Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 8, Issue 28, pages 39-46, 2022

Economic Impact Assessment of Cyber Attacks on the Smart Power System

Umair Shahzad
Department of Electrical and Computer Engineering,
University of Nebraska-Lincoln,
Lincoln, NE, USA
umair.shahzad@huskers.unl.edu

***Abstract*–A smart power system is essentially a cyber-physical system (CPS) which incorporates unique features of both a power system and a Supervisory Control and Data Acquisition (SCADA) system. The role of SCADA system is to aid in online measurement, control, and management of power system. The presence of cyber layer significantly advances the effectiveness and efficacy of the smart power system. However, this layer also increases the vulnerability of the system against various outside threats and intrusions, commonly known as cyber threats or cyber attacks. Therefore, it is of great significance to assess the impacts caused by these attacks on the smart power system. Therefore, this paper uses a risk-based approach to assess the economic impacts caused by these attacks on the smart power system. The IEEE 39-bus test system was used to demonstrate the effectiveness of the proposed approach. Two different case studies were conducted. All simulations were conducted using DIgSILENT PowerFactory commercial software.**

Keywords-Cyber attack; economic impact; risk; SCADA; smart grid; vulnerability

I. INTRODUCTION

Due to various technological advancements, the power system has enhanced its flexibility, and is able to incorporate advanced architectures to meet the significant requirements of the modern power system functions [1-2]. Moreover, the communication technology has a vital role in enhancing the monitoring and control functions in the power systems. Therefore, more communication protocols are being researched. This transformation of power system is commonly known as the smart power system. National Institute of Standard and Technology (NIST) introduced the basic model of smart grid in [3]. The physical infrastructure of the power system is called the physical layer and other components such as Supervisory Control and Data Acquisition (SCADA), advanced metering infrastructure (AMI), and communication protocols are part of the cyber layer. These two layers form a diverse type of system knows as the cyber-physical system (CPS) [4]. Due to the evolving cyber space, complex threats and severe attacks are part of the smart power system analysis. These cyber threats are culminated using various malwares such as, Stuxnet, Flame, Duqu, etc. [5]. Various implications of typical cyber-attacks in power systems are illustrated in Fig. 1.

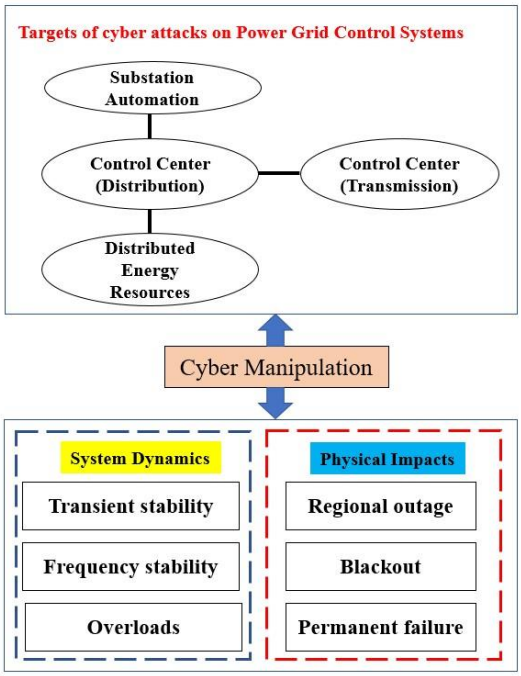

Fig. 1. Cyber-attack implications in power systems

Recent cyber studies indicate that the economic impact of a few cyberattacks on U.S. critical infrastructure could surpass $700 billion, and leave up to 70% of the U.S. without electrical power for at least six months [6-7]. Cyber threats are constantly on the rise owing to transformation of power systems as mentioned in the European Union Agency for Cybersecurity (ENISA) smart grid threat landscape report and NIST report for Guidelines for Smart Grid Cybersecurity [8-10]. For instance, a huge cyber-attack occurred on Ukraine's power system, by a malware (BlackEnergy), in 2015. The malware was installed by the intruders on the computers, located in control center. This cyber intrusion happening demonstrates that hackers can harm a large Information and Communication Technology (ICT) network within no time. Moreover, cyber hackers are difficult to trace because of cryptographic spear phishing and unknown source address. Moreover, cyber attackers can access any part of the network with full network access, and can cause large-scale system-wide havoc [11].

