A Decision Support Tool for Estimating the Relative Susceptibility of Electricity Distribution Grids to Cyberattacks

1st Xavier Weiss
Electric Power and Energy Systems
KTH Royal Technical Institute
Stockholm, Sweden

2nd Lars Nordström
Electric Power and Energy Systems
KTH Royal Technical Institute
Stockholm, Sweden

3rd Patrik Hilber
Electric Power and Energy Systems
KTH Royal Technical Institute
Stockholm, Sweden

***Abstract*—When considering the resilience of present and future power systems, cyberattacks are an evolving risk category. To balance cyber risks against other risks, cyber security assessment tools are needed. Existing tools tend to assume information about the attacker, the types of vulnerabilities in the system, and specific characteristics of the system, that in reality are often unknown. An open-source cybersecurity decision support toolbox called Threats2Power is therefore suggested that is designed to allow decision makers to balance cyberattacks against other risks. It fills the gap between highly-detailed cybersecurity tools and qualitative risk assessments. The toolbox has been validated by assessing it on both the CIGRE MV benchmark grid and a real-world LV grid. The proposed tool will enable distribution system operators to estimate the risk of incoming events before detailed information about the nature and severity of the threat is known, and put it side-by-side with estimates of other risks. Thanks to its more abstract formulation, the toolbox also enables researchers and companies to compare, share, and analyze network designs without exposing confidential information.**

***Index Terms*—Resilience, Decision Support Systems, Cyber-physical Energy and Communication Systems, Monte Carlo methods, Power System Vulnerability**

I. Introduction

Resilience against cyberattacks is particularly important in power system operation, where compromised equipment can potentially cause blackouts. It would therefore help decision makers to have an indicator that told them how susceptible their communication network is to cyberattacks, compared to other risks like extreme weather or physical attacks.

Threats2Power fills a gap between attack tree/graph-based cybersecurity tools and Cyber-Physical Power System (CPPS) simulations. Monte Carlo (MC) simulations have been used to avoid some of limitations of these approaches by applying probabilistic assessments instead of scanning for system-specific vulnerabilities. We consolidate these MC-based methods into a reusable open-source toolbox. In addition to testing the toolbox on a CIGRE MV grid and a real-world LV grid, we also propose an apparent power based definition of criticality that could help link cybersecurity results from a MC approach to physical operations without requiring dynamic co-simulation.

This work was funded by the Swedish Energy Agency (P2022-00692). Computations were enabled by the National Academic Infrastructure for Supercomputing in Sweden (NAISS), partially funded by the Swedish Research Council (P2022-06725).

In the critical domain of the electrical grid, cybersecurity tools have been applied to identify vulnerabilities and improve cyber resilience. For instance, ICSlang (a domain-specific language in the Meta Attack Language (MAL) [1]) is applied in [2] on a Ukrainian attack scenario and in [3] to perform a risk assessment on a IEEE-39 bus system. MulVAL is used in combination with network scanning and intrusion detection systems in [4] to model the impact of cyberattacks on a SCADA system in the energy domain. Most studies, however, have been constructed ad hoc without a specialized toolbox. Deep learning is for instance applied in [5] to predict network traffic, detect anomalous activity and generate attack graphs. Bayesian networks are constructed for 1 to 2000 bus electrical grids in [6] to compute the probability of compromise. However, without a reusable toolbox, the methods from these ad hoc studies cannot be readily applied.

A number of tools / frameworks have been developed to co-simulate power systems and information systems. The purpose of these tools is to provide detailed models of CPPS, including the impact of communication delays [7], the impact of cyberattacks on the data being transmitted [8], and the impact of failed communication nodes [9]. Hardware-in-the-loop co-simulators have been used in [10] to see how bad PMU data can result in power system faults and in [11] to see how data dropping, data interception and data manipulation impact the operators ability to supply loads. While Threats2Power could be used as a simple co-simulation tool, it is primarily designed to be an external decision support tool for performing cyber security assessments at a higher level of abstraction than these cyber-physical co-simulators.

