international journal of critical infrastructure protection 53 (2026) 100845

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

PowerRange: An immersive cyber range for power grid operators

Lennart Bader [a,b,*], Eric Wagner [c,a], Martin Serror [a]

[a] Cyber Analysis & Defense, Fraunhofer FKIE, Fraunhoferstraße 20, Wachtberg, 53343, NRW, Germany
[b] Security and Privacy in Industrial Cooperation, RWTH Aachen University, Im Süsterfeld 9, Aachen, 52072, NRW, Germany
[c] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 29 Av. John F. Kennedy, Luxembourg

ARTICLE INFO

Keywords:
CPS security
Power grids
Cyber range
Cybersecurity training
Co-simulation
Critical infrastructure security

ABSTRACT

Power grids are increasingly targeted by cyberattacks that can disrupt operations and even cause large-scale blackouts. As these critical cyber–physical systems become more digitized and reliant on communication technologies, their attack surface increases, making cybersecurity a growing concern. While technical and organizational measures are essential, their effectiveness is limited without addressing the human factor. Practical, user-centered training is thus crucial to ensure the correct implementation and usability of security measures. However, suitable training environments for power systems remain scarce. This paper introduces PowerRange, an advanced cyber range specifically designed for power grid operators. PowerRange extends a state-of-the-art power grid co-simulator with various user interaction capabilities, including hardware-in-the-loop integration and modern control room software. It supports flexible, automated configuration of realistic scenarios, enabling immersive, hands-on cybersecurity training for key stakeholders, including management, control room staff, and IT/OT personnel. Preliminary pilot training sessions indicate that, beyond improving technical skills, PowerRange promotes cross-functional collaboration and strengthens incident response capabilities.

1. Introduction

Power grids are complex networks encompassing the generation, transmission, and distribution of electrical power, designed to provide a stable and continuous electricity supply to homes, businesses, and industries. As critical Cyber-Physical Systems (CPSs), they are attractive targets for cyberattacks driven by financial gain, political agendas, or even personal vendettas [1–4]. Moreover, with the ongoing transition toward highly automated and distributed smart grids, they become more digitized and integrated with advanced Information and Communications Technology (ICT), leading to increased vulnerabilities and larger attack surfaces [5]. Cyberattacks on power grids range from simple physical tampering to more sophisticated communication-based attacks and stealthy false data injections, all capable of significantly disrupting operations. Notably, the repeated cyberattacks on the Ukrainian power grid are a stark reminder that such attacks can even lead to widespread blackouts [6].

Grid operators thus face the challenge of ensuring the safety and availability of power grids, including protection against cyberattacks. Addressing this challenge requires a comprehensive security strategy combining technical measures, such as firewalls, and organizational procedures, such as regularly updated security policies, to address evolving threats. However, even the most sophisticated security strategy does not suffice if the human factors are overlooked [7]. Consequently, grid operators must prioritize regular security training for their personnel, focusing on the *practical application* of security measures and procedures.

While a wide range of methods for cybersecurity trainings is available, determining which methods are most effective remains an open area of research [8]. However, there is a consensus that awareness campaigns relying on static learning materials, such as posters and brochures, have a minimal impact on promoting security-compliant behavior [9]. More effective approaches involve comprehensive training sessions addressing distinct roles, requirements and learning objectives [10]. Furthermore, participants should be actively engaged through practical exercises or game-based approaches. Such training activities are most effective when conducted in realistic environments, as this enhances the transfer of acquired skills to daily work routines [11].

Nevertheless, developing effective cybersecurity training for industrial CPSs, such as power grids, presents several challenges [12,13]. First, the training must include hands-on, practical activities to ensure participants are well-prepared for real-world cybersecurity incidents.

* Corresponding author at: Cyber Analysis & Defense, Fraunhofer FKIE, Fraunhoferstraße 20, Wachtberg, 53343, NRW, Germany.
E-mail addresses: lennart.bader@fkie.fraunhofer.de (L. Bader), eric.wagner@uni.lu (E. Wagner), martin.serror@fkie.fraunhofer.de (M. Serror).

https://doi.org/10.1016/j.ijcip.2026.100845
Received 21 October 2025; Received in revised form 9 January 2026; Accepted 28 February 2026
Available online 3 March 2026

Second, it should support a team-based approach, as responding to cyberattacks typically involves multiple actors within a grid operator, which requires collaboration, communication, and consolidating expertise during critical situations. Third, the training should closely mirror real-world scenarios within a realistic environment to maximize engagement and ensure the transferability of learned procedures. However, there is a shortage of realistic and safe training environments for power grids that enable such comprehensive trainings [14].

To address this gap, we introduce PowerRange, an advanced cyber range for power grid operators, based on the open-source research testbed Wattson [15]. Wattson enables the safe execution of multi-stage cyberattacks and sophisticated countermeasures within configurable power grid scenarios and integrates Operational Technology (OT) and Information Technology (IT) networks with power generation and distribution processes as a real-time co-simulator for both, power grid and ICT systems. We extend Wattson into a realistic cyber range, enabling dynamic and immersive cybersecurity training tailored to the specific needs of power grid operators. As such, it supports the practical application of security measures and concepts, helps identify weaknesses in their usability, and ultimately ensures engagement across all organizational levels, from management and control room staff to IT and OT personnel. To gather preliminary feedback on PowerRange and the proposed training concept, we conducted two pilot training sessions. The results furthermore underscore the critical role of communication and coordination in improving preparedness against cyberattacks. Before delving into PowerRange's design, we conduct a thorough related work analysis and derive the key design requirements.

In particular, we make the following novel *contributions*:

- We extend Wattson into a real-time cybersecurity training environment for power grid operators (Section 3).
- We introduce PowerOwl for flexible and automated scenario derivation, enabling rapid adaptation to various training requirements (Section 4).
- We develop an exemplary training concept covering offensive and defensive cybersecurity approaches for diverse use cases (Section 5).

2. Requirements and related work

Cyber ranges provide a realistic yet controlled environment for executing cyberattacks and evaluating cybersecurity measures [16]. A key advantage is their isolation from operational systems while still offering users a comparable and safe work environment [17]. Thereby, virtualization, either by emulation or simulation, is crucial in delivering realistic and scalable training scenarios at reasonable costs. Additionally, cyber ranges often incorporate physical elements to enhance realism and user immersion, making them a versatile tool for hands-on cybersecurity training. However, designing cyber ranges for CPSs, such as power grids, presents unique challenges.

In the following, we discuss the specific requirements for cyber ranges tailored to the power grid domain and subsequently review related work on cyber range approaches.

2.1. Identified requirements for cyber ranges targeting CPSs

To accurately represent CPSs, cyber ranges must not only model the ICT infrastructure but also faithfully emulate control centers, field devices, and the underlying physical processes [13,18]. Therefore, cyber ranges for CPSs should follow a modular and easily extensible architecture consisting of physical and virtual modules [17]. This complexity is further increased when accommodating the needs of diverse user groups, including IT security specialists, domain experts, and management. At the same time, cyber ranges must enable easily accessible exercises for both individual groups and collaborative scenarios, which are essential for effective cybersecurity training [12].

Table 1
Evaluation of related work with respect to the identified requirements, using a scoring system ranging from fully supported (++) to not supported (−−).

Approach	Realism	Flexibility	Scope
ThunderCloud [19]	−−	−−	−
CPSA [20,21]	+	−	+
EPIC [22]	++	−	+
GridAttackSim [23]	++	+	−
Wattson [15]	++	+	+

Although the various components of a cyber range can be modeled individually, either physically or virtually, an orchestration module is needed to ensure seamless integration and provide the required flexibility regarding learning objectives and exercise formats [13,17]. Furthermore, the ICT typically encompasses standard IT protocols and domain-specific OT protocols, such as IEC 61850 for power grids, necessitating tailored adaptations for the target domain.