Reference [11] discussed an account of cyber systems in a typical smart grid. The article highlighted

the significance of cyber protection and cyber-physical system testbeds. Reference [12] provided a review of the cybersecurity necessities in smart grids. Moreover, it entailed various kinds of dangerous cyberattacks. In [13], a cybersecurity protection methodology for control systems of smart grid was elaborated. References [14-15] entailed a detailed review of models, and approaches, for the cyber-physical interaction. Reference [16] presented an offline co-simulation testbed for evaluating various cyber-attacks and their technical impacts. Reference [17] provided an original model for the assessment of the validity of an active cyber-physical network. In addition to these works, there are numerous research works which highlighted the significance of incorporating cyber security in power systems. These works signified that research literature on cybersecurity issues in smart power systems is swiftly rising. The main shortcoming of these research papers is that they focus on identifying security threats. Moreover, majority of them focus on assessing the technical impacts of cyber threats rather than assessing the economic impacts. This imperative gap is the main theme of this paper, i.e., to provide a quantitative economic assessment of impact of cyber-attacks in terms of risk.

In today's time, the role of SCADA cannot be underestimated. It is used to collect data and information from remote facilities using remote terminal units (RTUs), and to send the control signals to power system components, such as switches and circuit breakers. As the power system becomes highly dependent on the SCADA system for its effective and efficient functioning, the liability of the robustness and resilience of power system increases. This increases the system vulnerability to external cyber threats [18]. Thus, it is of great significance to assess and quantify the various impacts which can be caused by cyber-attacks on the power system. To conduct such assessment, it is essential to do a quantitative study of the severity of cyber-attacks [19-20]. As SCADA directly controls the power system, it is beneficial to examine the various effects of cyber-attacks on the SCADA network. Consequently, these attacks will impact power system operation in various ways.

Conventional risk assessment of power system considers the impact of failures of *(N-1)* components and consequently, evaluating the corresponding impacts. With the evolution of technology and evolution of power grid to smart grid, the threat of cyber-attacks is on the rise. Thus, it is important to evaluate the risk-based impact of these attacks on the power system. Some research work has been done in this direction. Reference [21] discussed comprehensively about the risk of several components of the electric power network. Similarly, [22] proposed a risk-based method to evaluate the impact of cyber-attacks within the control system. Reference [23] devised a Bayesian-logic based risk assessment method to enumerate the impact of outside threats on the industrial cyber-physical systems. Reference [24] used a Petri-net model to analyze information security risk assessment in a power system. To consider the impact of cyber-attacks, the security objectives related to cyber-attacks must be defined. These objectives are essential to guarantee the control and monitoring functions are within a satisfactory risk level. The objectives are confidentiality, integrity, and availability [25]. Within the domain of smart power grids, these three objectives can be defined as follows [25]. These objectives are collectively known as the CIA (confidentiality-integrity-availability) triad, as shown in Fig. 2. These terms are briefly discussed below.

Fig. 2. The CIA triad

Confidentiality implies that only the authorized people can access the data or information. This also includes various personal information and exclusive information. A loss of confidentiality could result in loss of reliability of the information. Confidentiality measures are essential to protect the information from unlicensed misuse.

Integrity means that data and information during and after transmission should not be modified. This is very vital particularly for the control systems which send signals to power system components such as switches and circuit breakers. The loss of integrity can result in system collapse. Integrity measures are important in protecting the information from unauthorized alteration.

Availability implies that components and network services should be promptly available to authorized users only. A loss of availability can cause disruption in the use of services and devices. Availability measures protect uninterrupted access to the network.

An adversary can attack a smart grid using three different ways: component wise, protocol wise, and topology wise. The component wise attack targets the field devices such as switches and circuit breakers. Protocol wise attacks focus on the communication technology deployed. Topology wise attack target the topology (radial, interconnected, mesh, etc.) of the communication system of the smart grid [26]. In this work, it is assumed that adversary has full information on the power system, including the topology of the grid and locations of critical components such as lines, generators, circuit breakers, etc.

Although, there are various types of cyber-attacks that can occur in a typical power system, the major ones are shown in Fig. 3.