Here, and throughout this paper, the term 'abstract' refers to the deliberate reduction in model precision/detail in Threats2Power compared to previous CPPS and cybersecurity models. As argued in [12], this improves both the analytical tractability and transparency of the Threats2Power models, which are desirable characteristics for a decision support system. By making as few and as simple assumptions as possible, we ensure the susceptibility indicator from Threats2Power remains relevant under changing technologies, security policies, and exploits.

MC-based methods have been applied extensively to analyze CPPSs. In [13] sequential MC simulations are used to determine the effect of physical and cyber failures and

979-8-3315-8138-1

thereby derive the financial loss to the operator. In [14] a similar sequential MC simulation is combined with a linear programming problem to calculate maximum power flows and, from there, derive reliability indices. The vulnerability of specific components to cyberattacks is derived in [15] using MC sampling. Strategies for dynamic defense allocation are explored in [16] by sampling the rate at which attacks occur from a Poisson distribution. These studies show that MC-based approaches are especially valuable when little cybersecurity data is available. We therefore apply MC simulations in Threats2Power's abstract approach.

In an electrical grid some components may be more critical to maintaining power than others. Link criticality is used as a proxy for criticality in [17]. In [18], instead of a single missing link, the probability of function loss is proposed as a criticality measure based on N-1, N-2 and N-3 scenario analysis. Finally, in [19] critical components are identified in several scenarios via a tri-level optimization problem where attackers have finite budgets and follow a heuristic attack strategy. However, in reality, the criticality of a component will depend on the exact operational conditions present when it is exploited. We therefore proposes a novel criticality metric based on the physical characteristics of the system, rather than one or more operational scenarios.

The Threats2Power toolbox presented in this work includes the following contributions:

1) Development of a Monte Carlo algorithm for approximating the distribution of compromised devices for any power system communication network. This is packaged into a reusable, open-source toolbox that enables high-level decision support regarding cyber risks.
2) A method for linking the compromise of specific communication network devices to the impact they have on the power system, by introducing a Maximum Theoretical Capacity (MTC) based proxy for the criticality of power system equipment.
3) A statistical approach for summarizing the general susceptibility of the Distribution System Operator (DSO) to cyberattacks by analyzing the criticality distribution produced by a Monte Carlo simulation.

II. Process

Threats2Power is a cybersecurity decision support toolbox which determines the susceptibility to cyberattacks of a power grid and its communication network. As shown in Figure.1, it takes a communication network topology and attacker budget as input, runs a MC simulation on it and then produces a statistical distribution of the number of devices that were compromised in N simulated attacks. The communication network can either be a real network, if the user has access to one, or a procedurally generated one from [20]. If a power system topology is also provided, it can produce a criticality distribution based on the importance of the power system equipment the communication network device monitors. The susceptibility indicator is then defined as the average (mean) of the criticality distribution for a grid section. This indicator can be compared numerically between different networks, so a higher value indicates the network is more susceptible to cyberattacks.

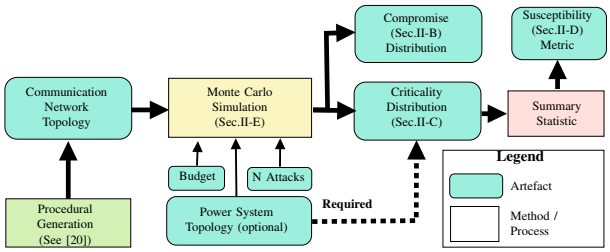

Fig. 1: Typical workflow in Threats2Power, the power system topology is required to build a criticality distribution.

A. Effort

Effort represents the amount of time and/or resources required by an attacker to compromise an asset. Inspired by [1], this is by default modelled by sampling an exponential distribution:

$$Effort = -\frac{\ln(U)}{\lambda} \tag{1}$$

were λ is a rate parameter and U is a uniform distribution in the range $(0, 1)$. To capture the greater security/robustness of components higher in the hierarchy, λ is set to 0.01 for the control centre, 0.1 for the aggregators and 1 for devices. While expert-based numbers from [1] could be used here, this would reduce the level of abstraction of Threats2Power.

