PowerDuck: A GOOSE Data Set of Cyberattacks in Substations

Sven Zemanek
sven.zemanek@fkie.fraunhofer.de
Fraunhofer FKIE

Immanuel Hacker
i.hacker@iaew.rwth-aachen.de
RWTH Aachen University
Fraunhofer FIT

Konrad Wolsing
konrad.wolsing@fkie.fraunhofer.de
Fraunhofer FKIE
RWTH Aachen University

Eric Wagner
eric.wagner@fkie.fraunhofer.de
Fraunhofer FKIE
RWTH Aachen University

Martin Henze
henze@cs.rwth-aachen.de
RWTH Aachen University
Fraunhofer FKIE

Martin Serror
martin.serror@fkie.fraunhofer.de
Fraunhofer FKIE

ABSTRACT

Power grids worldwide are increasingly victims of cyberattacks, where attackers can cause immense damage to critical infrastructure. The growing digitalization and networking in power grids combined with insufficient protection against cyberattacks further exacerbate this trend. Hence, security engineers and researchers must counter these new risks by continuously improving security measures. Data sets of real network traffic during cyberattacks play a decisive role in analyzing and understanding such attacks. Therefore, this paper presents *PowerDuck*, a publicly available security data set containing network traces of GOOSE communication in a physical substation testbed. The data set includes recordings of various scenarios with and without the presence of attacks. Furthermore, all network packets originating from the attacker are clearly labeled to facilitate their identification. We thus envision *PowerDuck* improving and complementing existing data sets of substations, which are often generated synthetically, thus enhancing the security of power grids.

CCS CONCEPTS

• **Security and privacy** → *Intrusion detection systems*; **Denial-of-service attacks**; • **Networks** → *Cyber-physical networks*; • **General and reference** → **Measurement**.

KEYWORDS

data sets, network traffic, smart grid security, IDS

1 INTRODUCTION

The increasing digitalization of power grids holds many opportunities, particularly for shifting from a centralized energy production

based on conventional energy sources to a more decentralized production using renewable energies [4]. However, this evolution also amplifies the risks of cyberattacks since initially air-gapped systems become connected to one another and, in some cases, even to the Internet without implementing sufficient security measures [10]. Unfortunately, severe consequences have already manifested in the past in various incidents, such as Stuxnet [5] or the attacks on the Ukrainian power grid [13]. Hence, academia and industry need to intensify their research in cybersecurity for power grids to effectively improve existing and enable the development of new sophisticated security measures for power grids.

An essential prerequisite for the respective security research is accurate data about the underlying processes, e.g., communication traffic and state information. Nevertheless, such data is often unavailable to researchers due to security concerns of power grid operators and the high availability requirement of such systems. Instead, research often relies on artificially generated or simulated data (e.g., [2, 7, 9]), subject to abstractions and simplifications. Meanwhile, a better approach for getting realistic data is performing measurements in a physical testbed with real hardware.

Related Work. There are already several publicly available data sets recorded in different testbeds and scenarios in the industrial automation domain with an enormous impact on security research. Examples of such data sets include recordings in the Secure Water Treatment (SWaT) testbed [3] and the HIL-based augmented ICS security (HAI) data sets [12]. Possible use cases for these data sets include, for example, the evaluation and enhancement of anomaly detection approaches, such as [6]. Unfortunately, there is a lack of corresponding real-world security data sets for power grids, and, therefore, researchers often use synthetically generated data to evaluate their approaches (e.g., [8]). However, such data is often subject to abstractions and simplifications due to the complex physical processes of power grids and thus has limited use for security research. Recently, the authors of [1] published a data set recorded in the Electric Power and Intelligent Control (EPIC) testbed containing network and process data. Nevertheless, the considered attack scenarios are limited to malicious reconfigurations of the devices present in the testbed and their impact. The scenarios in the data set also do not include actual executions of the considered attacks. Instead, a recommendation is to mutate the collected data, e.g., for anomaly detection, which is again of limited use.

Contributions. Therefore, this paper presents *PowerDuck*[1], a publicly available data set for cybersecurity research of power grids. We recorded the data in a real-world testbed representing the secondary technology of a substation in the high and extra-high voltage grid. The setup consists of three Intelligent Electronic Devices (IEDs), a station control system, and the surrounding networking infrastructure. Moreover, the IEDs also implement a curative measure similar to a busbar protection to represent cascading effects. In this setting, we recorded the IEC 61850 GOOSE data traffic in different normal operation and attack scenarios with varying parametrizations. Additionally, we convert our data set to and label malicious packets in the Industrial Protocol Abstraction Layer (IPAL) format [14] to facilitate their identification and analysis. The resulting data set thus offers a broad range of possibilities for cybersecurity research and is particularly suited for testing Intrusion Detection Systems (IDSs) in power grids.