The rest of the paper is organized as follows. Section II describes the computation procedure for computing economic impacts and consequent risks due to cyber attacks resulting in line and generator outages. Section III elaborates the mathematical formulation. Sections IV and V present case studies

and simulations. Section VI presents results and discussion. Finally, Section VII concludes the paper with suggested future research directions.

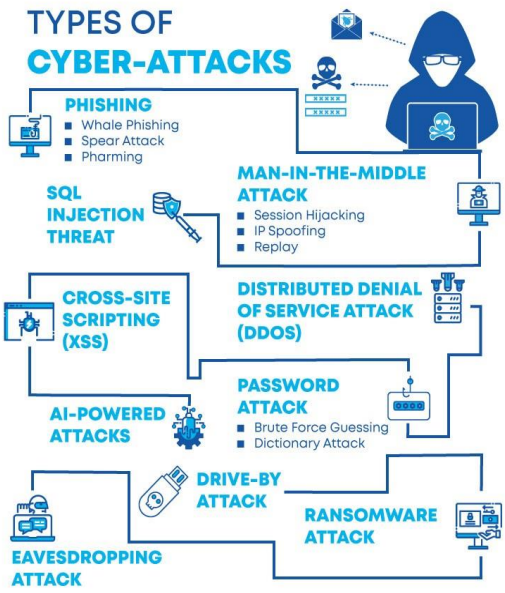

Fig. 3. Types of cyber attacks

II. Computation Procedure

The computation procedures are outlined in Fig. 4 and 5. Firstly, referring to Fig. 4, in the first step, optimal operating cost of the system is computed under normal conditions. This is denoted by C_o. At this stage, there is no cyber-attack, and the system is operating normally. Then, the intruders take control of a line breaker and opens it. After this line outage, the resulting optimal cost and its deviation from base-case optimal cost is computed. The process is repeated till all lines have been outaged (one at a time). Finally, the risk due to line outages, denoted by R_L, is computed. In the next step (Fig. 5), the same process is conducted, incorporating *(N-1)* generator outages, and consequently, the risk due to generator outages, R_G, is computed. The net impact ω is then computed by adding these both risk indices (R_L and R_G).

III. Mathematical Formulation

Let C_o be the optimal operating cost of the system under normal conditions (no cyber-attack). Let C_{Ln} denote the optimal cost of the system under n^{th} *(N-1)* line outage due to cyber-attack. Then, deviation from optimal cost under this condition is given by ΔC_{Ln}. Mathematically, we can write it as follows

$$\Delta C_{Ln} = C_{Ln} - C_o \tag{1}$$

The average cost deviation due to *(N-1)* line outage is given by ΔC_L. Mathematically,

$$\Delta C_L = \frac{\sum_{n=1}^{N_L} \Delta C_{Ln}}{N_L} \tag{2}$$

where N_L denotes number of lines in the system.