B. Compromise

Since exploits can fail, once an attacker has expended the necessary amount of effort in (1), the asset either becomes compromised or not. This is evaluated based on a Bernoulli distribution:

$$Compromise(k; p) = p^k(1-p)^{(1-k)}$$

Where p is the probability of success (0.5 by default for all assets), and $k \in \{0, 1\}$ is the binary outcome.

C. Criticality

The total criticality by MTC for a physical grid can be derived as follows:

$$C_{MTC} = \sum_{(i,j)\in\mathcal{B}, i\neq j} \overline{S_{i,j}} + \sum_{k\in\mathcal{I}_i} \overline{S_k} \tag{2}$$

$$\text{Where } \overline{S_{i,j}} = U_i \overline{I_{i,j}} n_{i,j} \quad \text{lines}$$

$$\overline{S_{i,j}} = \overline{S_{i,j,rated}} \quad \text{transformers}$$

$$\overline{S_k} = \sqrt{\overline{P_k^2} + \overline{Q_k^2}} \quad \text{other components}$$

were $\mathcal{B}$ is the set of buses and $\mathcal{I}_i$ is the set of components at bus i. $\overline{S_{i,j}}$ is the maximum magnitude of the apparent power in the line or transformer between bus i and bus j. U_i is the nominal voltage magnitude at bus i, $\bar{I}_{i,j}$ is the thermal limit of the line, and $n_{i,j}$ is the number of parallel lines between bus i and j. $\overline{S_k}$ is the maximum magnitude of the apparent power consumed or produced by the k^{th} component located at substation i, which is found from the size of the real $\overline{P_i}$ and

reactive $\overline{Q_i}$ power of that component. To deduce compromised criticality, in this study, we map one communication device to each bus, load, line, generator, transformer, and switch.

The MTC metric is presented in action on the CIGRE MV Benchmark [21] in Figure.2. MTC is quasi-static, since it does not depend on the real-time state of the system. It is also easy to evaluate and has a well-defined unit that enables comparisons to be made between different grid sizes/voltages.

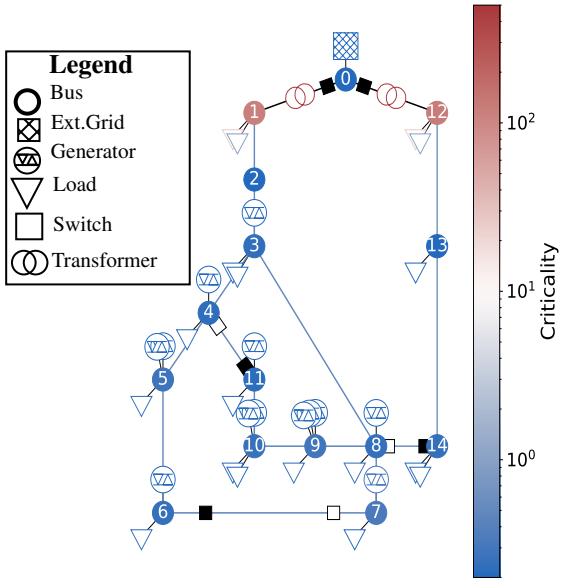

Fig. 2: Criticality by MTC for CIGRE MV Benchmark.

D. Susceptibility

Susceptibility is defined as the average number of devices compromised in a random cyberattack, weighted by their criticality:

$$\text{Susceptibility} = \frac{\sum_0^N \sum_{j=0}^D \sigma_j C_j}{N} \tag{3}$$

Where N is the number of random attacks simulated (MC runs), D is the number of devices in the communication network, $\sigma_j \in \{0, 1\}$ is a binary variable indicating whether the j^{th} device was compromised and C_j is the criticality of the j^{th} device. Using MTC from (2), susceptibility is thus the average amount of apparent power capacity (in MVA) a random cyberattack will compromise.