The structure of this paper is as follows. Section 2 thoroughly describes the real-world testbed we used for the data recordings and the considered operation scenarios. Then, we provide details on the recorded data in Section 3. We discuss possible use cases of *PowerDuck* in Section 4 and conclude this paper in Section 5.

2 CONSIDERED SETUP

In this section, we detail the considered setup for recording *Power-Duck*. We begin with a comprehensive description of the substation testbed in Section 2.1. Then, we present the different scenarios of our measurement campaign in Section 2.2.

2.1 Testbed

The testbed represents the secondary technology of a substation in the high and extra-high voltage grid, where the setup is sufficiently complex to simulate advanced cyberattacks while still remaining readily understandable. In the following, we describe the physical structure of the testbed as well as the implemented IED application.

Structure. Figure 1 depicts our substation testbed. It consists of a station control system connected to three IEDs. The communication between the IEDs and the station control system occurs in the same network, which thus replicates the station network of a substation. To keep the setup manageable, we designed it as a single switch without redundancy systems. Furthermore, a separate network connects the substation control system with the control room. The system's scalability is mainly defined by the number of hardware devices and the time to set up the configuration. In contrast to a fully simulated environment, automatic reconfiguration of the testbed is impossible. However, it would be possible to extend the testbed by a simulation.

The communication between IEDs and the substation control system uses the IEC 61850 GOOSE protocol and flows through a central switch. Since an integral part of the *PowerDuck* data set consists of traffic recordings, we use the switch's SPAN port to capture all GOOSE packets passing through the switch. Moreover, as a realistic attack vector in power grids [4], we assume that an attacker controls a device (i.e., a PC) connected to that switch.

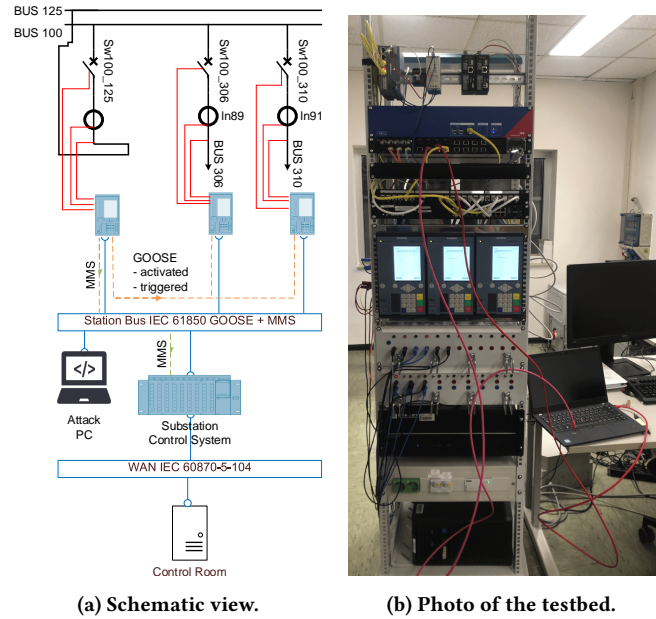(a) Schematic view.

(b) Photo of the testbed.

Figure 1: Overview of our substation testbed. The setup consists of a station control system and three IEDs connected through a station bus. Moreover, an attack PC is attached to the station bus, thus with direct access to the local network.

For the considered measurement scenarios, we connected a voltage measurement of the public power grid to the three IEDs and implemented a circuit breaker emulation. This circuit breaker emulation is thus implemented with the help of the I/Os on the IEDs and enables a realistic emulation of the switching process, including correct time delays. Through this setup, we can verify the effects on the corresponding real-world assets and thus the impact of our attacks. Mainly, we can observe the opening of circuit breakers when they should not open or vice-versa, and that protection mechanisms, which should open the circuit breakers in case of a fault, do not work. A result of such attacks could be a partial blackout and even have a more severe impact when executed as a coordinated attack. Moreover, malfunctioning protection mechanisms may damage equipment and thus lead to prolonged outages.