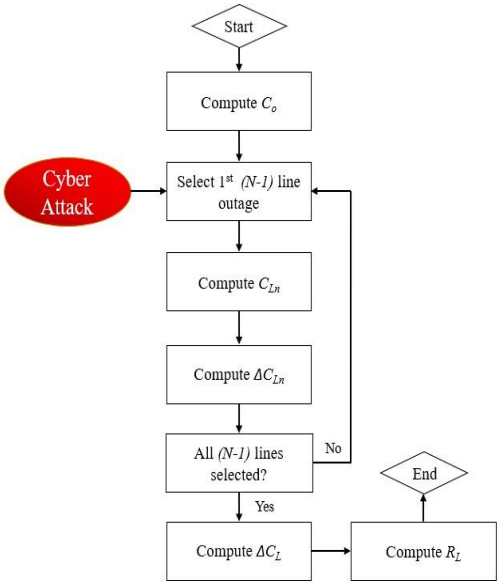

Fig. 4. Procedure for assessing risk due to line outages

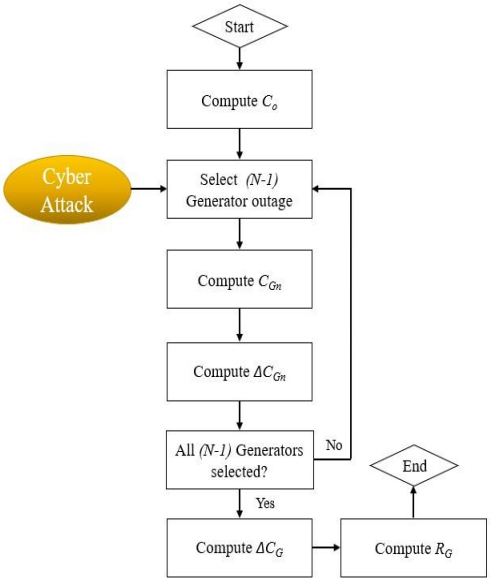

Fig. 5. Procedure for assessing risk due to generator outages

The risk due to *(N-1)* line outage is given by R_L, i.e.,

$$R_L = P_L \times \Delta C_L \tag{3}$$

where P_L denotes probability of line outage by cyber-attack and its value is assumed to be 0.0001.

Let C_{Gn} denote the optimal cost of the system under n^{th} *(N-1)* generator outage due to cyber-attack. Then, deviation from optimal cost under this condition is given by ΔC_{Gn} as follows

$$\Delta C_{Gn} = C_{GN} - C_o \tag{4}$$

The average cost deviation due to *(N-1)* generator outage is given by ΔC_G

$$\Delta C_G = \frac{\sum_{n=1}^{N_G} \Delta C_{Gn}}{N_G} \quad (5)$$

where N_G denotes number of generators in the system.

The risk due to *(N-1)* generator outage is given by R_G, i.e.,

$$R_G = P_G \times \Delta C_G \quad (6)$$

where P_G denotes probability of generator outage by cyber-attack and its value is assumed to be 0.0001.

Let ω denote the net economic impact due to both *(N-1)* line and *(N-1)* generator outage, caused by cyber-attack. Assuming both these outages are independent, we can write,

$$\omega = \Delta C_G + \Delta C_L \quad (7)$$

Let R_T denote the total risk due to both outages, i.e.,

$$R_T = P_C \times \omega \quad (8)$$

where P_C denotes probability of cyber-attack (on a single line and generator) and is given by

$$P_C = P_L + P_G = 0.0001 + 0.0001 = 0.0002 \quad (9)$$

IV. Case Study I: Generic Cyber Attack

The IEEE 39-bus test system was used to conduct the required analysis for this study. The single line diagram is shown in Fig. 6. The numerical data and parameters were taken from [27]. The coefficients of generator cost curves for thermal generators were taken from [28]. DIgSILENT PowerFactory software was used to conduct the required simulations [29]. Further, it was assumed that generators and lines are equally prone to attack by cyber intruders. Although, this may not be always true, depending on the location of generators, but for the simplicity of presenting and analyzing results, this is a reasonable assumption.

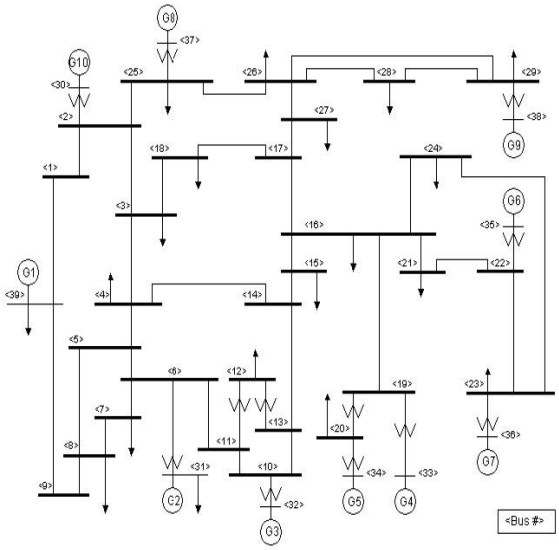

Fig. 6. IEEE 39-bus test system

V. Case Study II: Data Integrity Attack

The IEEE 39-bus system was used for conducting required simulations. In this case, data integrity attack on automatic generation control (AGC) was modeled. This is the kind of attack in which the attackers target to manipulate the data [30-31]. There are generally two types of data integrity attacks: Min and Max.