Building on these established requirements for cyber ranges targeting CPSs, we identify key requirements specific to their use in immersive cybersecurity training. While tailored to the power grid domain, these requirements are also applicable to other critical CPSs. Accordingly, cyber ranges for immersive training of power grid operators must satisfy the following comprehensive requirements:

Realistic Training Environment. The cyber range must include virtual and physical components accurately representing the grid operator's infrastructure, including the power grid, ICT systems, control centers, and IT/OT devices. Such setups facilitate the transfer and testing of security concepts within safe and realistic training environments.

Flexible and Scalable Training Scenarios. The cyber range must support realistically scaled training scenarios regarding the power grid and network topologies as well as the executed cyberattacks. These scenarios should be easily adaptable to the operator's specific needs and interchangeable to prevent repetition. This flexibility enables the identification of weaknesses in the implementation of security concepts while adequately preparing participants to detect and mitigate real-world threats in evolving situations.

Comprehensive Scope of Training. The cyber range must support various training approaches, encompassing defensive and offensive strategies. Additionally, it should enable the participation of all key actors within a grid operator, including management, control room staff, and IT/OT personnel. This cross-disciplinary approach fosters collaboration and coordination during cyber incidents.

2.2. Related work analysis

In the following, we thus examine related work on cyber ranges for power grids and CPSs concerning the identified requirements. Table 1 provides a summary of this evaluation.

ThunderCloud [19] is a virtual smart grid testbed designed primarily for cybersecurity training for computer science students. It comprises virtual machines simulating both the attack machine and the corresponding victim machine, which typically represents an IT service or a SCADA device, depending on the specific exercise. These virtual machines are hosted on the participants' personal computers, allowing for individual execution of the exercises. While this approach facilitates practical exercises from both attacker and defender perspectives, it is nonetheless constrained by non-scalable and static scenarios for an individual participant.

Cyber–Physical Security Assessment (CPSA) [20,21] facilitates the co-simulation of a power grid and its corresponding ICT network. In addition to assessing the impact of cyberattacks on power grids, CPSA also targets educational and training purposes, such as conducting forensic analysis of log files. While the authors outline various educational and training objectives that CPSA can address, it is not designed to function

as a comprehensive cyber range for advanced and flexible training scenarios.

The physical testbed *Electrical Power and Intelligent Control (EPIC)* [22] emulates a small-scale smart grid, incorporating key power supply stages such as generation, transmission, micro-grid, and smart home. This setup facilitates research on attack scenarios, their impacts, and potential mitigation strategies, providing a realistic and controlled environment for experimentation and training. However, the testbed lacks flexibility, as it is confined to static, small-scale scenarios, which limits its applicability as a dynamic and adaptable training environment.

The co-simulator *GridAttackSim* [23] combines power grid and ICT simulation to support cybersecurity research and training. It offers a flexible platform for modeling smart grid scenarios, including grid operations, communication networks, applications, and attack simulations. While GridAttackSim provides a strong foundation for training, its effectiveness as a comprehensive cyber range remains uncertain, particularly in addressing power grid operators' distinct roles and responsibilities during cyber incidents.

Wattson [15] is a co-simulator for power grids that supports comprehensive cybersecurity research, such as evaluating the impacts of cyberattacks and possible countermeasures. Through network emulation, it allows conducting real-world cyberattacks while accurately modeling the interactions between power grid assets and their associated Intelligent Electronic Devices (IEDs), i.e., between the physical and the network domain. Although Wattson provides a promising foundation for cybersecurity training, it lacks focus on real-time user interactions and flexibility regarding hardware integration and grid topologies.

In summary, the discussed approaches offer viable solutions for addressing specific learning objectives in cybersecurity education within the power grid domain. However, none of them satisfies all requirements defined in Section 2.1. In particular, they fall short in offering a flexible training environment emphasizing the practical application of security concepts and collaboration among all involved actors during a cyber incident. As discussed, such an environment is crucial for improving preparedness against real-world cyberattacks. Therefore, we outline PowerRange's design and how it meets these requirements in the following.

3. Design of the training environment

Based on the discussion in the previous section, we identified the open-source co-simulator Wattson [15] as a suitable foundation for the envisioned training platform. Since Wattson models the interaction between power grid assets and their associated IEDs, the OT communication, based on the IEC 104 [24] protocol, directly influences the power grid's state and vice versa. The network emulation reaches down to the link layer (ISO/OSI layer 2), crucially allowing to attach hardware devices, such as network switches, access points, and workstations, to the network and further enables to reproducibly conduct real-world cyberattacks [15]. Hence, Wattson offers a variety of features that directly contribute to a realistic training environment and flexible scenarios. Thus far, Wattson was primarily designed for cybersecurity research for e.g., dataset generation [25] or cyber-resilience analysis [26], and lacks various capabilities required for practical trainings. Therefore, we present the modifications and extensions implemented to transform Wattson into a flexible, realistic, and immersive cybersecurity training platform. We visualize the architectural overview in Fig. 1.

3.1. Network emulation

As a first step, we redesigned Wattson's network emulation by replacing Containernet [27] with a native implementation. With Containernet, changing the topology during the emulation, including virtual machines, and dynamically attaching hardware devices is error-prone. Additionally, routing capabilities are not natively supported by Containernet and thus have to be included externally.

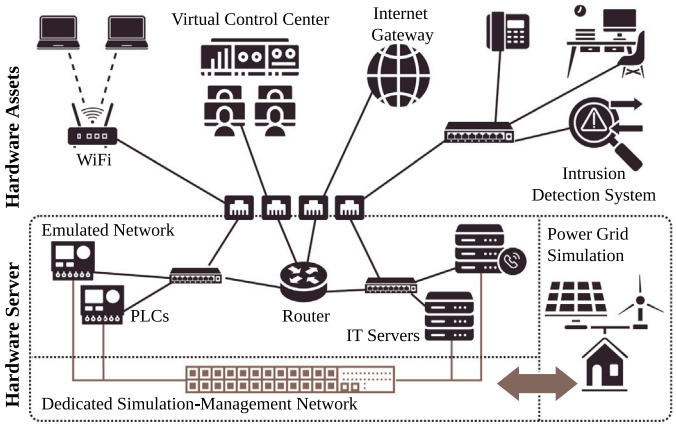

Fig. 1. PowerRange uses Wattson to create a digital twin of the power grid and its ICT network. All devices that the participants should interact with can be attached as hardware devices to the emulated network, creating an immersive and realistic training environment.

The updated framework supports three types of hosts: *linux networking namespaces*, *docker-based hosts* and *virtual machines*. The object-oriented design enables seamless substitution and extension of host implementations and flexible integration of hardware devices while further supporting real-time topology changes during runtime. With traffic shaping for each link and interface, aspects covering packet loss, bandwidth limitations, jitter and delays are freely configurable to recreate realistic networking behavior. Since the network relies on emulation (in contrast to simulation), it behaves like a physical network down to layer 2. Emulation provides valuable advantages over simulation, since it *recreates* the actual behavior of the network by switching, routing and forwarding packets based on respective protocols. Hence, physical devices can be directly connected to the emulated network without further modifications, network traffic can be captured with software and hardware tools, and communication protocol stacks from physical systems are compatible with Wattson by default. These features enable hardware-in-the-loop (HIL) scenarios as well as the usage of real-world malware or attack patterns, which contributes to all identified cyber range requirements. With network namespaces and potential air-gapped operation, Wattson now provides an isolated infrastructure for safely conducting such attacks without risks for external systems. For cybersecurity trainings, where the attacks are under full control of the trainers, the network emulation can also be attached to external networks without risks for these infrastructures.

