Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research

Ghada Elbez
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
ghada.elbez@kit.edu

Gustavo Sánchez
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
sanchez@kit.edu

Sine Canbolat
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
sine.canbolat@kit.edu

Sophie Corallo
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
sophie.corallo@kit.edu

Clemens Fruböse
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
clemens.fruebose@kit.edu

Florian Lanzinger
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
florian.lanzinger@kit.edu

Nicolai Kellerer
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
nicolai.kellerer@kit.edu

Gustav Keppler
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
gustav.keppler@kit.edu

Felix Neumeister
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
felix.neumeister@kit.edu

Bernhard Beckert
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
bernhard.beckert@kit.edu

Anne Koziolek
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
anne.koziolek@kit.edu

Martina Zitterbart
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
martina.zitterbart@kit.edu

Veit Hagenmeyer
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
veit.hagenmeyer@kit.edu

Abstract

The increasing reliance of power grids on information and communication technologies has exposed them to sophisticated cyber threats. This paper introduces a dedicated cybersecurity testbed for energy systems, emphasizing key insights and lessons learned from our practical evaluations. By integrating a tailored threat model with focused experimental scenarios, we investigate specific attack vectors and assess the resilience of energy infrastructures under realistic conditions. Our work streamlines interdisciplinary approaches—drawing on software-defined networking, intrusion detection, and risk assessment—to deliver clear, actionable strategies for enhancing grid security testing. The results underscore novel, empirically validated methods that balance theoretical rigor with practical applicability, advancing the protection of critical energy systems.

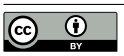
CCS Concepts

• **Security and privacy**; • **Hardware** → **Power and energy**;

Keywords

Security, Smart Grid, testbed, IEC 61850.

ACM Reference Format:
Ghada Elbez, Gustavo Sánchez, Sine Canbolat, Sophie Corallo, Clemens Fruböse, Florian Lanzinger, Nicolai Kellerer, Gustav Keppler, Felix Neumeister, Bernhard Beckert, Anne Koziolek, Martina Zitterbart, and Veit Hagenmeyer. 2025. Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research. In *The 16th ACM International Conference on Future and Sustainable Energy Systems (E-ENERGY '25), June 17–20, 2025, Rotterdam, Netherlands.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3679240.3734649



E-ENERGY '25, Rotterdam, Netherlands

ACM ISBN 979-8-4007-1125-1/25/06
https://doi.org/10.1145/3679240.3734649

1 Introduction

Modern energy systems are increasingly interlinked with Information and Communications Technology (ICT), a factor that, while

enhancing efficiency, also introduces new vulnerabilities and cyber threats [9, 17]. In response, we have established a specialized cybersecurity testbed designed to yield practical insights from real-world scenarios. This facility enables interdisciplinary research that not only investigates targeted threat vectors and resilience strategies, but also bridges diverse approaches from control system engineering to cybersecurity analytics.

The primary motivation behind our testbed is to create a realistic yet controlled environment where novel security approaches can be evaluated and refined. By simulating operational dynamics that closely mirror those of actual power grids, our lab supports focused experimental use cases that are directly transferable to real-world applications. This approach facilitates the generation of valuable data and actionable insights, which are critical for advancing the state of cybersecurity in energy systems.

Our work in the testbed has already uncovered important lessons regarding the integration of advanced remote access solutions and the application of Software-Defined Networking (SDN) within energy infrastructures. These findings have not only enhanced our understanding of specific attack vectors and resilience mechanisms but have also highlighted the importance of reducing overly technical details in favor of clear, research-driven insights. Such a focus fosters an environment where interdisciplinary collaboration can thrive, ultimately contributing to the broader cybersecurity research community.

Our contributions are:

- A clear presentation of the testbed architecture that prioritizes practical insights and lessons learned from realistic experimental setups, emphasizing targeted threat models and resilience strategies.
- A discussion of current research initiatives, showcasing preliminary results that inform both the strengths and challenges observed in securing energy systems.
- An exposition of how interdisciplinary research, aligned with the NIST Cybersecurity Framework, can be effectively integrated into a unified testbed environment to drive innovative cybersecurity solutions.

The remainder of the paper is organized as follows: Section 2 details the lab's infrastructure and capabilities. Section 3 outlines the research initiatives and key experimental findings. Section 4 examines the interdisciplinary aspects and connections to the NIST Cybersecurity Framework. Further lessons learned and future research directions are discussed in Section 5, and conclusions are provided in Section 6.

2 Security Lab Energy

In this section, we give an overview of our lab's architecture.

