Determining Asset Criticality in Cyber-Physical Smart Grid

Yazeed Alrowaili, Neetesh Saxena and Pete Burnap

School of Computer Science & Informatics, Cardiff University, United Kingdom
{alrowailiyf,saxenan4,burnapp}@Cardiff.ac.uk

Abstract. Cybersecurity threats in smart grids have incredibly increased in the past years, and there is a strong need to protect these critical systems. Moreover, cyber-risk assessment and determining asset criticality are needed to apply the best remediation plan if the system is compromised. Still, due to the heterogeneity between operation technology (OT) and information technology, it is not easy to protect such a system altogether. Hence, the criticality of OT resources should be identified by their characteristics, helping operators understand that different assets can cause additional damage and require further protection or need more vital remediation plans. In this work, we proposed a methodology that can identify and indicate the frequency and impact of an asset in the system to determine its criticality. Moreover, the effectiveness and feasibility of the proposed method are evaluated by a 12-bus power system using the PowerWorld simulator by performing attacks on critical assets such as circuit breakers and evaluated their impact on the physical system. Finally, the test results demonstrate that targeting the most critical assets identified can severely impact the system while targeting the least critical assets is manageable.

Keywords: Smart grid, cyber risks, critical assets, attack impact, OT.

1 Introduction: Context and Motivation

Smart grids (SGs) can be classified as one of the many types of critical infrastructure. Moreover, it can monitor the flow of measurement units such as power from generation to consumption and match generation flow in real-time or near real-time by limiting and/or controlling any electrical load [1]. It provides control automation and transmit power from generation plants to transmission lines, distribution substations, and later to the consumers. Furthermore, cybersecurity threats targeting these systems have incredibly increased, and the failure to protect these OT assets will cause a significant impact [2]. According to the research analysis of the cyber-attack on the Ukrainian Power Grid done by E-ISAC and SANS ICS, on Dec. 23, 2015, there was a service outage on three energy companies that affected 225,000 customers for 3-7 hours in 103 cities [3]. Moreover, the current focus on protecting such a system is either specified on listing the possible attacks or attack paths that can occur on the system or classifying the criticality of ICS assets from an IT or business perspective [4]. Yet, there is little focus on criticality evaluation based on the damage that can occur after a successful attack on OT assets under physical processes.
Contribution. Firstly, we proposed a new method that identifies and determines the criticality of OT assets within the physical system. Secondly, we evaluated the proposed method using the PowerWorld with a 12-bus case by performing attacks on critical assets, such as circuit breakers, and measured their impact on the physical system. Finally, we analysed the damage when the most critical and the least critical assets are zero-day attacked, gaining unauthorised access to the system by exploiting software vulnerability [5].

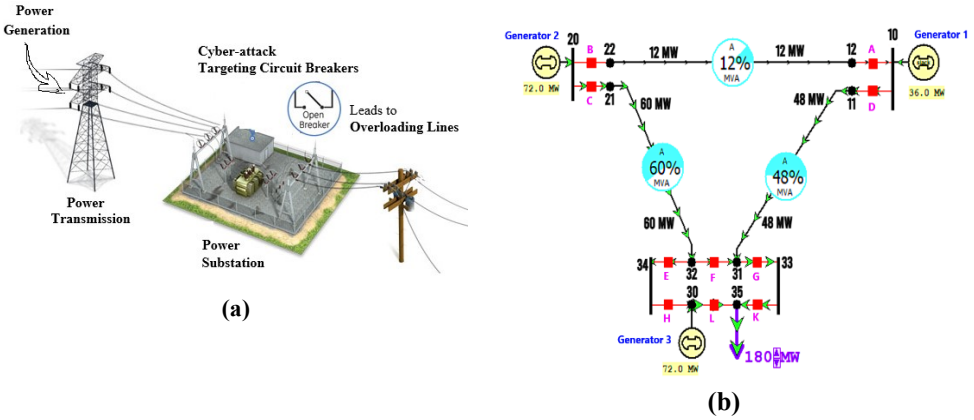

Fig. 1. (a) Smart grid substation system model. **(b)** 12-bus power system case normal scenario.