We further realize a `RemoteNetworkEmulator` interface which provides external access to the running emulation (especially for trainers), enabling dynamic manipulations of the network topology and interaction with all nodes, links, and interfaces from outside the co-simulation. Thus, mirror ports can be defined flexibly, physical interfaces can be attached to emulated network nodes, and cyberattacks can be conducted dynamically without a pre-defined playbook. These changes have been integrated into the open-source repository of Wattson.[1]

3.2. Power grid simulation

In addition to enhancing network emulation, we extend Wattson's power grid simulation, which is based on pandapower [28]. Pandapower provides lightweight steady-state power flow computations, which are well-suited for cybersecurity training. Crucially, they can

[1] https://github.com/fkie-cad/wattson

keep up with the real-time network emulation, as evaluated in Wattson's original publication [15]. In contrast to the behavior-recreating network emulation, the power grid simulation calculates *how* a real-world power grid behaves under the given configuration, environmental influences and demand behavior.

To enable flexible interaction for control center participants, we developed an object-oriented power grid model that extends the capabilities of the underlying pandapower-based simulation. This model introduces features such as energy storage handling and percentage-based power control, while continuing to use pandapower for efficient power flow computations. In parallel to the network emulation, we implemented a `RemotePowerGridModel`, which provides external interfaces for observing and modifying the power grid state in real time. This grid modeling approach is integrated into PowerOwl (cf. Section 4), which facilitates the derivation and orchestration of training scenarios. Since steady-state simulation abstracts from transient (i.e., intermediate) grid behavior and only covers the grid state once all transient effects have settled, low-level protection equipment or equipment damage due to very short voltage spikes cannot be represented in Wattson. While transient behavior would increase the accuracy of the power grid simulation for these aspects, the required computational costs increase significantly as well [15]. Since steady-state simulation has been proven to accurately cover numerous cyber attacks [15], it is more than sufficient for training responses for such cyber incidents. For significantly different training scenarios, we already prepared Wattson to utilize different simulation approaches, such as transient Real Time Digital Simulation (RTDS) [29], with our object-oriented power grid representation and decoupling of power grid modeling and simulation.

3.3. IT and OT components

Besides the changes to the co-simulation environment's core, we further extend Wattson with additional IT and OT components. For a realistic and immersive experience, IT components and subnets have to be part of the training scenario. This includes, for instance, Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers, office subnets, a Session Initiation Protocol (SIP) telephony solution, and a gateway to connect to the Internet. We provide host implementations for these servers and services to be used within Wattson. They can be used as lightweight Docker containers and offer additional immersion features, such as realistic logging and remote access via Secure Shell Protocol (SSH). Further, we extend the IT components with a docker-based Open Shortest Path First (OSPF) router, offering firewall capabilities with SSH-based management and a web interface (Webmin) to configure routing tables and firewall rules. Similarly, we extend the OT components with SSH servers, advanced logging and optional additional services. All components, especially emulated OT devices, can interact with the power grid simulation by obtaining live measurements via the co-simulation management network and manipulate the grid state by issuing respective simulation queries. This enables realizing, for instance, the control commands issued by the operator via IEC 104 within the power grid simulation, such that they influence the physical process in accordance with a real power grid.

3.4. Hardware-in-the-loop

For an immersive experience, the participants should be able to interact with the simulation environment as if it was a real physical system. Hence, using HIL is a crucial element of a cybersecurity training. As explained in Section 3.1, we extended Wattson for excessive inclusion of physical hardware. In particular, we attach hardware switches to the emulated network that are part of different IT and OT subnets (cf. Fig. 1). To these switches, we attach WiFi access points and cable-based workstations for each participant. Hence, trainees can interact with physical devices that are seamlessly integrated into a larger scale network emulation with hundreds of devices to compromise between realism (i.e., hardware devices) and training scenario scalability. By deploying DNS and DHCP services within the emulated network, participants are seamlessly connected to the communication network and can access the Internet through the integrated gateway, if desirable. Furthermore, switch configurations can be dynamically adapted to expose mirror ports on physical interfaces, enabling the on-demand integration of e.g., Intrusion Detection Systems (IDSs).

3.5. Immersive control center

To visualize the power grid's state and for issuing control commands, we create the Virtual Control Center (VCC), visualized in Fig. 2. It interfaces with the Master Terminal Unit (MTU) in the control center and offers a graphical user interface (GUI) to the control center staff to interact with the power grid via the communication network. The VCC features various visualization modes, most notably a single line diagram (SLD), a technical diagram displaying stations in a tree-like structure along with all associated assets. Key metrics, such as voltage levels, are prominently highlighted within the diagram, utilizing visual aids like flashing indicators and color highlights to alert staff to any issues. The VCC *observation center* provides an overview of all events and issues requiring operator attention to guide the participants during training. With the included state estimation (SE), which allows to estimate the grid's state with a limited set of available measurements, missing or faulty measurements can be incorporated in the visualizations.

Operators can interact with Remote Terminal Units (RTUs) responsible for various grid assets through visual grid representations and a dedicated *data point view* to request specific measurements or issue control commands. Beyond controlling assets remotely, the VCC also allows to manually track the power grid's topology, accommodating actions taken in collaboration with on-site personnel. While the VCC offers a variety of functionalities, its primary focus is to provide only those features that are necessary for the respective training. Hence, it provides an intuitive interface for operators that are familiar with proprietary real-world control software while reducing the system's complexity. This aids trainees to focus on the respective tasks instead of the required software handling and provides a common ground for all participants.

Multiple participants across various devices or screens can simultaneously use the VCC, as multiple instances synchronize with one another. Unlike commercial systems that require significant configuration effort, the VCC automatically adapts to the power grid and network of each scenario without manual interference, paving the way for flexible scenario selection. Based on feedback and observations during training, the VCC can be modified to further improve the immersion and to evaluate the usability and impact of e.g., different variants of visual hints.

3.6. Real-world cyberattacks

Beyond realistic normal operations, effective cybersecurity training must also feature real-world cyberattacks. Such attacks should impact both the network and the power grid when executed properly and be detectable and preventable by IT and OT personnel, just like real incidents. Using Wattson with our extensions, we can conduct actual cyberattacks and countermeasures. To support dynamic and adaptive scenarios, we designed a modular catalog of attack building blocks. These can be combined on demand to form complex, multi-stage attacks that evolve based on participant behavior and the effectiveness of defensive actions.

While Wattson already implements various cyberattacks, they mostly focus on the *impact* on the power grid. For realistic training, *reconnaissance*, *lateral movement*, or *privilege escalation* must be part of a multi-stage cyberattack as well. Hence, our catalog includes attacks for these phases that can be configured dynamically during training. These

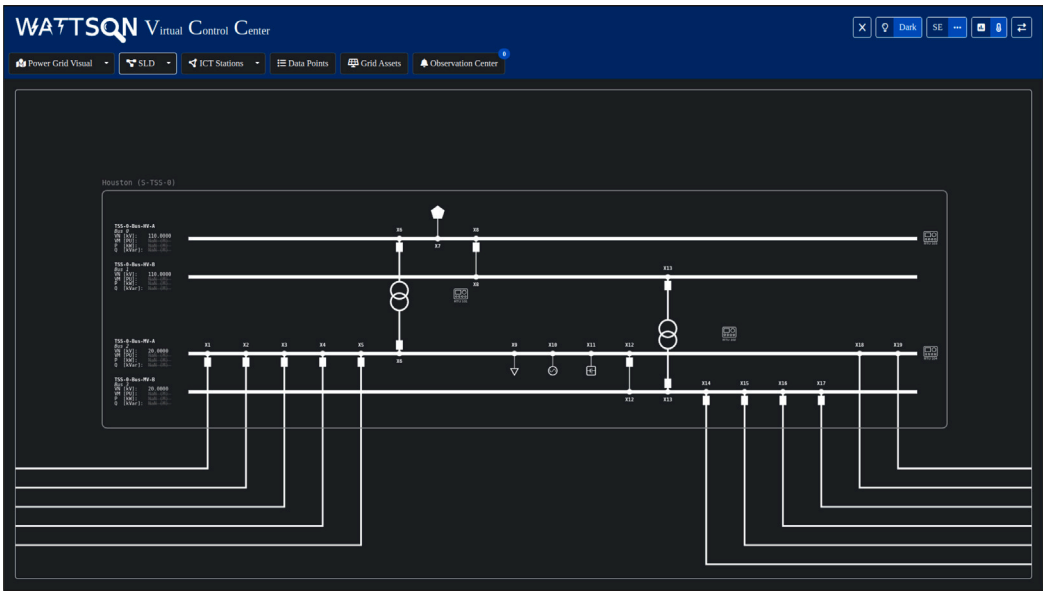

Fig. 2. The Virtual Control Center (VCC) offers a realistic and immersive control interface mimicking the functionality of real-world software.