IED Application. The IEDs use the IEC 61850 GOOSE protocol to transmit their measurements to the substation control system. Additionally, the IEDs host an application similar to a busbar protection and implement a curative measure. This application ensures that when the circuit breaker of the first IED is opened, the circuit breakers of the other IEDs are also opened to prevent further damage. We implemented this behavior using two GOOSE signals, one indicating the activation of the curative measure and the other indicating the current state of the circuit breaker. Hence, triggering the curative measure would require both signals, an activation and an open circuit breaker.

We defined different measurement scenarios based on this setup to cover distinct testbed behavior under normal and attack conditions. In the following, we briefly describe these scenarios.
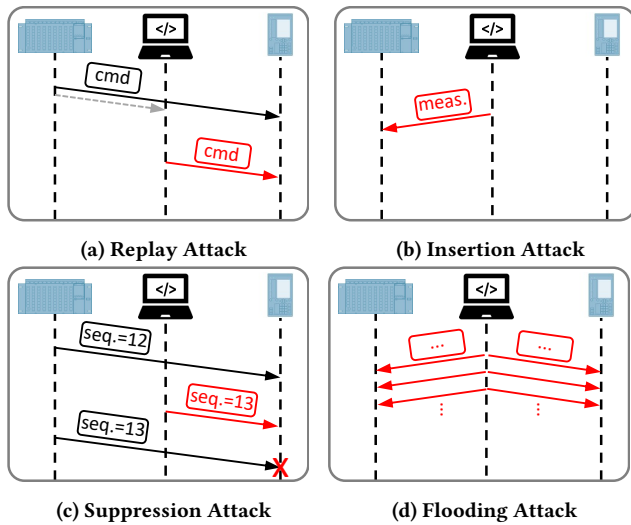
(a) Replay Attack

(b) Insertion Attack

(c) Suppression Attack

(d) Flooding Attack

Figure 2: Examples for the distinct attacks, including a station control system (left), an attack PC (middle), and an IED.

2.2 Scenarios

The *PowerDuck* data set includes traffic captures from normal operation scenarios as well as different attack scenarios with varying configurations. The selected attacks represent typical communication attacks targeting the IEC 61850 GOOSE protocol [2] and are thus independent of the used hardware. As such, they are particularly suited for the *Exploitation* and *Act on Objective* phases of the cyber kill chain model [15]. In the following, we provide a general overview of the considered scenarios for our measurement campaign. For a detailed description, including the specific parametrizations of the different scenarios, we refer to Table 1.

Normal Operation. The testbed operates normally without any attacks, i.e., the substation control system successfully performs different switching operations. The recorded traffic from the corresponding four measurement scenarios thus serves as a reference for the normal operation of the involved systems.

Replay Attack. The attacker eavesdrops on one or more regularly exchanged GOOSE packets to replay them later. Such packets could include, e.g., a switching command or an outdated measurement and thus lead to wrong switching operations. For this attack, we recorded data from three distinct measurement scenarios. Fig. 2a depicts an example of this attack.

Insertion Attack. As shown in Fig. 2b, the attacker sends a specially crafted packet to disturb switching operations. Such a packet could include, e.g., a wrongly announced switch opening or forged measurements, leading to six different scenarios. For all insertion scenarios, repetition packets were sent in the temporal pattern according to the GOOSE specification.

Suppression Attack. The attacker exploits GOOSE sequence numbers to manipulate the protocol states of the involved systems, e.g., by sending crafted packets with increasing sequence numbers. Then, legitimate packets are discarded, which leads to a *denial of service*, as illustrated in Fig. 2c. We recorded data from five different scenarios. For all suppression scenarios, repetition packets were sent in the temporal pattern according to the GOOSE specification.

Flooding Attack. The attacker quickly sends many (large) packets to overburden the communication network, which might lead to packet drops of legitimate requests and hence to a *denial of service*. We depict the general flooding scenario in Fig. 2d and further recorded two distinct variations of the attack.

With the present description of the testbed setup and the measurement scenarios, we continue with the details of the recording process and the resulting data structure in the following section.

3 PROPERTIES OF THE DATA SET

This section details how we executed our measurement campaign for *PowerDuck* in our real-world testbed using the defined scenarios in Section 3.1. Furthermore, we describe the structure of the *PowerDuck* data set in Section 3.2.

3.1 Data Collection

To capture the relevant network traffic for the different scenarios, we used the SPAN port of the central switch that connects the different entities of our testbed, i.e., the attack PC, the substation control system, and the IEDs. Moreover, we recorded the outgoing network traffic on the attack PC to unequivocally label data packets originating from the attack PC in the *PowerDuck* data set.