E. Monte Carlo Approach

The compromise distribution of a communication network can be estimated through a MC simulation. Since the number of attacks simulated is finite, the MC approach only approximates the true compromise distribution, but is thus able to work on larger networks.

Algorithm.1, shown in action in Figure.3, represents a single MC simulation where the entrypoint, attack path, effort required to compromise and probability to compromise are all randomly sampled. The random attacker will continue until there are no more nodes left to compromise or they have run out of budget. The results of the attack are stored, from which the compromise / criticality distributions are gradually built.

Algorithm 1 Pseudocode of Monte Carlo analysis algorithm

```
node = entrypoint
budget = total_budget
available = set(); visited = set(); compromised = set();
visited.add(node)
if ¬node.compromised then                ▷ Try to compromise
    is_successful, effort_spent = node.attack(budget)
budget = budget − effort_spent
if is_successful then
    available.update(node.neighbours)
    compromised.add(node)
available = available − visited           ▷ Difference of 2 sets
if budget > 0 and Length(available) > 0 then
    node = Random(available)
    GOTO Line 4
```

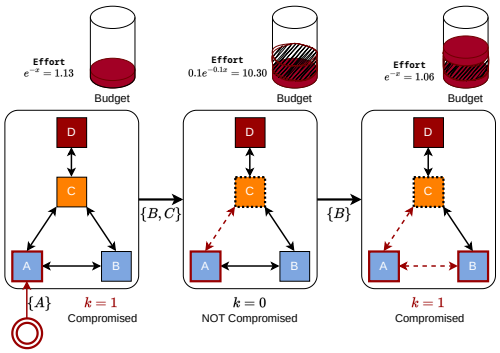

Fig. 3: Illustration of Algorithm.1 in action on a 4-node communication network

III. Testing

A. CIGRE MV Grid

To evaluate criticality, a physical grid is needed. For this a communication network was generated using [20] for the CIGRE MV benchmark [21], as shown in Figure.4.

The effect of increasing the attacker's budget is visible in Figure.5. Evidently, as the budget increases the number of compromised devices tends to increase as well. As a compromise between accuracy and computation time, a budget of 100.0 will be used when constructing the criticality distributions. A limitation of this approach is that because the real-world variation in skill and available resources of attackers is unknown, the actual compromise distribution may be shifted to the right (underestimated budget) or to the left (overestimated budget). Nevertheless, if all DSOs are evaluated with the same budget it still enables a relative comparison between them.

By also calculating the criticality for each attack, a criticality distribution can be constructed - as shown in Figure.6. Here $1,000,000$ attacks are simulated, with each attack launched from a randomly selected entrypoint. Computation time for the $1,000,000$ attacks used on the CIGRE network was 31.06 minutes on two EPYC™ Zen2 2.25 GHz 64-core processors, with 255 CPU threads dedicated to attacks and one dedicated to data collection. The number of compromised assets in each cyber attack, multiplied by their individual criticality, is aggregated into bins. Two bin widths are shown to help

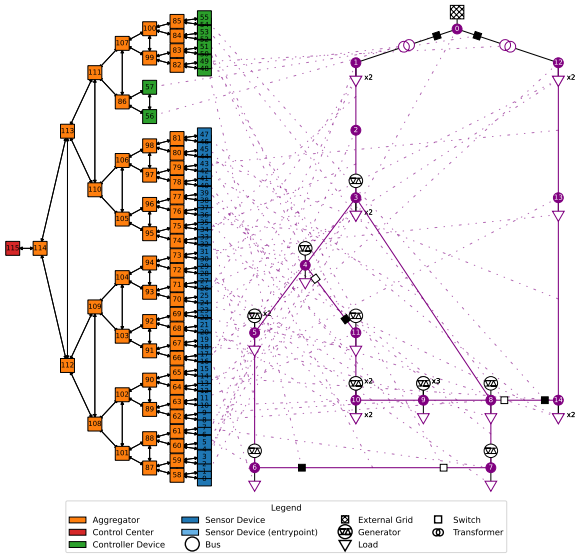

Fig. 4: CIGRE MV benchmark. Devices in the communication network (LHS) map one-to-one to specific equipment in the physical grid (RHS).