attacks include (a) scanning for hosts, services and ports, e.g., with `nmap`, (b) lateral movement via SSH brute forcing and vulnerability detection, (c) privilege escalation on accessible hosts, (d) local Denial-of-Service (DoS) by stopping services or shutting down nodes, (e) network-based DoS with flooding (`hping3`) and Address Resolution Protocol (ARP) spoofing (`arpspoof`), (f) process impact via control command issuance (cf. Industroyer [30]) (g) control interference via machine-in-the-middle (MitM) attacks, and (h) false data injection (manipulation of visible grid state) via an MitM attack. While attacks common for IT networks, such as flooding, are implemented with the help of standard tools, we utilize custom implementations for the process-impacting attacks. This ensures compatibility with all desired OT protocols, customizable behavior for training purposes, and their safe application with targeted effects. For instance, for the MitM attacks, we implement protocol state machines for TCP and IEC 104 with Python based on `scapy`, allowing our attacks to observe, modify, extract and inject measurements and commands in an existing connection. During the training, the trainers can select appropriate attack building blocks and combine them as needed for multi-staged attacks.

4. Automatically deriving training scenarios

Besides the technical features and participant immersion *within* a training session, the training *scenario* is an important factor for a flexible and realistic training environment by itself. Such a scenario consists of a power grid topology, a corresponding ICT network, the configuration of the respective OT communication protocol, and further configurations, vulnerabilities and features. With individual power grid topologies, employees of different grid operators can participate in training sessions tailored to their specific work environment and daily routines. This training also includes the preparation for future use cases and newly designed security concepts. Flexible adaptations of topologies and cyberattacks improve the ability of participants to react to new situations, particularly with regular training.

Achieving this flexibility while maintaining compatibility with the training environment, i.e., Wattson, poses a significant challenge. Manually configuring each scenario becomes an unreasonable task for larger power grid topologies, whereas fully automatic scenario creation requires a significant amount of effort and might limit the scenario flexibility. Hence, we follow the approach of automatically deriving a training scenario based on a given power grid topology. Therefore, we now introduce PowerOwl to support the deterministic, configurable derivation of training scenarios for Wattson.

Availability Statement. PowerOwl will be available under an open-source license after the review phase.

4.1. Power grid modeling

The power grid consists of different elements that are connected to each other. From a modeling perspective, we can distinguish between *nodes*, e.g., busbars, that are connected by *edges*—usually power lines or transformers. Further, *assets* such as loads and generators are attached to the grid via a node. In our model, we further specify edge *annotators*. Circuit breakers and other switches can annotate the connection of an edge and a node or form a direct connection between two nodes (e.g., for double busbars).

In the `PowerGridModel` within PowerOwl, we assign all elements of a power grid to these four classes as depicted in Fig. 3 (left). While GridNodes, GridEdges, and GridAnnotators directly influence the topology, GridAssets only affect the grid's behavior. Each of these GridElements is described by a collection of *attributes* of different categories, mainly *properties* (e.g., the maximum current for a line), *configurations* (e.g., the active power consumption of a load), and *measurements* (e.g., the current voltage at a busbar). Each attribute is represented by a `GridValue` that holds the actual value along with information such as the unit and scale of the attribute. When changing a configuration of a GridElement, a power flow computation is triggered to compute the resulting measurements for all GridElements, updating the respective GridValues. While the power grid model allows to represent and simulate the power grid, further semantics, such as the definition of facilities, the derivation of a suitable ICT network, and the definition of communication behavior require a broader model, which PowerOwl achieves with the Multi-Layer Graph (MLG).

4.2. Scenario model: The multi-layer-graph

A training scenario requires more than just a model of the power grid. Wattson requires at least a corresponding network topology and a data point configuration, i.e., a specification on the behavior of the OT communication protocol(s). To automatically derive this information, additional contextual information is necessary. For instance, to decide on whether a GridElement is observable and even controllable remotely via an RTU, determining the type of facility of the GridElement is

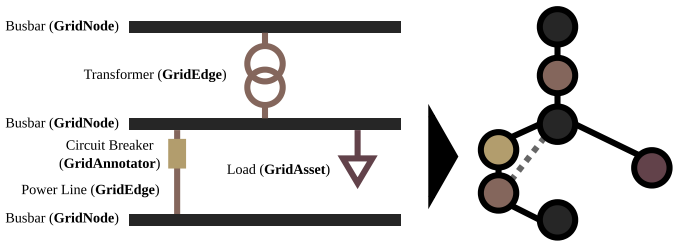

Fig. 3. A model of the power grid (left) can be transferred to a graph representation (right), where each grid element is represented by a node and edges represent their, e.g., physical or logical, relations.

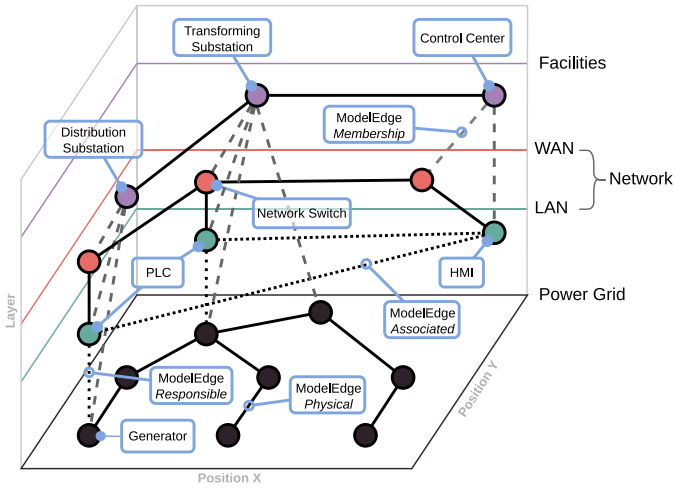

Fig. 4. The Multi-Layer Graph (MLG) structures entities, such as power grid and network elements, and facilities on hierarchical layers. Edges between nodes indicate their relationships and interactions. They can cross layer boundaries. The schematic representation of a simplified MLG features three top-level layers, with two sub-layers for the network layer.

important. While buses in a transforming substation might be equipped with digitized monitoring devices, a bus representing a single household usually is not directly observable via the OT network. Similarly, the resulting network topology and configuration also depends on such contextual information.

To achieve a flexible, extendable and universal representation of all potential contextual information required for automatically deriving a training scenario, we introduce the Multi-Layer Graph (MLG) for PowerOwl, extending the concept of Klaer et al. [31], who propose a graph-based approach for the Smart Grid Architectural Model (SGAM) [32]. In PowerOwl, we design and implement the MLG as an undirected graph consisting of `ModelNodes` and `ModelEdges`. Both of these components support additional attributes—most importantly, every `ModelNode` is assigned to a `GraphLayer`. These layers follow a hierarchical structure, i.e., each layer can have child layers. Fig. 4 visualizes the simplified concept of the MLG, while Fig. 7 provides a full graphical representation in Appendix.

