Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures

Dennis van der Velde‡, Martin Henze*, Philipp Kathmann†, Erik Wassermann§,
Michael Andres‡, Detert Bracht††, Raphael Ernst*, George Hallak‖, Benedikt Klaer‡,
Philipp Linnartz¶, Benjamin Meyer**, Simon Ofner*, Tobias Pletzer§, Richard Sethmann†
‖*devolo AG,* Aachen, Germany · george.hallak@devolo.de
‡*Fraunhofer FIT,* Aachen, Germany · {dennis.van.der.velde, michael.andres, benedikt.klaer}@fit.fraunhofer.de
**Fraunhofer FKIE,* Wachtberg, Germany · {martin.henze, raphael.ernst, simon.ofner}@fkie.fraunhofer.de
***KISTERS AG,* Aachen, Germany · benjamin.meyer@kisters.de
¶*RWTH Aachen University,* Aachen, Germany · p.linnartz@iaew.rwth-aachen.de
§*Schleswig-Holstein Netz AG,* Quickborn, Germany · {erik.wassermann, tobias.pletzer}@sh-netz.com
††*umlaut energy GmbH,* Aachen, Germany · detert.bracht@umlaut.com
†*University of Applied Sciences Bremen,* Bremen, Germany · {philipp.kathmann, richard.sethmann}@hs-bremen.de

Abstract—**The fundamental changes in power supply and increasing decentralization require more active grid operation and an increased integration of ICT at all power system actors. This trend raises complexity and increasingly leads to interactions between primary grid operation and ICT as well as different power system actors. For example, virtual power plants control various assets in the distribution grid via ICT to jointly market existing flexibilities. Failures of ICT or targeted attacks can thus have serious effects on security of supply and system stability. This paper presents a holistic approach to providing methods specifically for actors in the power system for prevention, detection, and reaction to ICT attacks and failures. The focus of our measures are solutions for ICT monitoring, systems for the detection of ICT attacks and intrusions in the process network, and the provision of actionable guidelines as well as a practice environment for the response to potential ICT security incidents.**

Index Terms—**electric power systems, ICT, cyber security, cyber attacks, intrusion detection, monitoring, incident response**

I. INTRODUCTION

Power supply is undergoing a fundamental change as Information and Communication Technology (ICT) systems are implemented by all power system actors [1]. At the same time, the increased expansion of distributed generation and the integration of new consumer types (e.g., charging infrastructure) at the distribution grid level, require rethinking conventional grid operation [2], [3]. Different actors, grid operators, energy production, as well as private and industrial customers increasingly interact, e.g., by offering flexibility and market mechanisms controlled and enabled by ICT components.

As a result, malfunctions on the ICT level can directly impact physical grid operation, potentially leading to local or large-scale power outages. This makes the power system ICT infrastructure—Transmission System Operators (TSOs), Distribution System Operators (DSOs), Virtual Power Plant (VPP) operators, metering point operators, and manufacturers—an attractive target for advanced cyber attacks [4], as indicated by the successful attacks on the ICT infrastructure of the Ukrainian power grid in 2015 and 2016 [5], [6].

To prevent such cyber attacks, existing security measures must be accompanied by a close monitoring of irregularities and fast incident response. This requires a comprehensive Intrusion Detection System (IDS) as a measure for ICT networks of power system actors that takes domain-specific characteristics (e.g., process information) into account [7]. To obviate the need for long pilot phases for integration into grid operation, current and advanced security technologies need to be tested in interaction with primary technology in a realistic environment. Finally, as even the best security measures do not offer full protection against complex attacks, non-cyber-security experts need technical guidelines to quickly decide if a given event is a cyber attack or failure.

