verify the assumptions and models' validity. When the two approaches can be used, preference should be given to the analytical approach, and simulation can be used to validate the assumptions and the models. Since the simulation aims

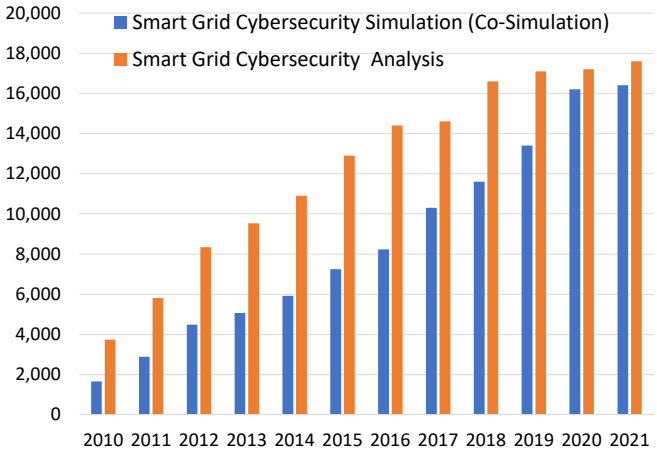

Fig. 2: Number of publications related to smart grid attack simulation and analysis from 2010 to 2019.

not to verify the model but to validate the reality of the modeling process, the assumptions applied by the simulation model could be slightly different from the analytical model for better analysis.

Therefore, using the simulation approach is one possible direction to conduct cybersecurity experimentation for smart grids. Additionally, the power grid and the network should be simulated independently as well as the interaction between them should be captured. Consequently, these specifications not only complicate the system architecture but also influence its performance. Co-simulation is an emerging technology to deal with this issue.

The application of simulation (co-simulation) and analysis for experimentation study on smart grid cybersecurity has been growing in recent years. Figure 2 shows the number of publications related to smart grid simulation and analysis from 2010 to 2019. The data on the table were retrieved from Google Scholar using a keyword search. The query strategies for co-simulation of smart grid attacks is ("Smart Grid" OR "Smart Grids") AND ("Simulation" OR "Co-simulation") AND ("cybersecurity" OR "cyber security" OR "security"); While the search pattern for smart grid attack analysis is ("Smart Grid" OR "Smart Grids") AND ("Analysis") AND ("cybersecurity" OR "cyber security" OR "security").

The co-simulation approach and analytical modeling approach are discussed in the following section.

C. Co-simulation Approach

Co-simulation is the coordination of two or more simulation models, which differ in their run time and representation. It can simulate the network and the power grid separately. Moreover, co-simulation enables monitoring of the reciprocal relationship between the physical power grid and the communication network. The objective is to make the different simulators' modules available for combined simulations, which run independently and only exchange data when needed. It allows users

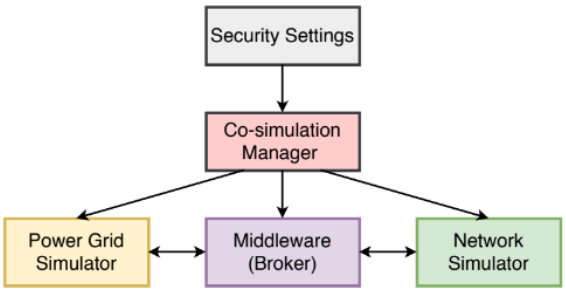

Fig. 3: General architecture of the co-simulation approach for smart grid cybersecurity experimentation

to implement and examine other communication and power hardware/protocol integration.

Unfortunately, as mentioned earlier, the integration complicates the simulators' code base, introduces bugs, and sometimes replicates work that has already been completed. It also poses numerous difficulties that need to be overcome, such as differences in time scales, time synchronization, communications delays, and appropriate model reuse. To overcome these challenges, a reliable middleware or broker should be placed in the center of the co-simulation approach's architecture to monitor and control the communication between the two smart grid components.

Furthermore, to manage the co-simulation activity, a general manager is needed. It receives attack data and configuration from the security component, then transfers to the power grid and network simulation, and awakes the middleware to conduct a simulation.

D. Analytical Modeling Approach

Another possible direction to conduct cybersecurity experimentation for smart grids is the analytical modeling approach, which aims to create a model for smart grid attack analysis. Attack analysis focuses on all possible attack paths where the system (or network) is accessed or compromised by utilizing technical capabilities to exploit a vulnerability. Given the existence of various complex threats, the ability to discover possible attack scenarios and minimize the effect of malicious attacks is becoming a significant problem. The attack analytical results allow the researchers or security decision-makers to determine which part of the network is the most vulnerable, evaluate the various defenses' efficacy, and decide how to secure the network most effectively, minimizing the potential impact of the attacks.