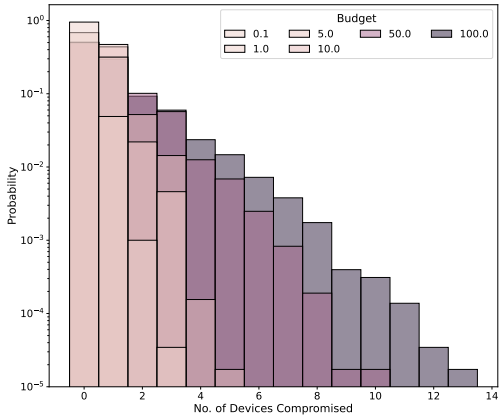

Fig. 5: Variation in compromise distribution with differing budgets of the attackers. The distributions of success probability for each component are ignored in this test.

identify smaller variations (bin width of 1) and draw focus to the overall trends (bin width of 5). For instance, the higher-probability region between 35 and 40 MVA is likely due to a combination of the communication network asymmetry seen in Figure.4 (see branch below aggregator 111) and the greater effort required, on average, to compromise an aggregator (internal node) compared to a device (leaf node).

The susceptibility of a DSO is then defined as the mean of its criticality distribution, in this case it is 13.21 MVA (compared to 191.6 MVA if the entire network were compromised). The 95% highest density interval, highlighted in red, lies between 0.0 and 50.0 MVA.

B. Real LV Grid

In order to validate Threat2Power's applicability to real distribution grids, the non-synthetic Low Voltage (LV) grid shared in [22] and shown in Figure.7 is considered.

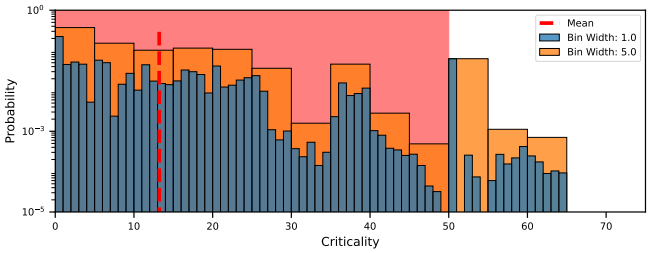

Fig. 6: Criticality Distribution for attackers with a budget of 100.0. Susceptibility is defined as the average (mean) critica

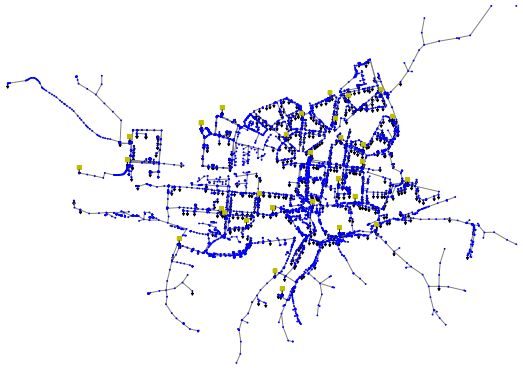

Fig. 7: LV Grid from [22] after conversion to PandaPower

Similar to the CIGRE network, $1,000,000$ randomized attacks with a budget of 100.0 are launched from one randomly selected entrypoint at a time. This means that on average, each node in the network will have 77 attacks that use it as an entrypoint (compared to 8621 for the CIGRE MV network). Due to the symmetry of the network (there is no deviation in the no. of children per aggregator) this is likely sufficient to capture the general susceptibility of the network, however this does imply that the distribution may not have converged close to the 'true' distribution. Computation time for the $1,000,000$ attacks used on the full LV network was 165.73 minutes, compared to 31.06 minute for the CIGRE network using the same hardware.