Only an optimal interplay of prevention, detection, and reaction allows to counter new advanced and unknown threats to ICT infrastructure in power systems and thus contribute to system safety and availability. To achieve this goal, we present our ongoing work on MEDIT to provide **m**ethods for actors in the **e**lectric power system to prevent, **d**etect and react to **ICT** attacks and failures along the following three segments:

1) As basis for our work, a *research and validation environment* for future distribution grids allows to investigate complex interactions or deviations from normal operation, e.g., through ICT attacks and failures. Here, MEDIT relies on an ICT energy co-simulation environment for large-scale investigation and a realistic distribution grid laboratory.
2) MEDIT's approach for the *prevention and detection of ICT failures and attacks* on uses monitoring for power system components to record and observe parameters of technical systems to detect abnormal behavior as well as intrusion detections systems to timely detect the active intrusion of third parties into the ICT infrastructure of energy actors.
3) To support the *reaction to ICT security incidents*, MEDIT relies on a realistic training and simulation environment

This is the author's version of a paper accepted for publication in the proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon). It is posted here by permission of IEEE. Not for redistribution. Cite as: D. van der Velde *et al.*, "Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures," in *Proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon)*, 2020.

© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

to teach technical personnel as well as actionable incident response guidelines that allow non-security experts to adequately mitigate and repel ICT failures and attacks.

II. ICT Infrastructure and Attack Vectors in Distribution Grids

The demand for real-time information and control of distributed assets for new operational concepts [2], [3], requires an extensive and partly parallel ICT infrastructure via private or public communication channels. This creates new risks and attack vectors for the entire energy supply system [4], [7].

In Figure 1, we exemplary give an overview of the envisioned ICT infrastructure of a DSO in future power systems. The central Supervisory Control and Data Acquisition (SCADA) system, which controls the distribution grid, is connected through firewalls to multiple networks such as the company network and the Internet, often used for remote access. To ensure security for this remote access, an additional terminal server separates connections and implements additional security mechanisms such as two factor authentication.

For the actual grid operation, however, the DSO uses a completely private ICT infrastructure owned and operated by the DSO. This communication network is often called Operational Technology (OT) network and is separated from the normal company network, used for the conventional office IT such as desktop PCs and printers. Through this OT network, the SCADA system receives measurements from various grid assets, e.g., voltage and currents from transformers in substations, and can even remotely control parts of these assets.

In the past, such control was usually limited to substations or on-load tap changing transformers. With the increased expansion of distributed generation units and the integration of new types of consumers, more and more assets are directly connected to the SCADA system. Examples include distributed energy resources such as wind turbines or photovoltaic systems and intelligent new measurement systems such as Smart Meter Gateways (SMGWs) which may provide new sensory input for the SCADA systems, as well as new controllable consumers such as electrical vehicle charging stations or battery systems.

Based on this ICT infrastructure, we can deduce typical communication patterns and group them into typical use cases for different actors in the power system. Using the resulting use cases and communication patterns, we identify the following clusters of likely attack vectors:

Direct attack on SCADA system: An attacker attempts to directly manipulate the SCADA system itself to gain control over it, disable it, or provoke its malfunction.

Indirect attack on SCADA system: An attacker attempts to manipulate information to provoke wrong decisions in the SCADA system (e.g., using false data injection).

Attack on OT network: An attacker attempts to manipulate or impede functionalities of active OT network components (e.g., switches/routers), leading to malfunction or unavailability.

Attack on Remote Terminal Units (RTUs) and attached devices: An attacker attempts to manipulate RTUs to gain control over them, disable them, or provoke their malfunction.

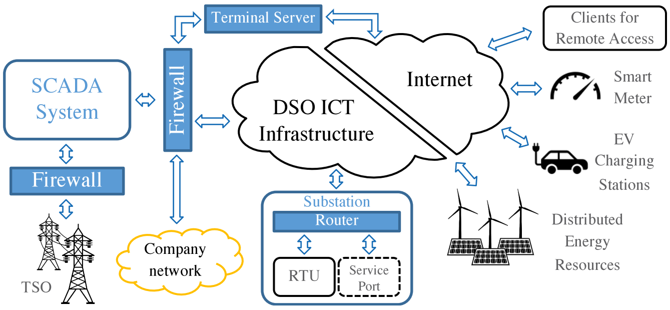

Fig. 1. In a future ICT infrastructure of a DSO, grid assets are connected to the SCADA system through dedicated infrastructure and/or the Internet.