A Min attack is defined as an integrity attack where the actual output y from the sensor i is modified to be y_{min}. Similarly, a Max attack is an attack where the actual output of the sensor i is modified to y_{max}. Mathematically [30],

$$y_{i\,\min} = \begin{cases} y_i(t) & \text{for } t \notin \Omega \\ y_{i\,\min} & \text{for } t \in \Omega \end{cases} \quad (10)$$

$$y_{i\,\max} = \begin{cases} y_i(t) & \text{for } t \notin \Omega \\ y_{i\,\max} & \text{for } t \in \Omega \end{cases} \quad (11)$$

where $\Omega = \{t_s, t_e\}$ is the attack duration, t_s and t_e are the attack start and end time, respectively.

Various quantities in power system such as current, voltage, frequency, etc. are instances of sensing signals. These measurement signals are sent to main control center every couple of seconds, using the SCADA network. They help in closing/opening of circuit breakers, ramping up/down of synchronous generators, etc. A data integrity attack on such vital signals can cause a lot of damage to power system. Fig. 7 shows a graphical interaction between these several modules [30].

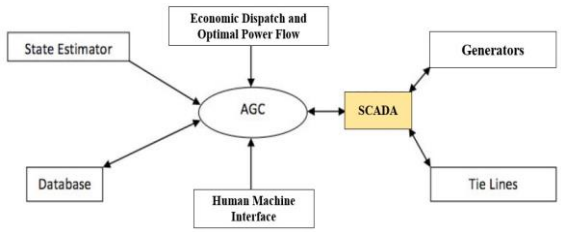

Fig. 7. Typical AGC schematic and interactions

As mentioned, AGC is very vital in relation with the sensing and control signals. The basic job of AGC is to correct line flows and adjust frequency deviations. It is also responsible for power exchange control between two different geographical areas. The frequency deviation and net power flow are used as inputs for AGC algorithm, as shown in Fig. 8 [30]. The communication channel which transmits frequency signal to control center is marked as *F*; whereas the communication channel transmission power flows is indicated by *P*. Therefore, a data integrity attack on any of these channels will result in frequency and/or power flow error.

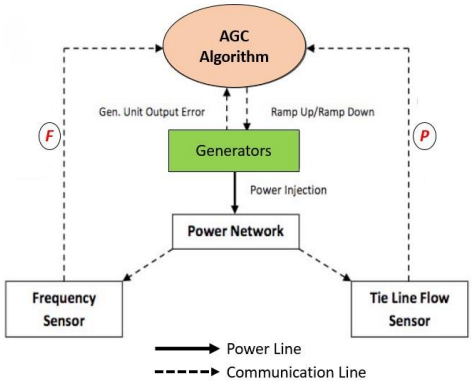

Fig. 8. Control system of AGC in a typical power system

VI. Results And Discussion

Based on the computation procedure described in Fig. 4 and Fig. 5, the value of C_o is computed to be $ 3,125,486. The graphical results for *(N-1)* generator outage is shown in Fig. 9. The corresponding tabular results are shown in Table I. Similarly, the graphical results for *(N-1)* line outage is shown in Fig. 10. The corresponding tabular results are shown in Table II.

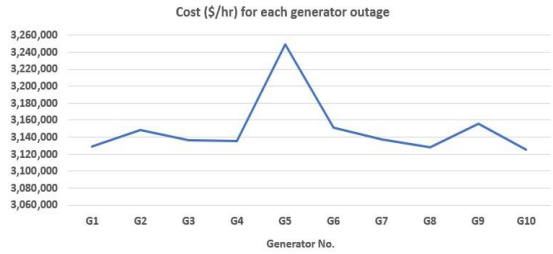

Fig. 9. Cost ($/hr) for individual *(N-1)* generator outages

Table I. Cost Deviations For Individual (N-1) Generator Outages

Generator Outage	C_{Gn} ($/hr)	ΔC_{Gn} ($)
G1	3,129,341	3,855
G2	3,148,804	23,318
G3	3,136,353	10,867
G4	3,135,166	9,680
G5	3,249,322	123,836
G6	3,151,645	26,159
G7	3,137,182	11,696
G8	3,128,192	2,706
G9	3,156,116	30,630
G10	3,125,628	142
		ΔC_G = $ 24,289

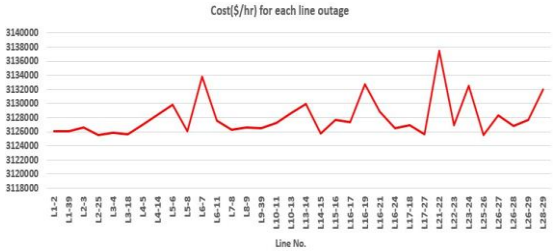

Fig. 10. Cost ($/hr) for individual *(N-1)* line outages.