Securing a network involves an in-depth analysis of regular operations and vulnerabilities. The conventional attack analysis classifies attacks based on information about reported attacks. Hence, such an approach cannot be extended to new (unknown) incidents. The concern is even more severe in emerging environments where very few reported threats are available, such as the smart grid. Researchers can gain several

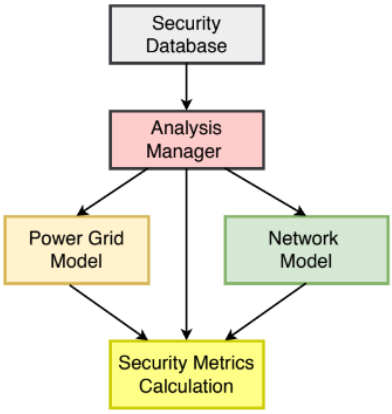

Fig. 4: General architecture of the analytical modeling approach for smart grid cybersecurity experimentation

benefits from using attack analysis, as follows:

- Firstly, the model provides the ability for researchers to capture all potential attack paths, meaning it is no longer limited to the protection of particular attacks.
- Secondly, it enables researchers to analyze the security of different smart grid attack scenarios.
- Finally, it offers an intuitive way of analyzing security flaws in systems and assessing possible counteractions since the sequences of the attackers' measures are captured in the model.

To control the attack analysis activity, a general manager is required. Attack data and configuration from the security component are acquired, then transferred to the power grid and network models. The security metrics calculation component receives attack data from the security component as well as the smart grid model. Finally, the security metrics are calculated and analyzed.

E. Approaches Comparison

The co-simulation approach makes assumptions about the model and the process behavior that it is simulating. It enables researchers to act on different attack types on the smart grid system and determine security metrics that can be used to compare normal operations against various attack scenarios. Therefore, the co-simulation approach aims at recreating vulnerability manipulation strategies and makes it possible to conduct training exercises. Furthermore, it enables the design and implementation of cybersecurity defense methodologies to anticipate similar future attacks.

Analytical modeling is a mathematical abstraction under different conditions. It enables researchers to identify all conceivable network attacks and calculate the desired security metrics. Plus, the attack graph can be generated. Therefore, this approach gives researchers a deeper understanding of the phenomena relevant to exploiting and patching vulnerabilities.

F. Implementation

Our objective was to design and construct a smart grid cybersecurity experimental methodology for smart grids that fulfills the design requirements mentioned in Section III-A. As our previous research, we implemented GridAttackSim (Cyber-Attack Simulation on Smart Grids) [16] and GridAttackAnalyzer (Cyber-Attack Analysis on Smart Grids) [17].

Based on the general co-simulation methodology for the smart grid cybersecurity experiment, we designed the architecture of GridAttackSim. This architecture includes six components, consisting of the pre-processing module, attack pattern library, ns-3, GridLAB-D, FNCS broker, and model manager. The communication network and power grid components are integrated into the designed architecture of GridAttackSim, making it possible to simulate various attack types. Our approach features a stable, user-friendly interface (GUI), an extendable set of attack patterns, and a powerful attack simulation tool with an attack schedule resulting in visualization functions. Moreover, case studies with IEEE 13 node and simple test feeders scenarios were performed to validate GridAttackSim.

The structure of GridAttackAnalyzer was established based on the standard analytical modeling technique for smart grid cybersecurity experiments. The aggregation of the smart grid model, security settings, and database are assigned as the input to prepare the analysis session's environment. Also, the preprocessing components are employed to calculate the security metric. GridAttackAnalyzer enables the analysis of various attack types. To facilitate its use, a user-friendly GUI was developed for GridAttackAnalyzer using the Python Tkinter. To validate GridAttackAnalyzer, a case study was conducted to handle the smart grid network concept with gateways and R4-12.47-2 PNNL taxonomy feeders. In the vulnerability analysis process, GridAttackAnalyzer is enriched by determining all possible attack paths and calculating the selected security metrics. Crucially, our proposed framework can generate the attack graph automatically.