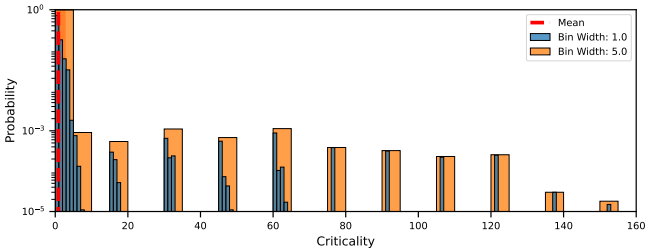

Fig. 8: Criticality distribution for real LV grid

As evidenced by the results in Figure.8, attackers with the same budget as a small network will usually only be able to compromise a much smaller fraction of a large network. This effectively means that a larger physical grid is more resilient against cyberattacks by virtue of having more components that need to be compromised in order for the attacker to have a noticeable impact on power system operation. However, this result may not hold if the network has many components with identical settings, for instance if they are all purchased at the

same time from the same vendor, since an attacker can then potentially re-use exploits.

The resulting susceptibility indicator is 0.86 MVA (compared to 1511.05 MVA if the entire network were compromised) which is lower than the 13.21 MVA of the CIGRE MV network in Figure.6. The 95% highest density interval, highlighted in red, lies between 0.0 and 2.72 MVA. The settings for aggregator and device defenses were identical between the two communication networks, hence the differences in susceptibility are most likely due to a larger network topology, which requires longer attack paths to reach the next device. The LV grid has more gaps in the criticality distribution than the CIGRE MV grid. These are likely due to certain high value (in terms of power capacity) assets such as the 30 transformers, which in a random walk are less likely to be visited than the greater number of single and three phase loads.

IV. Conclusion

Threats2Power takes a power system communication network and assesses its susceptibility to cyberattacks using a Monte Carlo approach. By associating a communication network with physical equipment, Threats2Power can also help determine how critical a compromised communication component is to the operation of the grid. The resulting susceptibility indicator, weighted by criticality, enables decision-makers to compare the risk of cyber threats to their system to that of other threats, such as extreme weather and physical attacks. The features of the toolbox have been demonstrated both on a medium voltage benchmark grid and a low voltage real world grid. In future work, the susceptibility indicator calculated by Threats2Power could be used to improve power system operation by weighting risks from incoming cyber threats as they occur.

Acknowledgments

A special thanks to Prof. Hussain Kazmi (KU Leuven) and Prof. Lennart Söder (KTH) for providing feedback on the article.

Open Source Repository

GitHub: https://github.com/DEUCE1957/Threats2Power

References

[1] W . Wideł, et al. (2023) The meta attack language - a formal description. Computers & Security(130), doi: 10.1016/j.cose.2023.103284

[2] S. Hacks, et al. (2022). A Multi-level Cyber-Security Reference Model in Support of Vulnerability Analysis. In: Almeida, JPA, Karastoyanova, D, Guizzardi, G, Montali, M, Maggi, FM, Fonseca, CM (eds) Enterprise Design, Operations, and Computing. EDOC 2022. Lecture Notes in Computer Science, vol 13585. Springer, Cham. doi:10.1007/978-3-031-17604-3_2

[3] I. Semertzis I, et al. (2022) Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs. In: Proceedings of the 10th Workshop on modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1-6, doi:10.1109/MSCPES55116.2022.9770140

[4] M.A. Haque, et al. (2020). Modeling Mission Impact of Cyber Attacks on Energy Delivery Systems. In: Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N. (eds) Security and Privacy in Communication Networks. SecureComm 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 336. Springer, Cham. doi:10.1007/978-3-030-63095-9_3

[5] A. Presekal, et al. (2023) Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Transactions on Smart Grid 14, pp. 4007-4020. doi: 10.1109/TSG.2023.3237011

[6] S. Sun, et al. (2024), A graph embedding-based approach for automatic cyber-physical power system risk assessment to prevent and mitigate threats at scale, IET Cyber-Physical Systems: Theory & Applications 8, pp. 91-108, Wiley Online Library. doi:10.1049/cps2.12047

[7] G. Celli, et al. (2014) "DMS Cyber-Physical Simulation for Assessing the Impact of State Estimation and Communication Media in Smart Grid Operation," in IEEE Transactions on Power Systems, vol. 29, no. 5, pp. 2436-2446, doi: 10.1109/TPWRS.2014.2301639.