2 Related Work

Attacks targeting assets at physical level are challenging to deal with, as evaluating assets criticality in a SG system should be specific to its characteristics. In this direction, Hasan et al. [6] proposed a method to detect and evaluate paths to critical energy delivery system nodes with network heterogeneity. However, the work uses logs and host logs, which mostly exist in IT systems. Corallo et al. [9] proposed a metric to evaluate assets criticality in the context of industry 4.0, aiming to recognise and assess the critical assets in ICS to protect them against cyber threats. However, this work was mainly focused on what impact can occur from a business perspective and quite limited in terms of offering a comprehensive evaluation for assets criticality in OT. Crespo et al. [10] proposed criticality evaluation in power line systems to offer a reliable, fast-maintained process in these systems by performing asset criticality evaluation and use the collected information to update the appropriate maintenance plan. Nevertheless, this work concentrates on assets maintenance strategy and determining its criticality they deal with, and the evaluation was also conducted on limited nodes. Recently, Vallant et al. [7] offer risk assessment methodology by identifying all possible vulnerabilities to cyber secure SG systems. However, thw work focuses potential threats and the likelihood of successful attacks only. In order to fill the gaps in identifying asset criticality in OT systems and evaluating cyber risks impact on the physical systems, we not only proposed a method for discovering OT assets with most and least criticality, but also evaluating their impact on smart grid system using PowerWorld simulator.

3 Approach

Our aim is to propose a method that can identify the most critical assets in the physical system and evaluates adverse impact that may occur when the system is compromised.

3.1 System Model and Simulation Scenario

Fig.1(a) presents a power substation system model where an adversary can target critical assets such as circuit breakers or transformers to create physical and/or operational damage to the system. Further, Fig.1(b) shows a test case of a 12-bus system regularly operated

with normal scenario on the Powerworld simulator. Moreover, this case was used to show this study on critical components, and it contains 12 buses, 3 generators, 10 breakers and one load. Furthermore, the focus is identifying the most critical asset (circuit breakers), seen as red squares. When an adversary attacks critical circuit breakers, it will cause all generators to increase their reactive power *(Mvar)*, consequently reducing system reliability and efficiency, making the system to no longer supply load, which can cause a blackout [8].

3.2 Proposed Method

We present the proposed method to determine criticality of each asset in the smart grid system and evaluate their cyber impact using PowerWorld tool. This method can be generalized to other cyber-physical systems considering relevant devices and OT operational impact. Further, identify most and least critical assets (scanning devices and apply our method) and then apply risk assessment methodologies to analyse cyber risks, and evaluate their impact (e.g., simulation) on physical systems. In our scenario, we determine each circuit breaker based on its frequent occurrence in use while supplying power from a *generator* to the load using a specified path. Moreover, this can be applied by identifying all possible *P* paths that a generator *(i)* uses to transmit the power as per the load requirement, then assess how many times (how frequently) a circuit breaker *(i)* Cb_i is used in all paths. The criticality can be calculated as: Criticality = Cb_i / P (1)

Algorithm1 Calculate Criticality of an Asset in Smart Grid

Input: All paths *P* for generator *(i)* & Number of frequent uses of Cb_i in all paths.
Output: Criticality score for Cb_i linked to a specified generator.

1: Let **P** denote total number of paths generator *(i)* uses to transmit the power to the load.
2: Let $\mathbf{Cb_i}$ indicate how many times circuit breaker *(i)* has been used in all paths **P**.
3: Applying *Equation (1)* listed above. *(where $0 \leq score \leq 1$)*
4: **if (**Cb_i score is > 0.5 *(meaning that Cb_i has appeared in more than half of paths)*) **then**
5: Declare most critical asset.
6: **else**
7: Declare least critical asset.

Table 1. Shows all possible paths and circuit breakers that existed in each path generator *(1,2,3)* uses to transmit power to load.

ID		A	B	C	D	E	F	G	H	L	K
Gen1	Path 1	✓	✓	✓			✓	✓			✓
	Path 2				✓			✓			✓
	Path 3				✓	✓	✓		✓	✓	
Gen2	Path 1	✓	✓		✓			✓			✓
	Path 2			✓		✓			✓	✓	
	Path 3			✓			✓	✓			✓
Gen3	Path 1									✓	
	Path 2					✓	✓	✓	✓		✓

Table 1 shows the frequent use of circuit breakers in all paths for *generators 1, 2, and 3*. Moreover, applying *Algorithm 1* in all generators with the giving data will indicate that circuit breakers ***(D, F, G, K)*** are considered the critical asset for ***generator 1***, and for ***generator 2*** are ***(C, G, K)***. Moreover, circuit breaker ***(L)*** is considered critical as the other breakers since it is the only breaker used in a specific path with ***generator 3***. Therefore, the most critical circuit breakers in this 12-bus system test case are ***(D, F, G, C, K, L)***.

