Poster: Cybersecurity Research and Training for Power Distribution Grids – A Blueprint

Martin Henze*
Fraunhofer FKIE
martin.henze@fkie.fraunhofer.de

Lennart Bader*
Fraunhofer FKIE
lennart.bader@fkie.fraunhofer.de

Julian Filter
RWTH Aachen University
julian.filter@rwth-aachen.de

Olav Lamberts
Fraunhofer FKIE/RWTH Aachen Univ.
olav.lamberts@rwth-aachen.de

Simon Ofner
Fraunhofer FKIE
simon.ofner@fkie.fraunhofer.de

Dennis van der Velde
Fraunhofer FIT
dennis.van.der.velde@fit.fraunhofer.de

ABSTRACT

Mitigating cybersecurity threats in power distribution grids requires a testbed for cybersecurity, e.g., to evaluate the (physical) impact of cyberattacks, generate datasets, test and validate security approaches, as well as train technical personnel. In this paper, we present a blueprint for such a testbed that relies on network emulation and power flow computation to couple real network applications with a simulated power grid. We discuss the benefits of our approach alongside preliminary results and various use cases for cybersecurity research and training for power distribution grids.

CCS CONCEPTS

• **Security and privacy → Network security**; *Intrusion detection systems*; • **Networks → Cyber-physical networks**; • **Computing methodologies → Modeling and simulation**.

KEYWORDS

security, cyber-physical systems, power grid, testbed, simulation

ACM Reference Format:
Martin Henze, Lennart Bader, Julian Filter, Olav Lamberts, Simon Ofner, and Dennis van der Velde. 2020. Poster: Cybersecurity Research and Training for Power Distribution Grids – A Blueprint. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), November 9–13, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3372297.3420016

1 MOTIVATION AND RELATED WORK

Power grids exhibit an increasing digitization and deployment of communication infrastructure [11], raising their susceptibility to advanced cyberattacks with potentially disastrous consequences [4]. Power *distribution* grids are especially prone to cyberattacks due to their heterogeneity and the ongoing integration of digital assets [4].

Resulting security threats render the mitigation of and appropriate reaction to attacks inevitable. Unlike home or corporate networks, cyber-physical systems (CPSs) also require to consider physical interactions [2]. We assess that simulation is best-suited to realistically model the physical aspects of a power grid along with its communication infrastructure in a flexible and efficient manner.

A simulated power grid enables various cybersecurity research and training functionalities, ultimately leading to more secure power grids. First and foremost, investigating real-time effects of attacks on the power grid, the communication network, and the operator's behavior becomes possible. Likewise, extensive datasets of physical grid state as well as benign and malicious network traffic can be created in a scalable and efficient manner, e.g, to train intrusion detection systems (IDSs). Further, different security approaches can be tested and evaluated, e.g., to optimize deployment of IDSs, or assess their impact on network and grid stability. Finally, we can realize training environments in which the detection of and reaction to cyberattacks can be trained in a realistic setting.

Consequently, simulation testbeds accompany huge potentials for cybersecurity in power distribution grids. Different related work already considered the so-called co-simulation of power grid and communication from different angles [7, 8, 12], mainly with the goal to study grid operation. Hence, these works typically either do not precisely model communication or do not allow for an easy integration of existing attack and defense applications. In contrast, DSSNet [3] is a hybrid simulation-emulation testbed that allows to execute real networking applications, but still abstracts from actual used communication protocols in the energy sector. Although MiniCPS [2] provides a toolkit for cybersecurity research and training for CPSs, it does not support power grids. Thus, a comprehensive environment for cybersecurity in power grids is missing.

In this paper, we present a blueprint for a testbed for cybersecurity in power grids and substantiate its benefits alongside various use cases. Specifically focusing on power *distribution* grids along with the widely used IEC 60870-5-104 protocol, we propose to combine the (communication) network emulator Mininet [6] with the power flow solver pandapower [10] to couple real network applications with a simulated power grid. Hence, we target use cases in cybersecurity research ranging from attack and security evaluations over dataset generation to teaching and training.