For instance, the *Network* layer can be further subdivided into *WAN* and *LAN* layers, facilitating the formation of more complex groups of nodes. Similarly, a `ModelEdge`, which connects exactly two `ModelNodes` on arbitrary layers, has a specific `EdgeType` indicating the relationship between the connected nodes. Edges can represent various types of connections, including *physical* connectivity, *logical association* (e.g., between a network device and a facility), or technical *responsibility* (e.g., between RTUs and grid elements). Consequently, the MLG provides a cohesive model that encompasses a wide array of concepts, allowing for flexible extensions and analyses of the modeled

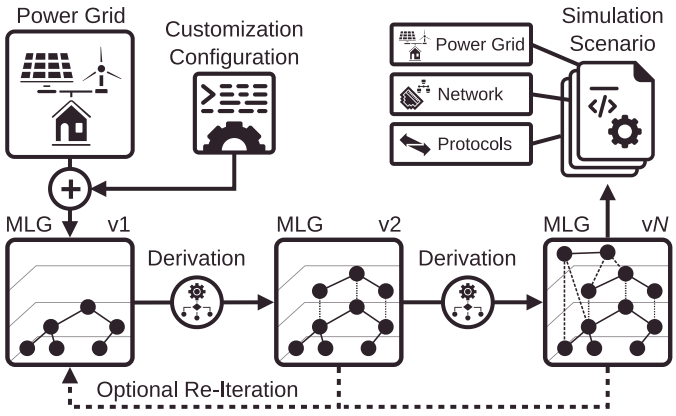

Fig. 5. The derivation process follows an iterative approach where multiple *Derivators* refine the training scenario model based on its MLG representation. Each phase can add, modify or remove information based on the provided customization options, e.g., the desired digitization level. When required, a re-iteration can be initialized to refine earlier derivation phases with contextual information from later stages. Finally, the resulting scenario model can be exported as a ready-to-use simulation scenario.

system using standard graph algorithms. Layers, as well as node and edge types allow to achieve different *views*, i.e., sub-graphs of the model, enabling tailored inspections for automatic scenario derivation. Hence, the MLG serves as the foundation for PowerOwl's derivation process (cf. Section 4.3).

To use the MLG for modeling and automatically deriving a training scenario, the first step is to insert the power grid components, i.e., all `GridElements` (including `GridEdges`) as nodes into the MLG and connect them via edges. Usually, these edges indicate a *physical* relation. However, to indicate the association between `GridEdges` and the `GridNode` in the presence of a `GridAnnotator`, a *logical* edge is inserted. Fig. 3 exemplarily visualizes how the power grid model is transferred into the MLG. The same concept of transferring domain-specific information into a graph-based representation can be applied for all required aspects of a training scenario, such that the MLG serves as the foundation and unified model for each training scenario.

4.3. Derivation process

To automatically derive one or multiple training scenarios based on the initial power grid topology, PowerOwl defines an iterative derivation process, where individual *derivators* use the MLG to analyze, modify and extend the scenario. The goal is to create a flexible scenario that is usable within Wattson. Further, the derivation should respect flexible configuration options to stear the process into a partially predefined direction (e.g., to reflect a future state of digitization). This derivation process is a linear procedure as visualized in Fig. 5 and consists of the following steps:

Power Grid Configuration: The grid is analyzed, possibly extended, and configured, including the identification of contextual attributes such as voltage levels.

Organizational Modeling: Organizational units are created, representing domains such as *operation*, *office* or the *control center*.

Facility Identification: Individual facilities are derived by grouping GridElements based on systemic roles. For instance, buses with different voltage niveaus and one or more transformers typically represent a substation.

ICT/IT Network Derivation: The corresponding ICT and IT networks are derived following a bottom-up approach where individual facility networks are derived first, before the backbone network follows. Depending on contextual information, the respective facility as well as user-made configurations are incorporated for assigning RTUs to GridElements, before IT equipment is placed and subnets are defined.

OT Communication Specification: The specification is derived for the different OT protocols, including IEC 104, IEC 61850 MMS and Modbus/TCP. Information objects, data attributes or registers are derived and linked to individual GridValues of GridElements.

Since power grid models often abstract certain details, such as low-voltage assets within a medium-voltage grid, PowerOwl enables automated modifications to derive, e.g., low-voltage networks at distribution substations. Hence, earlier stages of the derivation process (e.g., power grid configuration) may depend on information generated in later stages (e.g., facility identification). Thus, the derivation process is designed to be iterative, allowing outputs from a previous iteration to inform the next. This ensures both high flexibility and consistency in the resulting models.

Each derivation step is designed to be deterministic and follows a rule-based approach that respects configuration choices made by the user with the help of a Python or JSON-based custom configuration. For instance, to influence whether power generators are controllable by the grid operator, the respective configuration option (`generators-controllable`) can be set to different values to make all (or none) of the generators controllable, to manually select individual controllable generators from the power grid model, to apply the controllability based on the voltage niveau (e.g., to make only medium voltage generators controllable) or based on custom logic that has to be implemented by the user. All configuration options have default values to ease the derivation process. If the user desires a completely different derivation process, PowerOwl allows custrom `Derivators` for each derivation step. The configuration and derivation process for the user consists of the following steps:

1. **Power Grid Topology.** The user defines the power grid topology, either by using power grid models from the literature (such as simbench [33]) or by manually creating a PowerOwl `PowerGridModel`
2. **[Optional] Configuration.** The user provides an optional configuration for PowerOwl. For each derivation step, decisions on how to derive the respective aspect can be freely configured to achieve different levels of controllability, observability and complexity.
3. **Derivation.** PowerOwl iteratively derives the comprehensive MLG.
4. **[Optional] Validation.** The user can inspect the visual representation of the scenario and adjust aspects if desired.
5. **Export.** PowerOwl exports the MLG representation to a Wattson-compatible scenario configuration.

Hence, PowerOwl provides extensive flexibility if desired by the user while still maintaining an easy-to-use interface for the default derivation process.

4.4. Flexible scenarios and usability

While PowerOwl's derivation process is deterministic, it provides flexible behavior to allow users to granularly tune training scenarios for their specific needs. This flexibility covers the granularity of the power grid, i.e., voltage niveaus can be aggregated or, if missing from the initial power grid topology, disaggregated to automatically create a desired power grid topology. Further, the complexity of the ICT network can be influenced in various ways, e.g., by limiting the number of digitized substations, abstracting from certain devices or choosing different OT protocols. Combining the power grid and OT components, controllability of assets is flexible, e.g., PowerOwl allows to integrate controllable photovoltaic (PV) generators or restrict them to be only observable. Variable selection of protection equipment and IT infrastructures allow further refining the scenario. PowerOwl provides extensive configurability and flexibility. Nevertheless, the deterministic derivation process follows a rule-based approach that, e.g., potentially limits the possible ICT topologies. While this significantly enhances the usability and reproducibility, some ICT scenarios require significantly differing rule sets. To allow users to remove, modify or add assumptions and rules, each derivation step can be replaced, new steps can be added, or pre-defined steps can be removed entirely.

This resulting scenario contains extensive information which is primarily valuable during derivation and for advanced analyses. For cybersecurity training usage, the information on the power grid model, ICT network topology, and OT protocol configurations suffice. PowerOwl supports exporting the MLG as a ready-to-run scenario for Wattson. The additional information allows to automatically create documentation for the grid operator, identify cybersecurity vulnerabilities, or optimize both the network and power grid topologies.