Importantly, the inclusion of more and more intelligent assets into the ICT infrastructure results in the increase of possible attack vectors. In general, each interface to each asset is a potential attack vector, which could be used to compromise the OT network or the SCADA system. Furthermore, each asset for itself is a potential target, either to gain control over it, disable it or use it as a bridge-head for further attacks.

Our analysis of attack vectors in the ICT infrastructure of DSOs highlights the imperative need to support actors in the power system with methods to detect, prevent, and react to ICT attacks and failures. While certain attack vectors exhibit only little specifics to the energy sector and can thus be countered with traditional ICT security mechanisms [8], [9], a plethora of threats and risks specific to power systems needs to be accounted for. Our ongoing work on MEDIT targets specifically these threats and risks, striving for solutions that can practically be deployed in the ICT infrastructure of DSOs.

III. Research and Validation Environment

As MEDIT aims at the development of practically usable and deployable ICT security methods specifically for the power system domain, we require both an appropriate simulation environment and a distribution grid laboratory.

A. *ICT Energy Co-Simulation Environment*

Since both the behavior of the power system and the associated ICT network are relevant to develop and evaluate ICT security technology, an appropriate simulation environment has to map both domains and their interactions in a suitable level of detail. Complex interactions between ICT and the grid should be considered to examine and evaluate questions regarding the requirements of ICT used and repercussions on security of supply and system stability through ICT attacks or failures in a scalable and systematic manner [10]. To simulate attacks on ICT, special requirements are placed on the ICT simulation site. The main requirement is an explicit and extendable simulation of secondary equipment and their protocol-compliant communication as realistic as necessary. Furthermore, techniques used in ICT networks such as routing and packet switching must be simulated realistically to enable authentic attack simulation. In particular, the environment must enable the generation of extensive training data for an IDS. MEDIT evaluates different ICT simulators for their suitability.

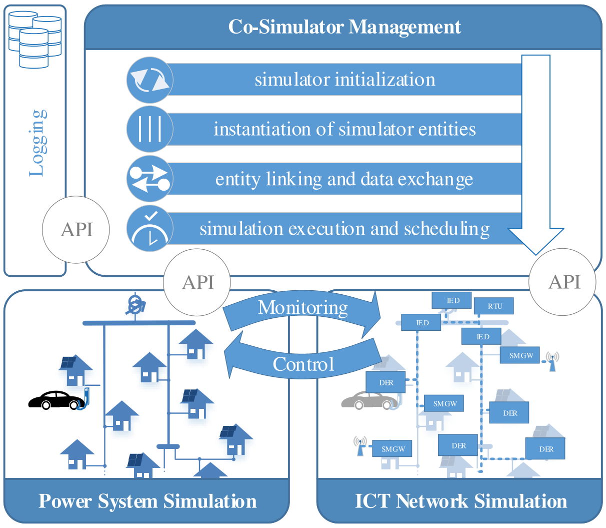

Fig. 2. MEDIT's co-simulation environment uses a co-simulation manager to interface with domain specific simulators for power systems and ICT.

Only through a realistic simulation, we can develop and train an IDS before validating it in a laboratory and finally deploying it in a real environment.

Co-simulation is a valid approach to couple simulators from different domains and model their interdependence. Different co-simulation standards, e.g., HLA [11] and FMI [12], as well as more specific frameworks, e.g., MOSAIK [13] and Ptolemy II [14], are available. Especially for the simulation of smart grids, co-simulation has already been investigated from different perspectives [15], [16]. For example, SGsim [17] uses OpenDSS for the power flow simulation and combines it with OMNeT++ [18] to simulate the ICT network.

While these standards and preliminary works provide valuable input for our work, we require a co-simulation that allows us to integrate the developed ICT monitoring and IDSs into the simulation environment and a protocol-compliant communication between components on the ICT site. Consequently, we use the approach of co-simulation to couple suitable, independent simulation environments for our purposes.