4 Experimental Results and Evaluation

This section shows an evaluation of our methodology when targeting the system's critical assets with zero-day attack and monitor generators reactive power *(Mvar)* for any changes.

4.1 System Operations under No Attack Scenario:

Table 2 shows generators information under a normal scenario, indicating that the measurements of *(Gen MW)* and *(Gen Mvar)* are normal and the system is under control, as shown in Fig. 1. We have kept *Gen MW* constant for our experiments and observing *Gen Mvar* values when targeting most vs. least critical assets in the system.

Table 2. Generators measurements on normal scenario

ID	Number of Bus	Name of Bus	Gen *MW*	Gen *Mvar*
1	10	10	36.00	1.23
2	20	20	72.00	1.88
3	30	30	72.00	2.97

4.2 System Operations under Attack Scenario:

Table 3 shows generators measurements when targeting the most critical circuit breakers [(F, L), C, D]. It can be seen that compromising the most critical breakers made the reactive power *(Gen Mvar)* for related generators increasing highly, which can cause overloaded transmission lines and/or overheating, as demonstrated in Fig. 2. For example, opening F and L circuit breakers (for generator 3) increases *Gen Mvar* (44.13 and 12.81) for generator 1 and 2, respectively, while it is further decreased for generator 3 (2.74) as compared to original *Gen Mvar* values from Table 2. As a result, line 10-20 and 10-33 are overloaded with 144% and 183%, respectively. This is true for other two cases as reflected in Fig. 2, when a circuit breaker C and D are opened in each case, which resulted into overloading lines 10-33 and 20-34 with 108%.

Table 3. Generator's measurements when targeting most critical circuit breaker (D)*, (C) or (F, L)*

Gen ID	Gen *MW for (F, L)*	Gen *Mvar for (F, L)*	Gen *MW for (C)*	Gen *Mvar for (C)*	Gen *MW for (D)*	Gen *Mvar for (D)*
1	36.00	44.13	36.00	8.47	36.00	0.65
2	72.00	12.81	72.00	1.60	72.00	6.51
3	72.00	2.74	72.00	5.83	72.00	5.88

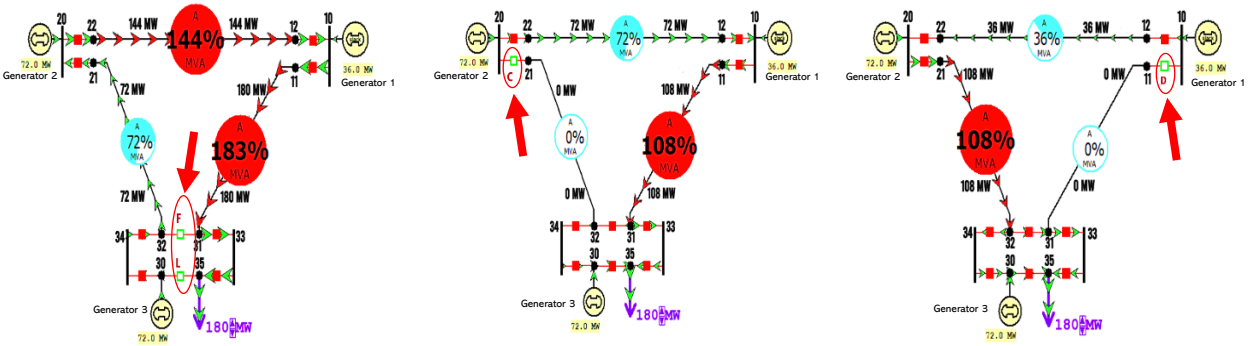

Fig. 2. Attacker compromises most circuit breakers in respective order *(F, L), (C), and (D).*

Further, Table 4 shows generators' measurements when targeting some of the least critical circuit breakers. Moreover, it can be seen that compromising the least critical breakers made the reactive power *(Gen Mvar)* for relevant generators increase slightly. Yet, it can be seen in Fig. 3 that the system is under control, and there are no threats or overload in transmission lines. As we can observe, line 10-20 is disconnected after opening A and B circuit breakers, whereas the lines 20-34 and 10-33 are with 72% and 36% capacity, respectively, once H circuit breaker is further opened.