2 BLUEPRINT FOR A SECURITY TESTBED

A cybersecurity testbed for power distribution grids needs to model the physical power grid and the communication network. In our blueprint, we propose to realize these components separately and introduce a dedicated coordinator that mediates between the individual simulations to ensure realistic mutual interactions (cf. Fig. 1).

*Both authors contributed equally to this work.

CCS '20, November 9–13, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-7089-9/20/11.
https://doi.org/10.1145/3372297.3420016

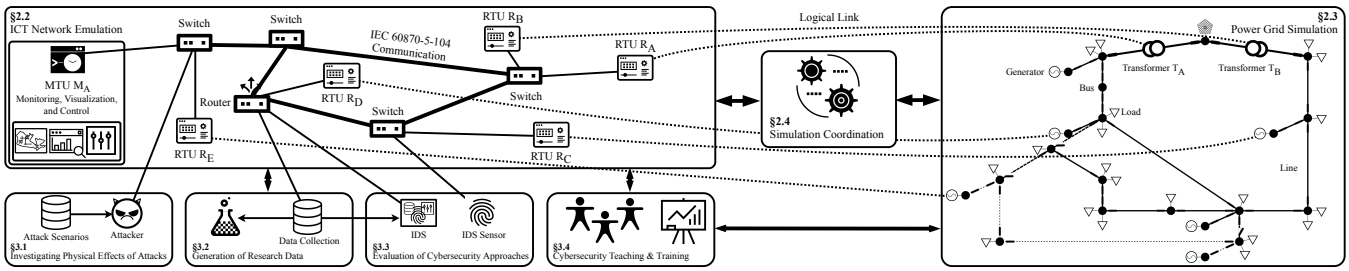

Figure 1: Overview on our proposed architecture blueprint at the example of a CIGRE power network [9] and an excerpt of the corresponding communication network. We indicate logical mappings between the communication network hosts and the power grid components exemplarily, e.g, RTU R_A controls and monitors transformer T_A in the power grid.

2.1 Power Grid and Network Topologies

To authentically replicate power distribution grids, we require information on both, the topology of the physical power grid (properties and interconnections of devices such as lines, transformers, or loads) and the communication network used to interconnect these physical assets (information on hosts such as Remote and Master Terminal Units (RTUs / MTUs)[1], and infrastructure such as routers and switches along with their configurations). While realistic information on power grid topology models is publicly available [10], models for corresponding communication networks and their configuration are missing [5]. Consequently, our blueprint relies on a smart grid architecture model-based approach [5] to automatically derive a communication network topology and its configuration from a power grid model. The resulting topologies, as well as linking information, enable us to derive a concurrent simulation environment for cybersecurity research and training.

2.2 Communication Network Emulation

To allow for the execution of real network applications as required by various research and training tasks, we propose to rely on communication network *emulation* instead of the *simulation* approach taken by most related work (cf. §1). More precisely, we propose to use Mininet [6] to represent and interconnect network components such as RTUs and MTUs (communicating over IEC 60870-5-104), network switches and routers, and hosts providing additional cybersecurity functionality, e.g, IDSs, as illustrated in Figure 1. Mininet enables flexible configuration of network parameters, covering link latencies, jitter, bandwidth, interface properties as well as flow rules and routing tables, while further providing support for software-defined networking. Due to the low-level representation of the network, i.e, down to individual interfaces, we can achieve a high degree of realism and execute real networking applications.

2.3 Power Distribution Grid Simulation

In contrast to the communication network emulation which operates in real-time, power distribution grid simulation only has to be performed upon switching operations, changes in power consumption or generation which can be modeled by time series data, or other well-defined external events. Consequently, we propose to use power flow calculations based on the current topology configuration using pandapower [10] to simulate the power distribution grid. As shown in Figure 1, a simulated power grid consists of a connection to an external grid, buses, lines with varying properties, transformers, switches, circuit breakers, loads and generators, which can be combined for more complex models.

[1]MTUs receive monitoring information from RTUs and issue control commands to supervise the grid's state and behavior, i.e, monitor and manage the grid.