The concept of our environment is shown in Figure 2. To create uniform interfaces between the domain specific simulators, MOSAIK [13] will be used as a co-simulation manager. For the simulation of power systems, static simulations based on PANDAPOWER [19] as well as dynamic simulations for examination of power system stability based on MATPAT [20] are integrated into the co-simulation environment. Here, we will focus on detailed modeling of medium and subordinate low-voltage grids with a high number of distributed resources.

Based on primary technology used in the power grid, communication processes and technologies as well as generated data flows are modeled via standardized protocols such as IEC 60870-5-104 and IEC 61850 to generate real process data traffic. The environment functionally maps the complete communication chain between the operational layer, station layer, and the field layer for DSOs. This includes modeling RTU functionality for aggregation and protocol conversion of process data and modeling of intelligent electronic device functionality as links to primary technology, locally implementing control and monitoring capability. This at the same time represents the logical interface between power grid simulation and network simulation. In addition, we also cover the influence of other actors on grid operation, e.g., by VPPs operators through the simultaneous control of grid resources.

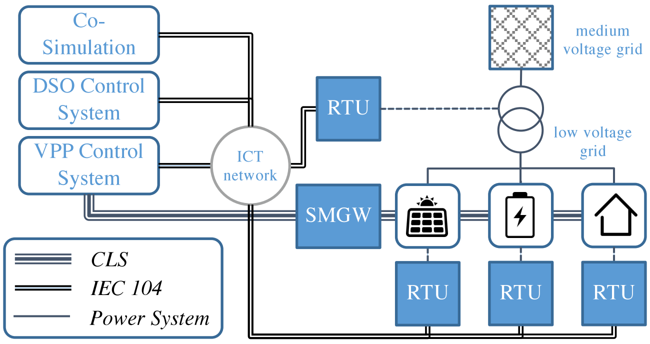

Fig. 3. A 10 kV distribution grid laboratory is extended with ICT infrastructure to represent the whole cyber-physical system of distribution grids.

By mapping real process data traffic in the simulation, it will also be possible to link the simulation with real control systems and real secondary equipment of the actors under consideration within our distribution grid laboratory. Thus, the simulation can be used for scaling the emerging process data traffic within a real environment as described in the following.

B. Distribution Grid Laboratory

Even if the simulation thus approximates reality, the integration of the developed technologies in a real laboratory for validation purposes is used to evaluate the integrability into real power systems. In particular, more complex systems such as a SMGW infrastructure cannot be completely represented in a simulation in accordance with reality and are therefore set up in the laboratory environment, which is utilized as one essential part of MEDIT's research and validation environment.

The laboratory at RWTH Aachen University consists of a medium/low voltage distribution grid including four distribution substations (10 kV/400 V), several distributed generation units (e.g., battery storage systems (15 kVA-100 kVA), photovoltaic inverters (10 kVA-36 kVA), and an 50 kW combined heat and power emulator), loads, secondary equipment and measurement devices, that can be interconnected flexibly. As shown in Figure 3, our existing laboratory is extended by the required ICT infrastructure to depict the whole cyber-physical system of the distribution grid, including ICT and relevant processes of the different power system actors (e.g., DSO and VPP operators). Our focus is on providing an infrastructure as close as possible to the reality. Therefore, the laboratory extension is conducted in accordance with the requirements of DSOs and VPPs operators.

Via secondary equipment and ICT, the assets are connected to a local distribution grid control system using the IEC 60870-5-104 protocol. Additionally, they are also connected to a VPP control system provided in the cloud using the IEC 60870-

5-104 protocol and the Controllable Local System (CLS) interface of the SMGWs. Suitable data points are defined for each asset and thus realistic process data traffic (control signals, measuring signals, status signals) will be generated, sent, and processed. Since the laboratory cannot provide an unlimited number of (physical) assets, it will be linked with the co-simulation environment in the ICT-domain to enable the generation of artificial yet validated data traffic to be sent to the control systems to demonstrate scalability. Consequently, the distribution grid laboratory is used to show the impact of cyber attacks on the ICT and on primary equipment as well as to validate the artificially generated data traffic and the developed tools for prevention, detection, and reaction.