We conducted an external user evaluation of GridAttackSim and GridAttackAnalyzer. Particularly, ten participants, who are Ph.D. candidates in cybersecurity or related topics, were invited to use the two frameworks and then give feedback based on the System Usability Scale (SUS) [18]. This well-known standardized questionnaire is a widely accepted, reliable tool for measuring usability. The evaluation criteria has been explained in our related research in [16] and [17]. The analysis reflects the result values of SUS for GridAttackSim and GridAttackAnalyzer, which are shown in Table I. These mean scores can be considered as acceptable (SUS $>$ 70) for both frameworks. The results show that users were satisfied with the usability of GridAttackSim and GridAttackAnalyzer.

TABLE I: SUS Results for GridAttackSim and GridAttackAnalyzer

No	Frameworks	Maximum Value	Minimum Value	Mean	Standard Deviation
1	GridAttackSim	87.5	55	74.3	9.5
2	GridAttackAnalyzer	90	60	72.2	10.2

IV. Cyber-Attack Analysis and Countermeasures

Cyber-attacks can lead to disturbances that transcend the virtual world and damage the physical system. In other words, physical attacks on the smart grid can affect the system's stability, leading to a load loss. By combining the functionalities of both GridAttackSim and GridAttackAnalyzer, it is possible to simulate and assess the characteristics and consequences of an attack on the smart grid physical system. In addition, countermeasures against cyber-attacks can be introduced.

Understanding the consequence of a physical attack on the smart grid system is essential. In GridAttackSim, the total load, current market-clearing quantity, current market-clearing price, economic impact of an attack, and bill amount are all aggregated into different metrics. The values of these metrics can be analyzed and contrasted in regular operation and attack scenarios to estimate attack consequences objectively.

GridAttackSim can be used by smart grid system developers not only to examine the repercussions of various attack types but also to facilitate early advancement and evaluation of innovative anomalous detection and mitigation techniques before their implementation. Since GridAttackSim enables researchers to create new attack models freely, it allows the experimentation and validation of the proposed attack modeling approach in a realistic case study.

GridAttackAnalyzer is used to investigate all potential attack paths, then determine which device included in the directions should be protected first. Moreover, GridAtackAnalyzer can help researchers estimate the attack's damage cost on the proposed smart grid system. For example, based on this information, a security analysis of the cyber-physical system (identifying "bottlenecks") is conducted, and recommendations for removing the identified vulnerabilities are supplied, taking into consideration their severity level.

IT professionals, cybersecurity specialists, and end-users must acquire a thorough knowledge of preventing and responding to security incidents in smart grids, which are usually not fully covered in conventional training and education approaches. There is a need for realistic cybersecurity training for smart grids. To achieve this goal, first, the smart grid practical cybersecurity training design requirements need to be clarified, then realistic cybersecurity training for smart grids should be implemented by applying these design requirements.

Our proposed framework can support cybersecurity training activity by integrating a training content component in the smart grid cybersecurity experimentation general architecture. Training content is an essential part of any training system. It includes all resources and information given to trainees to

develop their cybersecurity awareness and abilities. The co-simulation approach should be able to simulate the various types of attacks on the smart grid. Therefore, its training content should be designed to educate trainees on the attack characteristics. Additionally, the training content should include knowledge about the power grid and network communication, which are the smart grid's two primary components. The analytical modeling approach should be able to analyze different types of smart grid attacks. The publicly known information-security vulnerabilities and exposures database should be used to form the training content. Hence, the attacks' consequences can be highlighted in the training content. Moreover, the attack path should be included in the training content to inform trainees how the hacking attempt is successful. Our proposed framework can enhance the cybersecurity training activity by combining the training content component with the smart grid cybersecurity experimentation general architecture. Hence, GridAttackSim and GridAttackAnalyzer can be seen as practical applications for smart grid training activities.

V. Discussion and Conclusion

The community is approaching a new era in which technology will transform how people live, communicate, and engage with each other. One of the critical elements of the Industry 4.0 and Society 5.0 visions is the smart grid, which includes the network and power grid components. In recent years, smart grid systems have been the target of numerous cyberattacks that have serious consequences, such as loss of confidential data, blackouts, and destruction of power equipment. Therefore, it is essential to protect smart grid systems against cybersecurity attacks.

Building a reliable smart grid system for the evaluation and experimentation process in cybersecurity is not a trivial activity, since it entails high risks of destroying the electrical infrastructure and equipment, resulting in enormous economic consequences or even potential loss of human lives. As a result, simulation and analysis techniques can be considered effective solutions to reach the goal in this critical domain, where testing on a natural system is prohibited.