2.1 Description of the Lab Structure

The lab has three subsystems: Subsystem 1 for distributed generation, Subsystem 2 for a digital substation based on IEC 61850, and a SDN Subsystem connecting the two.

- **Subsystem 1**, shown in Figure 1, represents a distributed generation environment that has a homogeneous structure mainly consisting of Siemens devices. It uses a Hardware-in-the-Loop (HIL) approach with simulated power plants.

Table 1: Comparison of different recent Smart Grid (SG) testbeds for cybersecurity research (from years 2014 to 2024).

Testbed	Year	Protocols	Architecture	Applications
[4]	2014	• IEC 61850 (MMS, GOOSE, SV) • UDP	HIL	Distribution
[15]	2015	• IEC 61850 (MMS) • DNP3 • Modbus TCP	HIL	Distribution
[3]	2015	• DNP3 • TCP/IP • IEEE C37.118	HIL	Generation Transmission
[10]	2016	• IEC 61850 (MMS) • IEC 60870-5-104	Simulation	Transmission
[25]	2017	• Modbus TCP • DNP3 • other OT Prot.	HIL	Distribution
[23]	2018	• IEC 61850 (GOOSE, SV) • IEC 60870-5-104	HIL	Generation
[2]	2018	• IEC 61850 (MMS, GOOSE) • Modbus TCP	Hardware	Generation Transmission Consumer Storage
[14]	2018	• Modbus TCP	HIL	Distribution Storage
[20]	2019	• IEC 61850 (GOOSE) • DNP3 • IEEE C37.118.1a • NTP v.4	HIL	Distribution Transmission
[11]	2019	• TCP/IP	Simulation	Generation Consumer
[5]	2020	• IEC 61850 (MMS, GOOSE) • DNP3 • IEEE C37.118.2	HIL	Transmission
[22]	2022	• IEC 61850 (MMS, GOOSE)	HIL	Distribution
[12]	2022	• IEC 61850 (MMS, GOOSE) • MQTT	Simulation	Generation Transmission Consumer
Our Lab	2025	• IEC 61850 (MMS, GOOSE, SV) • IEC 60870-5-104 • Modbus TCP • PTP • NTP v.4	HIL	Generation Distribution Transmission Storage Consumer

- **Subsystem 2**, shown in Figure 2, represents a digital substation that has a heterogeneous structure consisting of components from different manufacturers. Here, we can conduct research on the interoperability of these components based on IEC 61850.
- **SDN Subsystem**, shown in Figure 5, connects Subsystems 1 and 2, where the control center in Subsystem 1 is the remote Supervisory Control and Data Acquisition (SCADA) for Subsystem 2.

Our lab focuses on the secondary side of the grid. Thus, Subsystem 1 contains simplified models for simulations. Power-plant manufacturers typically rely on subcontractors for Packed Units (PUs), which can be accessed remotely, posing potential vulnerabilities. We simulate this remote access in our lab but exclude PUs and subcontractor access. For cost efficiency, Subsystem 1 includes only one protection relay per power plant, unlike a real power plant, which would feature multiple relays for both the generator

and transformer station. In Subsystem 1, protection relays connect to analog amplifiers, while in Subsystem 2, Merging Units (MUs) convert analog values to Sampled Values (SV) packets for the relays, allowing us to explore both operational modes in the lab.

Uniqueness of Subsystem 1. The testbed features three power plants seamlessly integrated with the T3000 SCADA system over IPsec. Each plant employs a distinct type of Remote Terminal Unit (RTU), providing a realistic control center. Analog signals are generated by a real-time simulator, enhancing the authenticity of the lab. Additionally, the network is organized into VLANs—ensuring adherence to security guidelines and further emphasizing the subsystem uniqueness

Uniqueness of Subsystem 2. The lab is unique in its complexity due to a multivendor setup using real-world equipment and comprehensive integration of IEC 61850 standard. This enables interoperability investigations and the study of digital substation cybersecurity in a holistic network protocol environment.

Discussion. Our lab consists of three subsystems that balance real-setup with research flexibility, utilizing a multi-vendor HIL approach. Its primary advantage is its broad research scope; unlike many testbeds that focus on specific aspects (see Table 1), ours examines interactions among transmission, distribution, and communication networks. This enables us to assess the impacts of attacks on one or several subsystems, thereby investigating emergent effects within the increasingly complex and heterogeneous energy grid, for cybersecurity studies. However, our lab presents certain limitations that we consider relevant to share with the research community: Its construction and maintenance are resource-intensive, compounded by the rapid evolution of cybersecurity requirements, requiring continuous updates. To face these challenges, our adaptable research roadmap responds to such changes, and our interdisciplinary approach fosters large-scale collaboration among projects to optimize resource sharing. Furthermore, navigating complex energy regulations complicates lab operations and may restrict research. Our involvement in standardization committees helps address these challenges. As another limitation, research on inverter firmware in renewable energy plants is currently unfeasible due to the absence of physical power plants; however, it represents a potential direction for future investigation.