IV. PREVENT AND DETECT ICT FAILURES AND ATTACKS

MEDIT's methods to prevent and detect ICT failures and attacks particularly focus on suitable solutions for ICT monitoring and intrusion detection for power system actors.

A. ICT Monitoring System for Distribution Grids

ICT monitoring primarily serves to record and monitor parameters and status of technical systems. This makes it possible to detect, visualize, and react to malfunctions based on data from different sources. In power systems, malfunctions and disturbances can increasingly no longer be attributed to primary technology alone. Indeed, current events indicate that errors may increasingly occur on the IT and OT side [5]. As corresponding monitoring at ICT level is not yet fully implemented in practice, there is a risk that ICT-caused malfunction cannot be adequately attributed, leading to a "blind spot" [21]. To ensure reliable fault diagnosis, complex on-site procedures are therefore required. This can endanger network availability and system security, resulting in higher downtime [22].

To address this issue, MEDIT will develop an ICT monitoring system that identifies ICT error sources. Currently, DSOs use different suppliers for ICT components to ensure independent and reliable grid operation. Ensuring independence from manufacturers is reasonable, but complicates data collection for monitoring. Consequently, MEDIT has to evaluate existing monitoring protocols for their applicability. Based on this, a suitable monitoring solution has to be implemented and integrated. This involves working with existing data sources or data sources that can be made available with little effort.

The monitoring system should serve as a troubleshooting reference point for control center personnel without deeper ICT expertise. Thus, personnel can recognize whether a disturbance of the ICT infrastructure or of primary equipment is present. As a more advanced concept, security monitoring could trace the current status of devices more closely with regard to ICT security. Technologies such as hardware security modules can be used to better measure the security state. Our approach provides a solution for the current need, but also shows the advantages of extended monitoring. Power system actors can thus find a sweet spot of costs and benefits in terms of monitoring and continuously adjust their strategy.

B. Intrusion Detection System for Electrical Process Data

Coordinated ICT attacks on power system actors have a high threat potential. In ICT networks, using IDSs is a state of the art method to timely detect the active intrusion of third parties into the ICT infrastructure and thus enable countermeasures [23]. IDSs can be classified on the basis of used detection methods (signature/anomaly/specification-based), deployments (host/network), used information (network/protocol/process data), and inclusion of history (stateless/state-oriented) [24]. In contrast to office IT, process networks in the power system domain have a less heterogeneous structure. This results in a comparatively low number of different device types and applications and longer life span of devices, which allows MEDIT to specifically focus on power system specific communication protocols such as IEC 60870-5-104. Endpoints in these ICT networks fulfill a clearly defined purpose and are therefore limited to a known set of commands as well as communicate only with explicitly and upfront determined entities, which eases the specification of network compliant behavior [25].

To detect intrusions on the protocol layer, MEDIT will improve upon the protocol whitelisting approach [26], a three-step approach following the principle of security in depth based on (i) access-control detection, (ii) protocol whitelisting detection, and (iii) model-based detection. Within the ICT, we require network borders that define physical units, e.g., substations. Then, the goal of protocol whitelisting is to detect attacks that (i) connect to a substation network, (ii) send or manipulate RTU traffic, or (iii) scan the network.

For access-control detection, our IDS needs to monitor existing network participants on the OSI Layers 2-4. Protocol whitelisting detection monitors which protocols are used between endpoints in the network, while a deeper protocol analysis is performed by model-based detection. To perform protocol whitelisting, the IDS needs to know the network configuration and allowed communication patterns. MEDIT will propose a solution for the IDS whitelisting approach for power system specific protocols [26].

Furthermore, we will investigate to which extent anomalies in the area of grid operation can be evaluated as indicators of successful attacks on compromised areas of secondary and control technology. Examples are switching commands or setpoint adjustments that have led to a traceable blackout. Faulty measured values or messages identified by bad data detection as well as implausible load, generation and substation behavior and limit violations could also serve as indicators [27]. Attacks on the parametrization and integrity of the process data are therefore mapped in advance in the co-simulation and detected by a distributed network-based intrusion detection system. On the basis of stochastic methods and graph-based machine learning methods, e.g., GraphSAGE [28], these indicators and alarms from signature-based and whitelist methods can be correlated and the attack scenario can be reconstructed topologically and chronologically. The result of this correlation is an assessment of the state of compromising for individual OT and ICT devices as decision support for business continuity.