2.4 Coupling of Network and Grid Simulation

Although network emulation and power grid simulation can operate independently in theory, they depend on information from each other. E.g., MTU M_A in Figure 1 might issue a command to RTU R_A to change the behavior of the associated transformer T_A, thus requiring that the network emulation can write and read parameters of the simulated power grid. To achieve an actual mapping and mediation between both simulators, our blueprint relies on simulation coordination (cf. Figure 1) to provide the current power grid state and measurements to the respective communication network components, ensure that control commands are implemented by the power simulation, and trigger the power flow computation.

2.5 Assessing Feasibility and Scalability

To assess the feasibility and scalability of a cybersecurity testbed for power grids, we present preliminary performance results.

We measure the memory consumption when deploying the full *communication network* for the CIGRE [9] MV grid (25 hosts, 22 switches, 46 links) with prototype implementations of its components. Our preliminary results show that an RTU requires less than 65 MiB RAM and the whole network requires less than 1.4 GiB. Representing the MV Oberrhein [10] as a larger and more realistic network (181 hosts, 179 switches, 361 links) requires less than 8 GiB RAM, which is feasible even for current desktop systems.

Considering the simulation of the *power grid*, we investigate the time required for power flow computation. For the CIGRE MV grid (cf. Fig. 1) with 15 lines and 59 components this requires on average 7.4 ms. MV Oberrhein, as a realistic and considerably larger grid with 181 lines and 1588 components, shows an average runtime of 13.2 ms, indicating the general feasibility of our proposed approach.

3 REALIZING SECURITY FUNCTIONALITY

Our blueprint for simulating power distribution grids is designed to support various use cases in cybersecurity research and training.

3.1 Investigating Physical Effects of Attacks

The interplay of communication network and physical world is a special property of CPSs, drastically increasing the potential consequences of cyberattacks [4]. Our proposed cybersecurity testbed enables the flexible investigation of potentially unpredictable physical effects. We support conducting a variety of attacks (targeting both, communication network and grid components) against the simulated environment to observe the behavior of affected components. Due to the detailed modeling of the communication network, including individual interfaces and links as well as switch and host behavior, various attack scenarios can be reproduced and evaluated. Ultimately, this provides the potential to reliably assess the likelihood, required effort, and severity of cyberattacks against power grids, paving the way for developing advanced security measures.

3.2 Generation of Research Data

Sophisticated cybersecurity approaches such as semantic or process-aware IDSs [13] require extensive datasets of benign and malicious behavior, e.g., to train and validate machine learning models. Uniquely for CPSs such as power grids, these datasets need to cover both, network traffic and the corresponding physical state. Our testbed can cost-efficiently provide such data based on automated time-series information and execution of attacks (cf. §3.1). Thus, extensive data on the physical grid state and network traffic can be collected with the help of virtual interfaces and SPAN ports provided by each switch. Likewise, after each simulation step, the physical state of the power grid can be exported, both as is (ground truth) and as received by the MTU (subject to noise and potential modification attacks). From a different angle, our testbed also facilitates the creation of realistic honeypots which model a complex CPS, thus allowing for the collection of authentic attack data.

3.3 Evaluation of Cybersecurity Approaches

Qualitative evaluation of cybersecurity approaches requires deploying them in grids of varying complexity and size. Besides sole deployment, our blueprint allows to evaluate the efficiency, i.e, the rate of anomaly detection and false alarms, as well as potential undesired effects on the actual communication and grid infrastructures. Allowing for fine-tuned attacks (cf. §3.1) as well as flexible deployment of security approaches, e.g., IDSs such as Snort or Zeek, further aids in deployment optimization, e.g. IDS sensor placement. Respective pipelines, e.g., based on the Elastic stack, enable producing new, replicable, and publishable research data (cf. §3.2), as well as easing data visualization for evaluating the effects and efficiency of security concepts, and assisting in cybersecurity training.