Table II. Cost Deviations For Individual (N-1) Line Outages

Line Outage	C_{Ln} ($/hr)	ΔC_{Ln} ($)
1-2	3,126,055	569
1-39	3,126,098	612
2-3	3,126,620	1,134
2-25	3,125,545	59
3-4	3,125,828	342
3-18	3,125,688	202
4-5	3,127,045	1,559
4-14	3,128,393	2,907
5-6	3,129,847	4,361
5-8	3,126,069	583
6-7	3,133,851	8,365
6-11	3,127,571	2,085
7-8	3,126,236	750
8-9	3,126,645	1,159
9-39	3,126,486	1,000
10-11	3,127,296	1,810
10-13	3,128,625	3,139
13-14	3,129,931	4,445
14-15	3,125,793	307
15-16	3,127,673	2,187
16-17	3,127,323	1,837
16-19	3,132,710	7,224
16-21	3,128,809	3,323
16-24	3,126,484	998
17-18	3,126,960	1,474
17-27	3,125,620	134

21-22	3,137,411	11,925
22-23	3,126,915	1,429
23-24	3,132,526	7,040
25-26	3,125,500	14
26-27	3,128,273	2,787
26-28	3,126,774	1,288
26-29	3,127,729	2,243
28-29	3,131,974	6,488
		ΔC_L = $ 2,522

From Figs. 9-10 and Tables I-II, it is determined that Line 21-22 and Generator 5 result in highest system optimal cost (and hence greatest deviation from base-case optimal cost). Thus, these two components are considered most critical in terms of assessing cyber-attack impacts. Special attention must be paid to these components by system planners so that appropriate policies, and strategies can be devised to protect their integrity and to make the system as reliable as possible. Thus, the net economic impact ω of the cyber-attack due to both outages (line and generator) is computed as follows.

$$\omega = \Delta C_G + \Delta C_L = \$26,811/hr \quad (12)$$

$$R_T = P_C \times \omega = 0.0002 \times \omega = 5.362 \quad (13)$$

In the second case study, regarding the data integrity attacks, two different cases (known as AGC algorithm in this research paper) were simulated. This algorithm essentially represents the relation between system frequency deviation and power flows in the lines. This, in turn, determines the decision whether synchronous generation needs to ramp down or ramp up. Two different cases were considered. In the first case, generation of system was decreased by 10% and in the second one, it was decreased by 20%. The corresponding costs and results obtained are shown in Table III.

TABLE III. IMPACT OF DATA INTEGRITY ATTACK USING AGC ALGORITHM

Case Type	Cost ($/hr)
Base Case	3,125,478
Case 1 (10% generation decrease)	3,146,975
Case 2 (20% generation decrease)	3,248,627

The future trends in power system seem to move towards automation. It is very important to analyze and assess various impacts caused by cyber-attacks, well in advance, so that the planners can plan the system to adapt seamlessly to these attacks. Moreover, it is important to consider probabilistic behavior of power system when analyzing the severity of cyber threats, especially in the presence of renewable generation sources, such as wind and solar energy [32-38]. Moreover, the increasing number of researches [39-54] in recent years is a significant pointer to further delve into the research of cyber-attacks in power systems, incorporating various uncertainties.

VII. CONCLUSION AND FUTURE WORK

With the evolution of the conventional power grid to a smart grid, it is important to understand and assess various challenges encountered by it. One of the challenges is to assess the economic impact caused by a cyber-attack on vital power system components, such as generation units and transmission lines. This paper presented a method to assess the risk-based economic impact of a cyber-attack targeted towards all lines and generators. The IEEE 39-bus test system was utilized to conduct the required simulations and assessment. Two different case studies were conducted. The results showed that the economic impact is substantial enough to damage to the power system. Critical generator and line were also identified. This information is vital for power system planners for accurate decision-making.

As a future work, the impact of cyber-attack on the smart power grid can be considered in the presence of renewable generation, especially wind. Moreover, approaches to improve power system resilience in the presence of cyber threats is an open area of research. Effective approaches for co-simulation of power and cyber events should be explored. Appropriate modeling approaches, for other kinds of cyber-attacks, such as, confidentiality and availability attacks, must be researched, with respect to power systems.