V. REACT TO ICT SECURITY INCIDENTS

To support and prepare actors in the electric power system to react to ICT security incidents, MEDIT provides them with both, actionable incident response guidelines and a realistic simulation environment for security training.

A. *Actionable Incident Response Guidelines*

Reacting to cyber incidents and ICT failures does not only require tools but also operational guidelines with clear recommendations for actions. However, most guidelines in place (to comply with different security standards, e.g., ISO 27001 [29] or the German bill on IT security [30]) are mainly concerned with organizational measures, specifying who must be informed and what organizational processes should be carried out. Clear and specific instructions on technical levels are generally not provided. With MEDIT, we want to fill this gap by providing *actionable incident response guidelines*.

The goal of our guidelines is to provide distinct and precise actions for all employees who potentially have to deal with a ICT failure or cyber attack - especially those with no background in ICT, such as control center personnel. As illustrated in Figure 4, our core idea is to describe observations from employees' point of view. Based on each observation, different actions are proposed, which then can lead to new observations, providing a starting point for the next iteration.

To demonstrate our approach, we provide a brief example: We consider an operator, who detects implausible measurement in the SCADA system. The operator uses this initial observation as entry point for the work with our guidelines. To enable fast lookup of relevant instructions in the guidelines, all observations are categorized and indexed. In this example, the corresponding proposed action is to try to identify the source of the implausible measurements, enlisting other technicians if necessary. After performing the necessary steps, the operator (in our example) derives as new observation that one distinct RTU is the source of the implausible measurements.

Looking up this new observation in the guidelines, the operator is instructed to inspect this RTU's logfiles and configurations. In our example, the operator concludes that the RTU configuration was altered and unscheduled maintenance access was logged, potentially constituting a cyber security incident. Consequently, the information security manager and other stakeholders defined in the company's existing incident response guideline have to be informed and the correspondingly defined process has to be triggered.

Currently, our actionable incident response guidelines mainly focus on DSOs and VPPs. However, we are continuously extending these guidelines, by adding new observations, actions, and operators. The usefulness and practicability of our guidelines is evaluated in different workshops with DSOs, cyber security experts, and relevant stakeholders.

B. *Simulation Environment for Security Training*

Besides having actionable incident response guidelines, those responsible for adequately narrowing down and responding to failures and attacks within the ICT infrastructure of power systems require proper training of incident response measures. To facilitate such security training, we require an environment in which cyber attacks on the ICT infrastructure of power systems as well as as corresponding detective and responsive measures can be simulated.

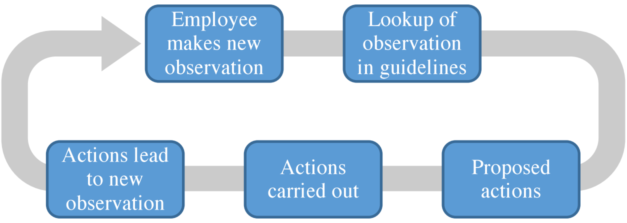

Fig. 4. Our actionable incident response guidelines support employees in reacting to ICT security incidents through an iterative observation/action cycle.

In the past, different frameworks for the simulation of cyber attacks on ICT infrastructure have been developed to facilitate research and training in security incident response, attack detection methods, and awareness [31]. E.g., SECPSIM [32] provides a training simulator for power system infrastructure security based on mathematical modeling. From a different perspective, BREACH [33] simulates a small company network, including legitimate user behavior and cyber attacks against the company, to facilitate incident response research and training. Contrary, the SWaT Security Showdown [34] is a capture-the-flag-like security training environment realized on top of the MiniCPS simulator for cyber-physical networks. While providing a general good starting point for realizing a simulation environment for security training for the ICT infrastructure of distribution grids, these existing approaches either do not consider the specifics of power systems or lack a realistic simulation of the ICT infrastructure.