This research identified the requirements for practical cybersecurity experimentation for the smart grid. We indicated the system design specifications as one of the key contributions. Furthermore, a general smart grid cybersecurity architecture that satisfies these requirements was implemented. To deal with the system's complexities while still achieving our goal, smart grid cybersecurity experimentation were divided into co-simulation and analytical modeling methodologies; their specifications and generic architectures were also established.

Our contribution was the introduction of GridAttackSim, a framework that enables the reproduction of a real smart grid system with different cybersecurity attacks and then assesses their effects, all in one place. We also introduced GridAttackAnalyzer, a smart grid attack analysis framework. By employing GridAttackSim and GridAttackAnalyzer, countermeasures against cyber-attacks can be familiarized.

Our framework can be used for the training of IT experts and cybersecurity professionals. IT experts and cybersecurity professionals can determine all possible attack paths based on evaluating various security metrics. As future work, GridAttackSim and GriAttackAnalyzer could be extended to integrate more power grid test feeders and network models.

Acknowledgment

This research is funded by International University, VNU-HCM under grant number T2021-01-IT.

References

[1] M. Fukuyama, "Society 5.0: Aiming for a new human-centered society," *Japan Spotlight*, vol. 27, pp. 47–50, 2018.

[2] I. Ghansah, "Smart grid cyber security potential threats, vulnerabilities and risks: Interim project report," *California Energy Commission*, 2012.

[3] C. Worley, "Hacking the skills shortage a study of the international shortage in cybersecurity skills," 2016, jA Lewis (Chair), Hacking the skills shortage A study of the International shortage in Cybersecurity skills [Video file]. Symposium conducted at the meeting of Center for Strategic & International Studies, Washington, DC. [Online]. Available: https://www.csis.org/events/hacking-skills-shortage

[4] I. Cert, "Incident response/vulnerability coordination in 2014."

[5] I. Ghansah, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[6] J. T. Langill, "Defending against the dragonfly cyber security attacks," *Retrieved*, vol. 11, p. 2015, 2014.

[7] T. FoxBrewster, "Ukraine claims hackers caused christmas power outage," *Forbes Security*, 2016.

[8] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "Epochs: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, 2006.

[9] Awad, Abdalkarim, Bazan, P. German, and Reinhard, "Sgsim: A simulation framework for smart grid applications," *2014 IEEE International Energy Conference (ENERGYCON). IEEE*, pp. 730–736, 2014.

[10] A. G. Wermann, M. C. Bortolozzo, E. G. da Silva, A. Schaeffer-Filho, L. P. Gaspary, and M. Barcellos, "Astoria: A framework for attack simulation and evaluation in smart grids," *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE*, pp. 273–280, 2016.

[11] T. D. Le, A. Adnan, R. Beuran, and W. L. Seng, "Smart grid co-simulation tools: Review and cybersecurity case study," *7th International Conference on Smart Grid (icSmartGrid2019). IEEE*, p. 273–280, 2019.

[12] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," *Proceedings. 11th IEEE International Requirements Engineering Conference, 2003*, 2003.

[13] E. Yu, "Towards modelling and reasoning support for early-phase requirements engineering," *Proceedings of ISRE '97: 3rd IEEE International Symposium on Requirements Engineering*, 1997.

[14] H. Mouratidis, P. Giorgini, and G. Manson, "Integrating security and systems engineering: towards the modelling of secure information systems," *CAiSE'03 Proceedings of the 15th international conference on Advanced information systems engineering*, 2003.

[15] K. Beckers, M. Heisel, L. Krautsevich, F. Martinelli, R. Meis, and A. Yautsiukhin, "Determining the probability of smart grid attacks by combining attack tree and attack graph analysis," *International Workshop on Smart Grid Security*, pp. 30–47, 2014.

[16] T. D. Le, A. Anwar, S. W. Loke, R. Beuran, and Y. Tan, "Gridattacksim: A cyber attack simulation framework for smart grids," *Electronics*, vol. 9, no. 8, p. 1218, 2020.

[17] T. D. Le, M. Ge, A. Anwar, S. W. Loke, R. Beuran, R. Doss, and Y. Tan, "Gridattackanalyzer: A cyber attack analysis framework for smart grids," *Sensors*, vol. 22, no. 13, p. 4795, 2022.

[18] M. R. Drew, B. Falcone, and W. L. Baccus, "What does the system usability scale (sus) measure?" in *International Conference of Design, User Experience, and Usability*. Springer, 2018, pp. 356–366.