[8] Y. Cao, et al. (2018) "A Simplified Co-Simulation Model for Investigating Impacts of Cyber-Contingency on Power System Operations," in IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4893-4905, doi: 10.1109/TSG.2017.2675362.

[9] J.H. Kazmi, et al. (2016) "A flexible smart grid co-simulation environment for cyber-physical interdependence analysis," Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Vienna, Austria, pp. 1-6, doi: 10.1109/MSCPES.2016.7480226.

[10] M. Kezunovic, et al. (2017) "The use of system in the loop, hardware in the loop, and co-modeling of cyber-physical systems in developing and evaluating new smart grid solutions." Proceedings of the 50th Hawaii International Conference on System Sciences, doi: 10.24251/hicss.2017.385

[11] Z. Liu, Q. Wang, Y. Tang (2020) "Design of a Cosimulation Platform With Hardware-in-the-Loop for Cyber-Attacks on Cyber-Physical Power Systems," in IEEE Access, vol. 8, pp. 95997-96005, doi: 10.1109/ACCESS.2020.2995743.

[12] Greif, Hajo. "Analogue models and universal machines. Paradigms of epistemic transparency in artificial intelligence." Minds and Machines 32.1 (2022): 111-133.

[13] Z. Liu, et al. (2021) "An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats," in IEEE Transactions on Power Systems, vol. 36, no. 2, pp. 851-864, doi: 10.1109/TPWRS.2020.3018701

[14] R. He, et al. (2020), "Reliability Modeling and Assessment of Cyber Space in Cyber-Physical Power Systems," in IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 3763-3773, doi: 10.1109/TSG.2020.2982566

[15] W. Wang, A. Cammi, F.D. Maio, S. Lorenzi, E. Zio (2018) "A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants", Reliability Engineering & System Safety, Volume 175, pp. 24-37, ISSN 0951-8320, doi:10.1016/j.ress.2018.03.005.

[16] M. D. Smith, M. E. Paté-Cornell (2018) "Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment," in IEEE Transactions on Engineering Management, vol. 65, no. 3, pp. 434-447, doi: 10.1109/TEM.2018.2798408

[17] P. C. Haritha, M. Anjaneyulu (2024) "Comparison of topological functionality-based resilience metrics using link criticality." Reliability Engineering & System Safety 243, doi: 10.1016/j.ress.2023.109881

[18] Šarūnienė, I., et al. (2024) "Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements." Reliability Engineering & System Safety 243, doi: 10.1016/j.ress.2023.109797

[19] Z. Liu, L. Wang (2022) "A Distributionally Robust Scheme for Critical Component Identification to Bolster Cyber-Physical Resilience of Power Systems," in IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 2344-2356, doi: 10.1109/TSG.2022.3147421

[20] X. Weiss, L. Nordström, P. Hilber P, E. Suren (2024) Procedural Generation of Communication Networks in Power Systems. Paper presented at the 15th Doctoral Workshop on Energy Informatics (DACH+), Mendrisio, Switzerland, 9 October 2024. doi:arXiv:2410.09405

[21] K. Strunz, et al. (2014) Benchmark systems for network integration of renewable and distributed energy resources. Conseil international des grands réseaux électriques (CIGRE), Task Force C6.04, April 2024. ISBN: 978-285-873-270-8.

[22] A. Koirala, et al. (2020) Non-synthetic European low voltage test system. International Journal of Electrical Power & Energy Systems 118:105712. doi:10.1016/j.ijepes.2019.105712