Thus, MEDIT will provide a simulation environment for security training specifically tailored to the training for reactions to ICT security incidents within the ICT infrastructure of electrical power systems. To this end, we couple an existing framework for the simulation of company networks [33] with both an ICT/energy co-simulation environment (cf. Section III-A) and a realistic distribution network laboratory (cf. Section III-B). To this end, we will connect these networks with virtual network interfaces (TUN/TAP). We can selectively insert virtual networking components, e.g., firewalls, routers, or IDSs (cf. Section IV-B), thus modeling realistic ICT infrastructure (cf. Section II). To connect to real world components, e.g., within our distribution grid laboratory (cf. Section III-B), the virtual network interfaces can be bridged to physical interfaces, thus realizing hybrid training environments. In this setting, we can control which traffic may flow between company and OT network, down to individual RTUs.

This training environment will allow training operators to run a variety of attacks, covering the different attack vectors (cf. Section II). To explore the network or exfiltrate information, they can run network scans or copy network traffic to their own machines. Other attacks may send rogue control commands to RTUs, causing them to malfunction or even destabilize the power system. In the most mischievous case, attacks may manipulate critical components while simultaneously falsifying sensor readings as cover-up.

By coupling the different components of MEDIT, our training environment will provide trainees with a unique opportunity, as we can run attacks that specifically target power systems in an appropriate and realistic environment.

VI. CONCLUSION

Fundamental changes in power supply lead to an increased deployment of ICT and interdependencies between primary grid operation and ICT across all power system actors. Consequently, ICT becomes an increasing target for attacks and failures that can have serious impact on supply security and system stability. To counter this threat, existing ICT security measures must be enhanced with an anomaly monitoring as well as fast and actionable responses to potential incidents.

In this paper, we presented MEDIT, a comprehensive collection of methods to prevent, detect, and react to ICT attacks and failures for various actors in electrical power systems. As a foundation of our work, we reported on our research and validation environment, including an ICT energy co-simulation environment as well as a distribution grid laboratory. These two components can be flexibly coupled to assess the impact of ICT attacks and failures as well as to validate the developed methods for prevention, detection, and reaction. To prevent ICT failures and attacks, we presented an approach for an ICT monitoring system for distribution grids that allows to observe the status of assets more closely with regard to ICT security. Based on this, our IDS for electrical process data envisions to detect anomalies in the area of grid operation as indicators of successful attacks on or failures of IT and OT technology. To support actors in electrical power systems in reacting to ICT security incidents, we presented our approach to provide actionable incident response guidelines as well as a realistic training environment for ICT security.

Currently, we are working on fully implementing the methods underlying our vision of MEDIT. This includes creating an ICT energy co-simulation designed to study ICT security, extending our distribution grid laboratory with ICT, implementing our methods of ICT monitoring for distribution grids and intrusion detection for electrical process data, crafting actionable incident response guidelines, as well as integrating a simulation environment for security training within our research and validation environment. The developed methods will be validated in simulation and prototypical deployment using our research and validation environment as well as discussed and refined in workshops with DSOs, cyber security experts, and relevant stakeholders. Our perspective is to apply our methods and solutions practically in the actual ICT infrastructure of the mentioned actors and thus provide important building blocks for securing power systems against the increasing risk of ICT attacks and failures.