Conclusion. To enable cybersecurity training with realistic yet flexible scenarios, we introduce PowerOwl for granularly tunable derivation of such scenarios. The resulting scenarios can be used in cyber ranges to create realistic infrastructures of both the power grid and the corresponding ICT network. PowerOwl's compatibility with Wattson paves the way for conducting cybersecurity training where participants can learn how to use technical solutions for preventing or detecting cyberattacks and for appropriate reactions to them. Further, well-established technologies and systems can be integrated into such training to evaluate their usability, i.e., their capabilities and user-friendlyness, in a safe environment in a stressful situation. We now continue to describe the conceptual training procedure and the results of how pilot training contributes to enhancing security.

5. Proposed training concept and pilot implementation

Completing the technical foundation for PowerRange and the possibility of deriving flexible training scenarios, we now detail the training procedure itself by introducing an exemplary training concept. It is important to note that PowerRange enables a broad spectrum of training configurations tailored to the specific requirements of different target audiences. Accordingly, Section 5.1 outlines the core components and general guidelines of one representative concept. Subsequently, Section 5.2 illustrates the application of the proposed concept through two pilot training sessions, while Section 5.3 summarizes the insights and feedback gathered from these sessions.

5.1. Training concept

We propose to conceptually divide the training into two phases: In the first phase, the participants receive a guided introduction to the scenario, including their roles, responsibilities, and available tools. They begin with routine operational tasks, such as maintenance activities. The second phase begins once a cyberattack is initiated and, eventually, becomes noticeable. At this point, the focus shifts to detecting the attack, responding appropriately, and initiating recovery procedures.

Moreover, the training concept targets all key stakeholders within a power grid operator who would be involved in responding to a cyberattack. Therefore, we propose to devide the participants into the three distinct groups *management*, *IT/OT personnel*, and *control center*. Within each group, participants take on specific roles to ensure a clear distribution of tasks and responsibilities.

The cyberattack comprises multiple building blocks designed to target specific participant roles. While IT-related attacks, such as DoS,

might disrupt the IT/OT staff, more advanced false data injection attacks primarily target the control center personnel. Additionally, cyberattacks can directly target the human factor, e.g., through social engineering tactics or blackmailing.

While the latter offers clear evidence for a potential cyber threat, the participants have further possibilities to detect the cyberattack. With log files, IDSs, and service monitoring, the IT/OT personnel can identify network anomalies, while the VCC shows warnings to alert the operators of potential issues. Some more subtle effects of attacks require different groups to collaborate to identify the origin, offering a valuable training lesson. For detection possibilities beyond the training environment, such as searching for planted devices in substations, tabletop elements can be integrated to extend the capabilities of the participants.

Finally, the participants should apply technical and organizational measures to respond to ongoing cyberattacks effectively. The main challenge lies in coordinating decisive responses to contain the attack, identify its origin, and address the underlying vulnerability to restore normal operations. The participants can carry out realistic countermeasures and observe their impact by leveraging the emulated network, the VCC, and management-level decision-making.

In summary, the anticipated learning objectives comprise, on the one hand, enhancing awareness of cyberattacks targeting power grids and their potential consequences, as well as fostering the practical application of both technical and organizational countermeasures. On the other hand, particular emphasis is placed on strengthening communication among the key stakeholders of a power grid operator during a cyberattack, thereby improving coordination, situational understanding, and overall incident response effectiveness.

5.2. Pilot training conduction

To validate the design of PowerRange and the proposed training concept, we conducted two independent pilot training sessions with 11 and 15 participants, respectively, all professionals from the energy sector. For the first training, the participants were operational staff from different German grid operators, while the second training's participants were international experts for power grid cybersecurity. The voluntary participation was offered free of charge, and feedback was collected anonymously and provided voluntarily as well. Although the gathered feedback and observations do not constitute a comprehensive training evaluation, they nonetheless provide valuable insights into the application of cyber ranges within the power grid domain and offer guidance for refining the proposed training concept.

Setup. Each training took place over a single day in a dedicated facility, where IT/OT, control center, and management personnel were assigned separate rooms with the flexibility to move between them. The IT/OT area comprised several workstations equipped with laptops connected to both the simulated IT and OT networks, utilizing Wattson's HIL capabilities. In addition, the IT/OT group was provided with security tools and documentation, including a commercial IDS for monitoring network traffic in the control center. Fig. 6 visualizes the possible physical interactions for trainees and trainers.

The control center area, in turn, featured operator workstations with large displays providing access to the *Observation Center* via the VCC interface. The VCC aggregates alerts related to grid status and network events, such as RTUs outages, thus enabling control center personnel to monitor, analyze, and respond to real-time incidents as the scenario unfolded.

The management area consisted of a large meeting room designed to facilitate information exchange and status discussions. It was equipped with presentation screens and whiteboards to support situational coordination and decision-making activities. Moreover, SIP telephones integrated into the IT network connected all participant groups and allowed for simulated communication with external stakeholders, including customers, media representatives, and relevant authorities.

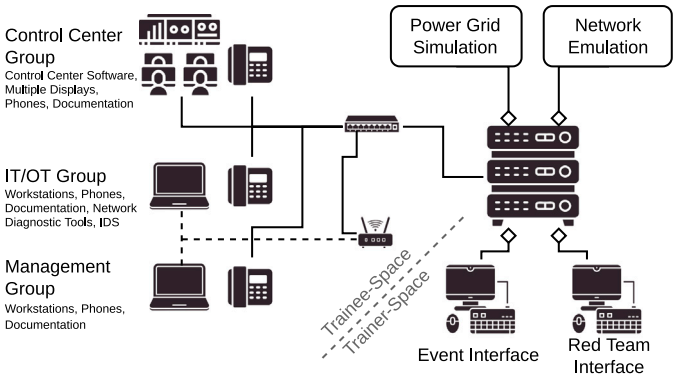

Fig. 6. During the training, PowerRange combines various physical/real-world interactions for trainees with virtual ones that are conducted by the trainers. While trainees interact with common and specialized software, phones, company procedure guidelines, documentation and external actors (government entities, customers, technicians) represented by trainers via phone or mail, the trainers can implement these actions within the training environment via the event interface, which directly links to the co-simulation environment. Trainers further take the role of the attackers via the red team interface.

The trainers had a dedicated room to interact with the training environment to induce events such as device failures, replicate actions of virtual remote personnel such as electrical engineers in substations, and conduct cyberattacks. PowerRange provides a set of predefined building blocks for these interactions and scenarios to minimize the required efforts by the trainers while also offering low level interactivity to allow flexible adjustment besides the predefined scenarios.

Introductory Phase. During the first two hours of training, participants were introduced to the scenario, training-specific interfaces, and available tools. Control center personnel, for example, received a guided, hands-on introduction to the VCC interface and its functionalities. Realistic tasks, such as coordinating planned maintenance or responding to capacity bottlenecks, were combined with deliberately induced ICT equipment failures, e.g., due to technical faults. Such failures, namely disconnected devices, were easily identifiable by control center personnel, since the VCC interface displayed the corresponding events.

Uncertain whether these events were already part of a cyberattack, the trainees naturally engaged in cross-group communication to assess the situation and resolve issues. They were generally suspicious of benign failures in both sessions, anticipating a cyberattack.

Cyberattacks. In both training sessions, the organizers also acted as the red team, i.e., the attackers. To focus on incident response rather than initial intrusion, the scenario assumes that the attackers already gained physical access to remote substations and installed malicious devices. Once the trainees are familiar with the scenario, group roles, and technical setup, the attackers initiate a multi-stage cyberattack. While key components are pre-defined, the attack progression is continuously adapted based on the progress and trainees' responses to ensure a challenging yet not-overwhelming training experience.