We conducted the individual measurements according to their description in Table 1. For each of the 20 scenarios, we performed the following general steps, where the exact actions depend on the respective parameters and whether it includes an attack or not:

(1) reset the circuit breakers and the substation control system;
(2) start the recording of data traffic;
(3) possibly start an attack;
(4) possibly perform one or more actions, e.g., open a circuit breaker; and
(5) stop the recording of data traffic.

The measurement duration varied between 5 and 18 minutes, depending on the scenario. We provide the exact durations in Table 1. Moreover, we slightly varied the timing of the different steps to obtain individual traffic patterns, not depending on a fixed timing.

Upon completing the recording of the data traffic, we performed the following postprocessing steps on the captured network traffic: We removed all packets from the recordings that do not belong to the IEC 61850 GOOSE protocol. Furthermore, we identified all packets originating from the attack PC with the help of the attack PC's recordings and described their purpose. Notably, we distinguished between proper actions and packets that simply repeat previous values according to the IEC 61850 GOOSE specification.

Besides providing the raw packet captures in the PCAP format, we also transcribed them into the IPAL format [14], facilitating further analysis and labeling of attack packets. IPAL provides an abstract representation of the recorded network packets using the JSON format. This representation enables a protocol-independent classification of the different packet types and the annotation those packets that originated from the attacker.

As an example, we visualized in Fig. 3 an insertion attack (no. 6) and a suppression attack (no. 10), as observed in the *PowerDuck* data set. The plots show when and how the attacker overwrites the actual process states in the distinct scenarios. In the following section, we provide further details on the structure of our data set.

No.	ID	Attack	Duration	Description
1	normal-1	–	00:14:14	Open IED 1's circuit breaker, then close everything again.
2	normal-2	–	00:18:26	Open IED x's circuit breaker, then close everything again; for x in {1,2}.
3	normal-3	–	00:12:38	Open IED x's circuit breaker, then close everything again; for x in {3,2,3}
4	normal-4	–	00:16:53	Open IED x's circuit breaker, then close everything again; for x in {2,1,3,1}
1	replay-opening-switch-isolated	*Replay*	00:05:35	Replay two packets that indicate an opening of IED 1's circuit breaker which have been recorded previously.
2	replay-opening-switch-w-context	*Replay*	00:05:36	Replay two packets that indicate an opening IED 1's circuit breaker and their value repetitions which have been recorded previously.
3	replay-old-measurements	*Replay*	00:05:20	Replay previously recorded measurements of IED 1.
4	insert-fake-open-w-intermediate	*Insertion*	00:05:07	Insert crafted packets (values: opening – open) that indicate an opening of IED 1's circuit breaker.
5	insert-fake-open-only-end	*Insertion*	00:05:24	Insert a crafted packet that indicates an open state of IED 1's circuit breaker.
6	insert-distort-meas-up-grad	*Insertion*	00:10:09	Insert crafted packets that indicate measurements of IED 1 raising from 399.45 to 419.91 over 186 seconds.
7	insert-distort-meas-down-grad	*Insertion*	00:10:25	Insert crafted packets that indicate measurements of IED 1 falling from 399.45 to 380.09 over 176 seconds.
8	insert-distort-meas-up-sharp	*Insertion*	00:11:20	Insert a crafted packet that indicates a measurement of IED 1 of 420.0.
9	insert-distort-meas-down-sharp	*Insertion*	00:11:32	Insert a crafted packet that indicates a measurement of IED 1 of 380.0.
10	sup-1-1-tbv0	*Suppression*	00:10:18	Insert two crafted packets (no delay) with a *stNum* value incremented by 1 and 2, respectively, while they still indicate a closed circuit breaker of IED 1.
11	sup-1-1-tbv1	*Suppression*	00:10:24	Same as sup-1-1-tbv0, but with 1s delay between the two packets.
12	sup-1-1-tbv2	*Suppression*	00:12:11	Same as sup-1-1-tbv0, but with 2s delay between the two packets.
13	sup-2	*Suppression*	00:11:29	Insert a crafted packet that has a *stNum* value incremented by 2, while its value still indicates a closed circuit breaker of IED 1.
14	sup-1	*Suppression*	00:11:44	Insert a crafted packet that has a *stNum* value incremented by 1, while its value still indicates a closed circuit breaker of IED 1.
15	flood-repeat	*Flooding*	00:10:34	Pick an observed packet announcing the state of IED 1 and send it repeatedly in quick succession.
16	flood-bloat-repeat	*Flooding*	00:11:33	Same as flood-repeat, but the size of the packet that is being flooded has been increased artificially to about the size of the MTU.