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

REFERENCES

[1] B. Panajotovic *et al.*, “ICT and Smart Grid,” in *TELSIKS*, 2011.
[2] R. Santodomingo *et al.*, “SGAM-based Methodology to Analyse Smart Grid Solutions in DISCERN European Research Project,” in *IEEE ENERGYCON*, 2014.
[3] P. McKeever and A. Monti, “Bottom-up approach to Energy Services Platform,” in *IEEE ENERGYCON*, 2016.
[4] F. Skopik *et al.*, “Dealing with Advanced Persistent Threats in Smart Grid ICT Networks,” in *ISGT*, 2014.
[5] R. M. Lee *et al.*, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC, 2016.
[6] R. M. Lee *et al.*, “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations,” Dragos Whitepaper, 2017.
[7] C.-H. Genzel *et al.*, “IT-Security for Smart Grids in Germany: Threats, Countermeasures and Perspectives,” in *ECCWS*, 2017.
[8] M. Henze *et al.*, “Network Security and Privacy for Cyber-Physical Systems,” in *Security and Privacy in Cyber-Physical Systems*, 2017.
[9] L. Roepert *et al.*, “Assessing the Security of OPC UA Deployments,” in *ITG ITSec*, 2020.
[10] S. C. Müller *et al.*, “Interfacing Power System and ICT Simulators: Challenges, State-of-the-Art, and Case Studies,” in *IEEE Transactions on Smart Grid*, vol. 9, no. 1, 2018.
[11] “IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules,” IEEE Std 1516-2010, 2010.
[12] T. Blochwitz *et al.*, “Functional mockup interface 2.0: The standard for tool independent exchange of simulation models,” in *MODELICA*, 2012.
[13] C. Steinbrink *et al.*, “CPES Testing with mosaik: Co-Simulation Planning, Execution and Analysis,” *Applied Sciences*, vol. 9, no. 5, 2019.
[14] C. Ptolemaeus, “System Design, Modeling, and Simulation using Ptolemy II,” Ptolemy.org, 2014.
[15] C. Steinbrink *et al.*, “Future Perspectives of Co-Simulation in the SmartGrid Domain,” in *IEEE ENERGYCON*, 2018.
[16] M. Vogt *et al.*, “A survey and statistical analysis of smart grid co-simulations,” *Applied Energy*, vol. 222, 2018.
[17] A. Awad *et al.*, “SGsim: A Simulation Framework for Smart Grid Applications,” in *IEEE ENERGYCON*, 2014.
[18] A. Varga, “The OMNeT++ Discrete Event Simulation System,” in *ESM*, 2001.
[19] L. Thurner *et al.*, “Pandapower—An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems,” in *IEEE Transactions on Power Systems*, vol. 33, no. 6, 2018.
[20] A. Roehder *et al.*, “Transmission system stability assessment within an integrated grid development process,” *CIGRE Sci. & Eng.*, vol. 8, 2017.
[21] C.-H. Genzel *et al.*, “Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilungsnetzbetreiber,” 2017.
[22] C.-H. Genzel *et al.*, “Moderne Energieverteilnetze: Bedrohungen und Gegenmaßnahmen,” *D·A·CH Security*, 2017.
[23] K. Gorzelak *et al.*, “Proactive Detection of Network Security Incidents,” ENISA Report, 2011.
[24] B. Morin and L. Mé, “Intrusion detection and virology: an analysis of differences, similarities and complementariness,” *Journal in Computer Virology*, vol. 3, no. 1, 2007.
[25] M. Serror *et al.*, “Towards In-Network Security for Smart Homes,” in *IoT-SECFOR*, 2018.
[26] Y. Yang *et al.*, “Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security,” in *IEEE PES GM*, 2014.
[27] G. Constante *et al.*, “Semantic-based detection architectures against monitoring-control attacks in power grids,” in *IEEE SmartGridComm*, 2019.
[28] W. L. Hamilton *et al.*, “Inductive Representation Learning on Large Graphs,” arXiv preprint arXiv:1706.02216 [cs.SI], 2017.
[29] “Information technology – Security techniques – Information security management systems – Requirements,” ISO/IEC 27001, 2017.
[30] German Bundestag, “Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz),” 2015.
[31] L. Topham *et al.*, “Cyber Security Teaching and Learning Laboratories: A Survey,” *Information & Security*, vol. 35, no. 1, 2016.
[32] C. Vellaithurai *et al.*, “SECPSIM: A Training Simulator for Cyber-Power Infrastructure Security,” in *IEEE SmartGridComm*, 2013.
[33] R. Uetz *et al.*, “BREACH: A Framework for the Simulation of Cyber Attacks on Company’s Networks,” in *DFRWS EU*, 2017.
[34] D. Antonioli *et al.*, “Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3,” in *ACM CPS-SPC*, 2017.