3 Conducted and Planned Research

Our cybersecurity efforts are divided into four Research Areas (RAs): VAS (Vulnerability Analysis in Software, PLCs, etc.) identifies threats via vulnerability assessment and security verification; SNPCS (Securing Network Protocols) focuses on network security and SDN integration; IDPC (Intrusion Detection and Prevention Concepts) designs IDS for protocols like IEC 61850 and IEC 60870-5-104; RAQ (Risk Analysis and Quantification) performs risk assessments to enhance alarm correlation. We describe each of these RAs:

Vulnerability Analysis in Software, O.S. of PLCs and Other Energy Control Components (VAS). Secure software development for critical infrastructure needs early and ongoing vulnerability detection [21], so we create methods based on Large Language Models (LLMs) to automatically identify and verify security requirements in software subsystems. To validate these methods, we apply them to the BelayBox of an Electric Vehicle (EV) charging station based on the EVerest framework shown in Figure 1.

Takeaways (VAS). Our existing work demonstrates the feasibility and usefulness of eliciting and analyzing requirements in all stages of software development. Thus, we are currently focusing on developing an automated threat modeling scheme.

Securing Network Protocols and Communication Structure (SNPCS). The shift to Distributed Energy Systems (DERs) poses challenges for SGs, requiring rapid coordination of numerous generators and consumers due to increased volatility. A reliable communication backbone is essential. We consider SDN suitable for this purpose [19] and aim to develop mechanisms to secure such networks. We also explore the applicability of different security standards in the energy domain, analyzing their impact in our lab infrastructure to provide insights into procedural, functional, and technical standards.

Takeaways (SNPCS). Our existing work we identified advantages SDN can bring to SG as well as the necessity to deploy specific security standards and recommendations. In our current work, we plan to further fine tune our solutions and further investigate their advantages and disadvantages.

Intrusion Detection and Prevention Concepts (IDPC). This research aims to create a robust Hybrid Intrusion Detection System (HIDS) that enhances detection accuracy and minimizes false alarms by analyzing physical, power, and cyber activities [16, 24]. It establishes a normal behavior baseline to identify anomalies and integrates various techniques to defend against attacks on control centers, SCADA systems, and distributed energy resources, ensuring secure connections using energy-standard protocols.

Takeaways (IDPC). Our existing work has demonstrated proof-of-concept implementations of ML-based IDSs and evaluated their robustness to specific adversarial attacks. Our current work focuses on developing a HIDS that integrates physical, power, and cyber data to improve detection while being robust.

Risk Analysis and Quantification/Qualifications (RAQ). Risk assessment is crucial for distributed generation and IEC 61850 substation testbeds due to their complexity [6], thus we aim at integrating it to Security Information and Event Management (SIEM) systems to enhance cybersecurity and counter attacks. SIEM solutions' risk analysis features are often rated as basic or average, highlighting a need for enhancement [8]. Our prior vulnerability assessment [7] will help us experimentally further evaluate the impact of attacks, such as time synchronization attacks, in the other Subsystems.