Table 1: Description of the measured scenarios in *PowerDuck*. For each scenario, the table includes a unique ID to simplify the retrieval of the corresponding data in *PowerDuck* and the respective duration (hh:mm:ss) of the measurement.

3.2 Data Set Structure

The *PowerDuck* data set contains the recordings of the 20 previously defined measurement scenarios (Section 2.2). The data is divided into the plain packet capture files in the `raw` folder and the IPAL transcriptions of those packet captures in the `ipal` folder. The files in those folders are again subdivided into four files in the `normal` subfolder, containing regular traffic, and 16 files in the `attack` subfolder, containing the traffic of the attack scenarios.

In the IPAL transcriptions, packets from regular traffic have their `malicious` value set to `false`. In contrast, packets originating from the attacker have it set to a string indicating the attack ID given in Table 1. This categorization is based on the JSON files in the `malicious` folder, which indicate and describe the attack packets. Consequently, such a description does not exist for the normal traffic scenarios, which do not include any attacks. The files in the `malicious` folder can be used to identify the attack packets in the packet capture files manually: The `ipalid` value describes the (0-based[2]) index of the corresponding packet in the packet capture file. All files in the data set are named according to the scheme `No-ID-file extension`, where `No` and `ID` correspond to those in

Table 1, e.g., `01-normal-1.pcapng` for the raw packets captures for the first normal operation scenario.

4 APPLICATIONS AND USE CASES

After presenting the properties of the *PowerDuck* data set in the previous section, this section briefly highlights potential applications and use cases of *PowerDuck* for security researchers and engineers. We thus identify and discuss the following application areas.

Security Analyses. An essential use of *PowerDuck* is to better understand existing attacks on the IEC 61850 GOOSE protocol in the context of power grids and helps to assess potential vulnerabilities. Such analyses include the concrete manifestation of the attacks on real systems and their possible impact on the network traffic.

(Synthetic) Traffic Generation. Since some use cases require larger amounts of network traffic than provided by *PowerDuck*, a viable approach is to use these real-world recorded traffic patterns to significantly improve synthetic traffic generation, such as proposed in [11]. Moreover, this approach enables modifications and variations of normal and attack traffic as needed to better fit the requirements of the target use case.

---

[2] Wireshark displays packet numbers with a 1-based index, e.g., locate the packet with `ipalid` 200, one has to look for the packet Wireshark displays as No. 201.

(a) Effects of an insertion attack (no. 6) as observed in the *PowerDuck* data set.

(b) Effects of a suppression attack (no. 10) as observed in the *PowerDuck* data set.
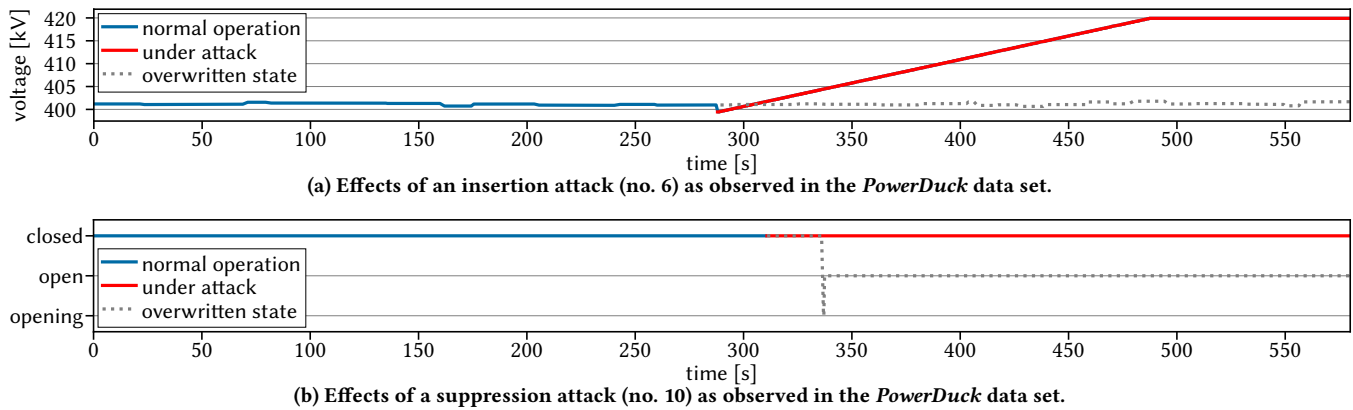
Figure 3: Visualization of two example attacks from the *PowerDuck* data set (insertion attack no. 6 and suppression attack no. 10). The plots show the manipulated information along with the actual overwritten states.