The attack began with reconnaissance activities to identify subnets, hosts, and vulnerable services. Although the IDS detected these scans in both sessions by triggering corresponding notifications, they went unnoticed by the IT/OT group. The missed notifications can likely be explained by the high number of false-positive alarms that occurred during the IDS setup, as these alarms had to be manually classified.

The attackers then sent a blackmail message via e-mail to the management group, demonstrating their access and demanding a ransom for not disrupting grid operations. Subsequent phases included lateral movement (e.g., SSH brute-force attacks) and network-based DoS techniques such as flooding and ARP spoofing. Using compromised credentials, the attackers also terminated services on affected devices.

These DoS-induced disruptions resembled earlier, benign device failures and thus did not immediately raise suspicion, although their effects were promptly investigated in both sessions. In the final phase, False Data Injection (FDI) attacks manipulated measurements to fabricate bottlenecks or blackouts, while Industroyer-like attacks issued malicious control commands, such as opening breakers, altering generator infeeds or disconnecting assets.

Responses. From a response perspective, the trainees faced three key challenges during the cyberattack: detecting the attack, establishing effective intra- and inter-group communication, and making timely decisions to counter the attack. Although the attackers issued a blackmail message early on, only the management group received it initially. In the first session, this information was not effectively shared with other groups—particularly the IT/OT group, which continued to interpret the DoS effects as technical failures. The participants in the second session displayed much better communication, influenced by explicit guidance from the organizers on the importance of information flow.

This communication gap delayed the implementation of countermeasures in both sessions. However, once awareness was aligned across groups, technical responses were executed effectively. Notably, while operational communication for coordinating concrete actions worked well, purely informative communication proved less effective.

During both training sessions, the IDS detected several attack phases and logged relevant information, including attack origins. Such data could have been used to block malicious traffic via available firewalls. However, due to high stress levels and the increasing number of alerts, the trainees had difficulties in effectively using the system.

5.3. Feedback and insights discussion

After both sessions, we collected voluntarily participant feedback on the training execution, scenario design, cyberattack simulation, and perceived challenges and insights. All trainees emphasized the value of such hands-on training and appreciated the realistic environment and cyberattacks.

A major feedback aspect was the importance of a realistic and complex yet accessible scenario during the training. During the first session, the scenario was perceived as overly complex and insufficiently clear. In response, the second training session leveraged the flexibility of PowerOwl to simplify the scenario and improve comprehensibility.

The importance of training effective and well-structured communication during critical incidents, especially across different teams, also emerged as key takeaway that often comes short in group-specific trainings. Similarly, for the usability of cybersecurity tools, familiarity was highlighted: While various technologies were provided, unfamiliar tools were largely unused during the training. For future training sessions, we plan to introduce dedicated preparatory courses focused on relevant technologies, and to integrate the particular technologies, e.g., IDSs, known to the participants.

Overall, the participants agreed that a comprehensive cybersecurity strategy must include practical training in technical tools and incident response procedures with a special focus on communication and coordination and that a cyberrange environment such as PowerRange is well-suited to conduct such training. However, a limitation of this study lies in the absence of a quantitative assessment of the training effectiveness. Building upon the present findings, future work should therefore refine the current training concept and systematically evaluate its effectiveness in achieving the defined learning objectives across multiple training sessions.

6. Conclusion

This paper introduces PowerRange, an advanced cyber range for power grid operators, seamlessly integrating a state-of-the-art power grid co-simulator with extensive user interaction capabilities. Besides combining power grid simulation and ICT network emulation, PowerRange thus includes HIL for IT/OT components and a control room software, enabling immersive, practical engagement across all organizational levels. Additionally, we present PowerOwl to support flexible, automated scenario generation tailored to specific training needs. With flexible components, such as HIL or the VCC, PowerRange allows creating tailored training scenarios and relying on both, generic building blocks (such as the VCC) as well as specialized real-world systems (e.g., real-world control software). Based on this architecture, we propose a training concept, which we preliminary evaluate through two independent pilot training sessions.

Our findings underscore the importance of hands-on training for enhancing cyber incident response capabilities in power grids. Regularly conducted training improves the practical application of cybersecurity measures and fosters better communication and coordination among key stakeholders. These insights highlight the necessity of addressing the human factor alongside technological advancements to strengthen the overall resilience of grid operations.

CRediT authorship contribution statement

Lennart Bader: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Data curation, Conceptualization. **Eric Wagner:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **Martin Serror:** Writing – review & editing, Writing – original draft, Validation, Supervision, Methodology, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors gratefully acknowledge the support and collaboration of the Future Energy Lab of the German Energy Agency (dena) in the realization of the pilot trainings.

Appendix. PowerOwl model derivation

PowerOwl creates a comprehensive model of a power grid scenario, including a representation of the power grid itself along with derived information such as the network topology with nodes, subnets and links, facilities, and communication protocol configurations.

Each entity, represented by a node in the MLG, has various *attributes* that further specify this entity. For instance, a `NetworkInterface` stores information such as the supported bandwidth, a MAC address, and, if applicable, an IP address.

The edges in the MLG indicate the relations and interactions of different entities. Besides basic *physical* connections, especially for power grid entities, responsibilities of OT network devices for power grid assets are indicated by *responsibility* edges.

While PowerOwl provides a default implementation for the derivation process, each derivation phase can be customized or replaced entirely if desired. Further, additional derivation processes can be implemented to different areas of the model. Here, the flexibility of the MLG allows for additional semantics of new layers or edge types.

Fig. 7 visualizes the MLG resulting from the derivation process from a small medium-voltage distribution grid, extending the conceptual visualization of Fig. 4.

Data availability

Data will be made available on request.

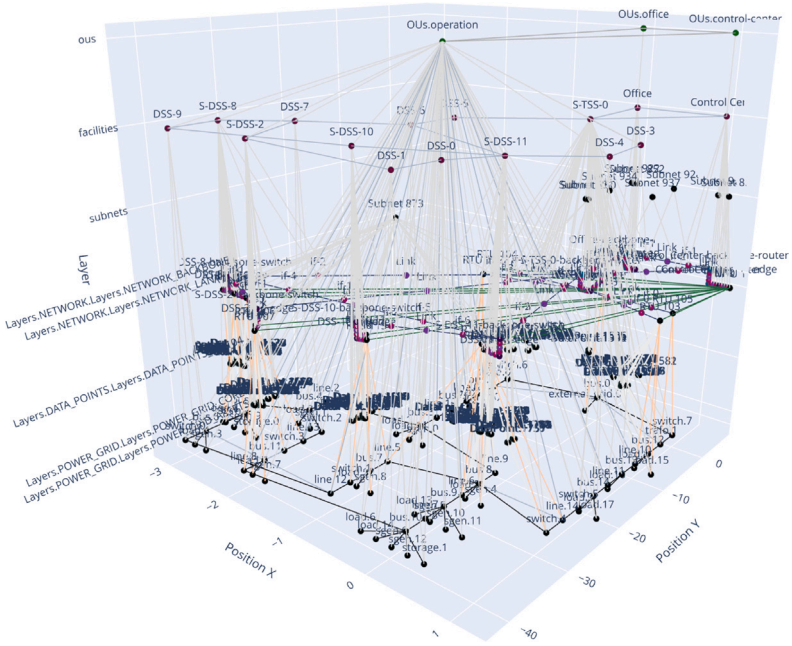

Fig. 7. The MLG resulting from a small medium-voltage distribution grid contains entities and their relations from several domains. Besides the power grid itself, resulting facilities such as transforming and distribution substations, a control center, and offices are represented in the graph. Networking equipment, covering hosts and switches, links and individual interfaces are derived based on the facilities and the power grid's topology. Finally, the power grid and network equipment are linked by including OT network protocol configurations, e.g., data point information for the IEC 104 protocol.