3.4 Cybersecurity Teaching & Training

Given the growing threat of cyberattacks, keeping personnel trained and ready to respond to security incidents is of paramount importance. Due to deviants in operators' setups, predefined training procedures are insufficient, while practicing in live infrastructure is unreasonable. Our blueprint allows such training by deploying operator-specific security infrastructure along with generic security tools to provide a realistic and familiar environment. Further, precise orchestration and coordination of cyberattacks within the training environment is possible by deploying dedicated attack hosts and modeling both, historic and potential future break-in scenarios, that entail varying levels of infrastructure access. Hence, personnel can test and train appropriate handling in case of such attacks in a dedicated environment. Other potential uses of our blueprint include cybersecurity teaching for computer science and electrical engineering students, or hosting capture-the-flag competitions as gamified security training [1]. Hybrid operation covering real-world components promises valuable insights as well.

4 SUMMARY AND NEXT STEPS

As a foundation to mitigate cybersecurity threats in power distribution grids, we presented a blueprint for a cybersecurity research and training testbed that allows to couple real network applications with a simulated power grid. Such a testbed enables various use cases in cybersecurity research and training, e.g., evaluation of the physical impact of cyberattacks, generation of datasets for training machine learning models, and testing of cybersecurity approaches.

Currently, we are working on fully implementing our blueprint in Python based on Mininet as network emulator and pandapower as power flow solver. Thereby, we strive to realistically mimic a European power distribution grid and its communication infrastructure using the MV Oberrhein grid topology and IEC 60870-5-104 as communication protocol. Besides realizing the actual testbed, we are implementing various use cases, ranging from advanced multi-staged cyberattacks, an IDS (based on Snort, ElasticSearch, and Kibana), as well as a fully-fledged training environment for technical personnel. In addition to performing synthetic performance benchmarks, we plan to validate our testbed against a medium/low voltage distribution grid with multiple distribution substations operated within a research laboratory at RWTH Aachen University.

Acknowledgments. This work has received funding from the German Federal Ministry for Economic Affairs and Energy (BMWi) under project funding reference 0350028 (MEDIT).

REFERENCES

[1] Daniele Antonioli et al. 2017. Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3. In *ACM CPS-SPC 2017*.
[2] Daniele Antonioli and Nils Ole Tippenhauer. 2015. MiniCPS: A Toolkit for Security Research on CPS Networks. In *ACM CPS-SPC*.
[3] Christopher Hannon et al. 2016. DSSnet: A Smart Grid Modeling Platform Combining Electrical Power Distribution System Simulation and Software Defined Networking Emulation. In *ACM SIGSIM-PADS*.
[4] Mark James et al. 2019. Improving the Cyber Security of the Electric Distribution Grid – Identifying Obstacles and Presenting Best Practices for Enhanced Grid Security. Institute for Energy and the Environment, Vermont Law School.
[5] Benedikt Klaer et al. 2020. Graph-based Model of Smart Grid Architectures. In *IEEE SEST*.
[6] Bob Lantz et al. 2010. A network in a laptop: rapid prototyping for software-defined networks. In *ACM HotNets*.
[7] Kevin Mets et al. 2014. Combining power and communication network simulation for cost-effective smart grid analysis. *IEEE Commun. Surveys Tuts.* 16, 3.
[8] Cornelius Steinbrink et al. 2019. CPES Testing with mosaik: Co-Simulation Planning, Execution and Analysis. *Applied Sciences* 9, 5.
[9] Kai Strunz et al. 2009. Benchmark systems for network integration of renewable and distributed energy resources. *Cigre Task Force C* 6, 04-02, 78.
[10] Leon Thurner et al. 2018. pandapower – An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems. *IEEE Trans. Power Syst.* 33, 6.
[11] Dennis van der Velde et al. 2020. Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures. In *IEEE ENERGYCon*.
[12] Mike Vogt et al. 2018. A survey and statistical analysis of smart grid co-simulations. *Applied Energy* 222.
[13] Konrad Wolsing et al. 2020. Poster: Facilitating Protocol-independent Industrial Intrusion Detection Systems. In *ACM CCS*.