Intrusion Detection Systems. PowerDuck offers a solid foundation for the training and testing of IDSs for power grids since the data set also includes labeled packets originating from an attacker. In particular, the recorded network traffic can be adapted and scaled to match the needed requirements in combination with an improved synthetic traffic generation.

To summarize, *PowerDuck* offers a solid foundation to address security analyses and implementations in the context of power grids, particularly considering the control in substations via the IEC 61850 GOOSE protocol. This real-world data set thus nicely complements and improves existing power grid data sets based on synthetically generated traffic. Moreover, the considered scenarios include not only the simple transmission of commands but also the (physical) reactions to such controls in an IED application, which might trigger further actions and thus influence the network traffic.

5 CONCLUSION

This paper presents *PowerDuck*, a publicly available security data set of IEC 61850 GOOSE network traffic in a substation testbed, consisting of a station control system, three IEDs, and an attack PC. We defined different scenarios, with and without the presence of attacks, to cover a broad behavior of our physical testbed. Furthermore, the IEDs implement a curative measure, similar to a busbar protection, which enables the triggering of cascading effects. The resulting data set thus contains the GOOSE network traffic of different scenarios. Additionally, it includes a transcription to the IPAL format, which facilitates a protocol-independent analysis and allows us to label the packets originating from the attacker.

Concerning its use cases, *PowerDuck* contributes to a deeper understanding of current attacks on substations through the IEC 61850 GOOSE protocol. More importantly, it offers a solid foundation to complement and improve the synthetic generation of IEC 61850 GOOSE network traffic, as the measurements in *PowerDuck* contain actual attacks in a real-world setup. Hence, it opens up new possibilities for modifying and scaling data sets to individual requirements, such as the training and testing of IDSs in power grids.

ACKNOWLEDGMENTS

REFERENCES

[1] Chuadhry Mujeeb Ahmed and Nandha Kumar Kandasamy. 2021. A Comprehensive Dataset from a Smart Grid Testbed for Machine Learning Based CPS Security Research. In *CPS4CIP*. Springer Int'l Pub., Cham.

[2] Partha P. Biswas, Heng Chuan Tan, Qingbo Zhu, et al. 2019. A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation. In *IEEE SmartGridComm*.

[3] Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. 2017. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In *Critical Information Infrastructures Security*. Springer Int'l Pub., Cham.

[4] Tim Krause, Raphael Ernst, Benedikt Klaer, et al. 2021. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* 21, 18 (2021).

[5] Ralph Langner. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy* 9, 3 (2011).

[6] Dan Li, Dacheng Chen, Baihong Jin, et al. 2019. MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks. In *International Conference on Artificial Neural Networks*. Springer, Cham.

[7] Chih-Yuan Lin, August Fundin, Erik Westring, et al. 2021. RICSel21 Data Collection: Attacks in a Virtual Power Network. In *IEEE SmartGridComm*.

[8] Ramin Moghaddass and Jianhui Wang. 2018. A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data. *IEEE Transactions on Smart Grid* 9, 6 (2018).

[9] Ángel Luis Perales Gómez, Lorenzo Fernández Maimó, Alberto Huertas Celdrán, et al. 2019. On the Generation of Anomaly Detection Datasets in Industrial Control Systems. *IEEE Access* 7 (2019).

[10] Martin Serror, Sacha Hack, Martin Henze, Marko Schuba, and Klaus Wehrle. 2021. Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 17, 5 (2021).

[11] Mustafizur R. Shahid, Gregory Blanc, Houda Jmila, et al. 2020. Generative Deep Learning for Internet of Things Network Traffic Generation. In *IEEE Pacific Rim International Symposium on Dependable Computing*.

[12] Hyeok-Ki Shin, Woomyo Lee, Jeong-Han Yun, and HyoungChun Kim. 2020. HAI 1.0: HIL-based Augmented ICS Security Dataset. In *USENIX Workshop on Cyber Security Experimentation and Test (CSET '20)*.

[13] David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. 2017. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. In *IEEE Conference for Protective Relay Engineers*.

[14] Konrad Wolsing, Eric Wagner, Antoine Saillard, and Martin Henze. 2022. IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID '22)*.

[15] Tarun Yadav and Arvind Mallari Rao. 2015. Technical Aspects of Cyber Kill Chain. In *Security in Computing and Communications*. Springer Int'l Pub., Cham.