REFERENCES

[1] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Cyber-vulnerability of power grid monitoring and control systems," *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research*, 2008, pp. 1-3.

[2] U. Shahzad, "Significance of smart grids in electric power systems: a brief overview," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 6, pp. 7-12, 2020.

[3] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. [Online]. https://www.nist.gov/sites/default/files/documents/publicaffairs/releases/smartgrid interoperability final.pdf"

[4] R. A. Gupta and M. Chow, "Networked control system: overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527-2535, Jul. 2010.

[5] B. Miller and D. C. Rowe, "A survey of SCADA and Critical Infrastructure Incidents," *Proceedings of the 1st Annual Conference on Research in Information Technology (RIIT)*, 2012, pp. 51-56.

[6] C. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4405-4425, Sep. 2018.

[7] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, Dec. 2017.

[8] ENISA Smart Grid Threat Landscape and Good Practice Guide. 2013

https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide

[9] ANL-GSS 15/4. Analysis of Critical Infrastructure Dependencies and Interdependencies, Argonne-Risk and Infrastructure Science Center, Argone National Lanoratory. 2015. [Online].

http://www.ipd.anl. gov/anlpubs/2015/06/111906.pdf

[10] National Institute of Standards and Technology. Guidelines for Smart Grid Cybersecurity—Smart Grid Cybersecurity

Strategy—Architecture and High-Level Requirements, vol. 1, 2014

https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[11] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power and Energy Systems*, vol. 99, pp. 45–56, 2018.

[12] Z. E. Mrabet, N. Kaabouch, and H. E. Ghazi, "Cyber-security in smart grid: survey and challenges," *Computer and Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[13] J. Jarmakiewicz, K. Maślanka, and K. Parobczak, "Development of cyber security testbed for critical infrastructure," *International Conference on Military Communications and Information Systems (ICMCIS)*, 2015, pp. 1-10.

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

[15] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control", *International Journal of Electrical Power and Energy Systems*, vol. 90, pp. 124–133, 2017.

[16] E. Hammad, M. Ezeme, and A. Farraj, "Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification," *International Journal of Electrical Power and Energy Systems*, vol. 104, pp. 817–826, 2019.

[17] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 7096-7108, Nov. 2018.

[18] P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," *Proceedings of the American Control Conference*, 2010, pp. 962-967.

[19] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," *First IEEE International Conference on Smart Grid Communications*, 2010, pp. 244-249.

[20] Y. Zhang, L. Wang, and W. Sun, "Investigating the impact of cyber attacks on power system reliability," *IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, 2013, pp. 462-467.

[21] D. Watts, "Security and vulnerability in electric power systems," *Proceedings of the 35th North American Power Symposium*, 2003, pp. 559–566.

[22] G. A. Francia III, D. Thornton, J. Dawson, "Security best practices and risk assessment of SCADA and industrial control systems," Online.

https://pdfs.semanticscholar.org/3143/940955a76a49646ba2954e0735a0ec18d7ca.pdf?_ga=2.212045074.762791812.1582664590-1974441452.1582574286

[23] K. Huang, C. Zhou, Y.-C. Tian, S.-H. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 8153-8162, Oct. 2018.

[24] Y. Fu, J. Zhu, and S. Gao, "CPS information security risk evaluation system based on petri net," *IEEE Second International Conference on Data Science in Cyberspace (DSC)*, 2017, pp. 541-548.

[25] R. Zhang, Z. Zhao, and X. Chen, "An overall reliability and security assessment architecture for electric power communication network in smart grid," *International Conference on Power System Technology*, 2010, pp. 1-6.

[26] T. Meraj, S. Sharmin, and A. Mahmud, "Studying the impacts of cyber-attack on smart grid," *2nd International Conference on Electrical Information and Communication Technologies (EICT)*, 2015, pp. 461-466.

[27] M. A. Pai, Energy Function Analysis for Power System Stability, 1st ed. Boston, MA, USA: Springer US, 1989.

[28] L. Shi, C. Wang, L. Yao, Y. Ni, and M. Bazargan, "Optimal power flow solution incorporating wind power," *IEEE Systems Journal*, vol. 6, no. 2, pp. 233-241, Jun. 2012.