References

[1] C.-C. Sun, A. Hahn, C.-C. Liu, Cyber security of a power grid: State-of-the-Art, Int. J. Electr. Power Energy Syst. 99 (2018) http://dx.doi.org/10.1016/j.ijepes.2017.12.020.

[2] G. Elbez, H.B. Keller, V. Hagenmeyer, A new classification of attacks against the cyber-physical security of smart grids, in: International Conference on Availability, Reliability and Security, ACM, 2018, http://dx.doi.org/10.1145/3230833.3234689.

[3] M.Z. Gunduz, R. Das, Analysis of cyber-attacks on smart grid applications, in: International Conference on Artificial Intelligence and Data Processing, IDAP, 2018, http://dx.doi.org/10.1109/IDAP.2018.8620728.

[4] C. Peng, H. Sun, M. Yang, Y.-L. Wang, A survey on security communication and control for smart grids under malicious cyber attacks, IEEE Trans. SMC: Syst. 49 (8) (2019) http://dx.doi.org/10.1109/TSMC.2018.2884952.

[5] V.S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, J.L.R. Torres, Cyber attacks on power grids: Causes and propagation of cascading failures, IEEE Access 11 (2023) http://dx.doi.org/10.1109/ACCESS.2023.3317695.

[6] D.E. Whitehead, K. Owens, D. Gammel, J. Smith, Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, in: Annual Conference for Protective Relay Engineers, CPRE, 2017, http://dx.doi.org/10.1109/CPRE.2017.8090056.

[7] M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and opportunities in securing the industrial internet of things, IEEE Trans. Ind. Informatics 17 (5) (2021) http://dx.doi.org/10.1109/TII.2020.3023507.

[8] J. Prümmer, T. van Steen, B. van den Berg, A systematic review of current cybersecurity training methods, Comput. Secur. 136 (2024) http://dx.doi.org/10.1016/j.cose.2023.103585.

[9] D. Ussher-Eke, From awareness to action: Designing effective cybersecurity training programs, Int. J. Sci. Res. Arch. 16 (2023) http://dx.doi.org/10.30574/ijsra.2025.16.2.2348.

[10] G. Kavallieratos, A. Amro, V. Gkioulos, G. Stamatescu, K. Rantos, T. Lagkas, K. Demertzis, F. Paterakis, A. Lekidis, C. Dalamagkas, et al., Best-practices-based training for improving cybersecurity in power grids, in: European Symposium on Research in Computer Security, Springer, 2024.

[11] V.E. Urias, B. Van Leeuwen, W.M. Stout, H.W. Lin, Dynamic cybersecurity training environments for an evolving cyber workforce, in: International Symposium on Technologies for Homeland Security, HST, IEEE, 2017, http://dx.doi.org/10.1109/THS.2017.7943509.

[12] H. Aldawood, G. Skinner, Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues, Futur. Internet 11 (3) (2019) http://dx.doi.org/10.3390/fi11030073.

[13] N. Chowdhury, V. Gkioulos, Cyber security training for critical infrastructure protection: A literature review, Comput. Sci. Rev. 40 (2021) http://dx.doi.org/10.1016/j.cosrev.2021.100361.

[14] T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, Cybersecurity in power grids: Challenges and opportunities, Sensors 21 (18) (2021) http://dx.doi.org/10.3390/s21186225.

[15] L. Bader, M. Serror, O. Lamberts, Ö. Sen, D. van der Velde, I. Hacker, J. Filter, E. Padilla, M. Henze, Comprehensively analyzing the impact of cyberattacks on power grids, in: European Symposium on Security and Privacy (EuroS&P), IEEE, 2023, http://dx.doi.org/10.1109/EuroSP57164.2023.00066.

[16] M.M. Yamin, B. Katt, V. Gkioulos, Cyber ranges and security testbeds: Scenarios, functions, tools and architecture, Comput. Secur. 88 (2020) http://dx.doi.org/10.1016/j.cose.2019.101636.

[17] G. Kavallieratos, S.K. Katsikas, V. Gkioulos, Towards a cyber-physical range, in: Cyber-Physical System Security Workshop, CPSS '19, ACM, New York, NY, USA, 2019.

[18] H. Holm, M. Karresand, A. Vidström, E. Westring, A survey of industrial control system testbeds, in: Secure IT Systems, Springer Int'l Publishing, Cham, 2015.

[19] J. Stites, A. Siraj, E.L. Brown, Smart grid security educational training with ThunderCloud: A virtual security test bed, in: Information Security Curriculum Development Conference, ACM, 2013, http://dx.doi.org/10.1145/2528908.2528927.

[20] N. Saxena, V. Katos, N. Kumar, Cyber-physical smart grid security tool for education and training purposes, in: International Workshops: Realigning Cyber Security Education, 2017.

[21] N. Saxena, V. Chukwuka, L. Xiong, S. Grijalva, CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid, in: Workshop on Cyber-Physical Systems Security and Privacy, ACM, 2017.

[22] S. Adepu, N.K. Kandasamy, A. Mathur, EPIC: An electric power testbed for research and training in cyber physical systems security, in: Computer Security, Springer International Publishing, Cham, 2019.

[23] T.D. Le, A. Anwar, S.W. Loke, R. Beuran, Y. Tan, GridAttackSim: A cyber attack simulation framework for smart grids, Electronics 9 (8) (2020) http://dx.doi.org/10.3390/electronics9081218.

[24] Telecontrol equipment and systems - Part 5-104: Transmission protocols - network access for IEC 60870-5-101 using standard transport profiles, 2006.

[25] E. Wagner, L. Bader, K. Wolsing, M. Serror, Sherlock: A dataset for process-aware intrusion detection research on power grid networks: Dataset paper, in: Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy, CODASPY'25, 2025, http://dx.doi.org/10.1145/3714393.3726006.

[26] L. Bader, E. Wagner, M. Henze, M. Serror, METRICS: A methodology for evaluating and testing the resilience of industrial control systems to cyberattacks, in: Computer Security. ESORICS 2023 International Workshops, Springer Nature Switzerland, Cham, 2023, http://dx.doi.org/10.1007/978-3-031-54204-6_2.

[27] M. Peuster, H. Karl, S. van Rossem, MeDICINE: Rapid prototyping of production-ready network services in multi-pop environments, in: IEEE Conference on Network Function Virtualization and Software Defined Networks, 2016, http://dx.doi.org/10.1109/NFV-SDN.2016.7919490.

[28] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, M. Braun, Pandapower—An open-source python tool for convenient modeling, analysis, and optimization of electric power systems, IEEE Trans. Power Syst. 33 (6) (2018) http://dx.doi.org/10.1109/TPWRS.2018.2829021.

[29] IEEE recommended practice for hardware-in-the-loop (HIL) simulation-based testing of electric power apparatus and controls, ieee std 2004-2025, 2025, http://dx.doi.org/10.1109/IEEESTD.2025.11144468.

[30] ESET Research, Industroyer2: Industroyer reloaded, 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/, (last accessed: 15 October 2025).

[31] B. Klaer, Ö. Sen, D. van der Velde, I. Hacker, M. Andres, M. Henze, Graph-based model of smart grid architectures, in: International Conference on Smart Energy Systems and Technologies, SEST, 2020, http://dx.doi.org/10.1109/SEST48500.2020.9203113.

[32] M. Uslar, S. Rohjans, C. Neureiter, F.P. Andrén, J. Velasquez, C. Steinbrink, V. Efthymiou, et al., Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective, Energies 12 (2) (2019).

[33] S. Meinecke, D. Sarajlić, S.R. Drauz, A. Klettke, L.-P. Lauven, C. Rehtanz, A. Moser, M. Braun, SimBench—A benchmark dataset of electric power systems to compare innovative solutions based on power flow analysis, Energies 13 (12) (2020) http://dx.doi.org/10.3390/en13123290.