Table 4. Generator's measurements when targeting the least critical circuit breakers *(A, B, H)*

Gen ID	Gen *MW for (A, B, H)*	Gen *Mvar for (A, B, H)*
1	36.00	0.66
2	72.00	2.61
3	72.00	3.25

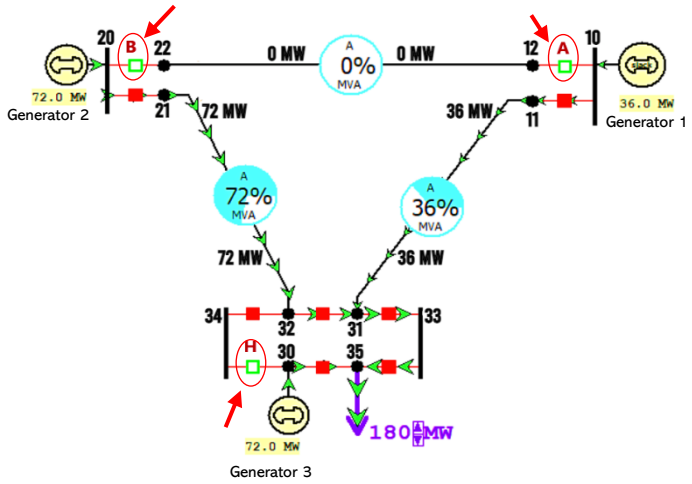

Fig. 3. Attacker compromises the least critical circuit breakers *(A, B, H)*.

5 Conclusion and Future Work

In conclusion, this work has summarised the importance of protecting critical infrastructure with smart grid as a case study. Moreover, it emphasises an approach for determining and evaluating the criticality of assets located in OT at physical level. Furthermore, a simulation approach to evaluate the criticality of the physical smart grid system under attack scenarios is also presented, which reflects the potential impact on the physical system. After determining critical assets, our results show that targeting the most critical assets identified in this work can severely compromise the system, making transmission lines to be overloaded beyond their capacities. while targeting the least critical assets is manageable and transmission lines are within the specified range along with stability of the overall system. In the future, we aim to extend this work to determine critical assets at higher levels with a scalable system (e.g., 37-bus case). Moreover, we aim to build a comprehensive methodology to compute and quantify criticality for assets starting from enterprise until the process level assets associated with processes and operations.

References

1. European Commission, “European Technology Platform,” *Energy*, vol. 19, no. 3, p. 44, 2006, Accessed: Feb. 22, 2021. [Online]. Available: http://europa.eu.int/comm/research/energy.
2. C. Ten, G. Manimaran and C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," in *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853-865, July 2010.
3. R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *Electr. Inf. Shar. Anal. Cent.*, p. 36, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
4. A. Corallo, M. Lazoi, M. Lezzi and P. Pontrandolfo, "Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level," *IEEE Transactions on Engineering Management*, 2021.
5. J. Frankenfield, “Zero-Day Attack Definition,” May 08, 2020. https://www.investopedia.com/terms/z/zero-day-attack.asp (accessed Jul. 10, 2021).
6. K. Hasan, S. Shetty, S. Ullah, A. Hassanzadeh, and E. Hadar, “Towards optimal cyber defense remediation in energy delivery systems,” *IEEE GLOBECOM*, 2019.
7. H. Vallant, B. Stojanović, J. Božić, and K. Hofer-Schmitz, “Threat modelling and beyond-novel approaches to cyber secure the smart energy system,” *Appl. Sci.*, vol. 11, no. 11, 2021.
8. HYTEPS, “Reduce your reactive power improves efficiency and saves costs,” *HYTEPS*, 2019. https://hyteps.com/power-quality/reactive-power/ (accessed Jul. 11, 2021).
9. A. Corallo, M. Lazoi, and M. Lezzi, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts,” *Comput. Ind.*, vol. 114, p. 103165, 2020.
10. A. Crespo *et al.*, “Criticality Analysis for improving maintenance, felling and pruning cycles in power lines,” in *IFAC-PapersOnLine*, 2018, vol. 51, no. 11, pp. 211–216.