[29] DIgSILENT PowerFactory User Manual, DIgSILENT GmbH, 2018 [Online]. Available: https://www.digsilent.de/en/downloads.html

[30] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," *IEEE PES General Meeting*, 2010, pp. 1-6.

[31] Y. Huang and A. Cardenas,"Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 73-83, Oct. 2009.

[32] U. Shahzad, "The need for renewable energy sources," *International Journal of Information Technology and Electrical Engineering*, vol. 2, pp. 16-18, 2015.

[33] U. Shahzad and S. Asgarpoor, "Probabilistic evaluation of line loading and line active power in an active distribution network using numerical and analytical approaches," *North American Power Symposium (NAPS)*, 2018, pp. 1-6.

[34] U. Shahzad and S. Asgarpoor, "Probabilistic risk assessment of an active distribution network using Monte Carlo simulation approach," *North American Power Symposium (NAPS)*, 2019, pp. 1-6.

[35] Y. Xiang, L. Wang, and Y. Zhang, "Power system adequacy assessment with probabilistic cyber attacks against breakers," *IEEE PES General Meeting | Conference & Exposition*, 2014, pp. 1-5.

[36] J. Stamp, A. Mcintyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," *IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1-8.

[37] D. Dudorov, D. Stupples, and M. Newby, "Probability analysis of cyber attack paths against business and commercial enterprise systems," *European Intelligence and Security Informatics Conference*, 2013, pp. 38-44.

[38] U. Shahzad, "Resilience in electric power systems," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, pp. 1-6, 2021.

[39] Q. Wang, Z. Liu, and Y. Tang, "Design of a co-simulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems," *IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2019, pp. 430-434.

[40] X. Cai, Q. Wang, Y. Tang, and L. Zhu, "Review of cyber-attacks and defense research on cyber physical power system," *IEEE Sustainable Power and Energy Conference (iSPEC)*, 2019, pp. 487-492.

[41] H. Tu, Y. Xia, C. K. Tse, and X. Chen, "A hybrid cyber attack model for cyber-physical power systems," *IEEE Access*, vol. 8, pp. 114876-114883, 2020.

[42] S. Ghosh and M. H. Ali, "Exploring severity ranking of cyber-attacks in modern power grid," *IEEE Power & Energy Society General Meeting (PESGM)*, 2019, pp. 1-5.

[43] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: line-switching and new attack scenarios," *IEEE Transactions on Smart Grid*, vol. 10, pp. 1704-1712, Mar. 2019.

[44] Y. Chen, V. Mooney, and S. Grijalva, "A survey of attack models for cyber-physical security assessment in electricity grid," *IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*, 2019, pp. 242-243.

[45] B. Gao and L. Shi, "Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system," *IEEE Access*, vol. 8, pp. 30322-30331, 2020.

[46] Z. Dong, M. Tian, and J. Liang, "Cascading failures of spatially embedded cyber physical power system under localized attacks," *37th Chinese Control Conference (CCC)*, 2018, pp. 6154-6159.

[47] B. Huang, M. Majidi, and R. Baldick, "Case study of power system cyber attack using cascading outage analysis model," *IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1-5.

[48] U. Shahzad, "A review of challenges for security-constrained transmission expansion planning," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, pp. 21-30, 2021.

[49] U. Shahzad, "Impact of renewable generation on probabilistic dynamic security assessment of a power transmission system," *Australian Journal of Electrical and Electronics Engineering*, vol. 18, no. 3, pp. 181-191, 2021.

[50] U. Shahzad, "The concept of vulnerability and resilience in electric power systems," *Australian Journal of Electrical and Electronics Engineering*, vol. 18, no. 3, pp. 138-145, 2021.

[51] U. Shahzad, "Vulnerability assessment in power systems: a review," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, pp. 17-24, 2021.

[52] U. Shahzad, "Probabilistic security assessment in power transmission systems: a review," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, pp. 25-32, 2021.

[53] U. Shahzad, "Smart grid and electric vehicle: overview and case study," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 8, pp. 1-6, 2021.

[54] U. Shahzad, "Probabilistic transient stability assessment of power systems using artificial neural network," *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 8, pp. 35-42, 2021.