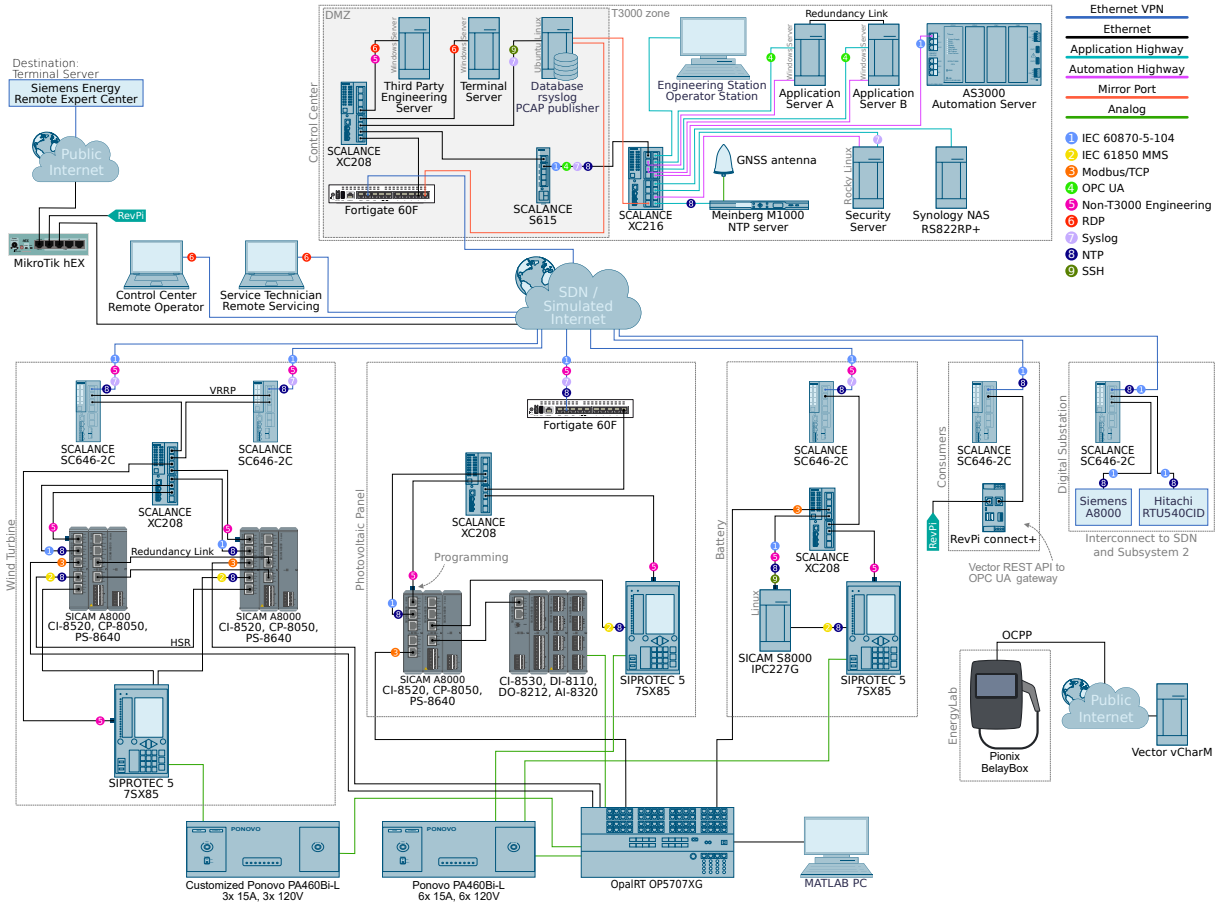


Figure 1: Overview of Subsystem 1 with connection to Subsystem 2 and SDN.

Takeaways (RAQ). Our existing published work has shown systematic approaches to risk assessment in the energy domain. Our current work expands the attack surface while investigating the impacts to achieve a comprehensive risk quantification method, focusing on integrating this into a SIEM system.

4 Interdisciplinarity as a Key Lesson Learned

Building a lab infrastructure for research in cybersecurity in energy systems involves various challenges and learning opportunities. One key lesson learned is interdisciplinary collaboration. In fact, cybersecurity in energy systems requires expertise from multiple domains, such as computer science and electrical engineering. Our aim through this initiative is to foster collaboration among experts from these fields in order to enhance research outcomes. Cybersecurity in energy systems requires addressing specific needs outlined in four RAs that align with broader standards and frameworks. This research aims at understanding cybersecurity risks and develop targeted solutions energy systems.

4.1 NIST Cybersecurity Framework (CSF)

The correlation of the research domains highlighted in Section 3 and Figure 3 with the NIST CSF "*National Institute of Standards and Technology - Cybersecurity Framework*" [1, 18] serves to ensure that ongoing research adheres to established industry standards. This systematic approach supports the identification and resolution of critical deficiencies within the framework's categories (*Identify*, *Protect*, *Detect*, *Respond*, *Recover*, and *Govern*) and offers a systematic means of organizing and integrating findings. This alignment enhances research relevance by prioritizing real-world applications, promoting interdisciplinary collaboration between researchers and industry stakeholders, and advancing organizational security. It also supports effective risk management and allows for evaluation of research against the framework's objectives. In NIST CSF, various cybersecurity domains are integrated as follows: During the *Identify* phase, vulnerability analysis is used to spot weaknesses in assets and systems. Moreover, threat modeling is utilized to determine potential threats and attack vectors. Finally, risk assessment is performed to prioritize protective measures and compliance, ensuring identification processes are aligned with regulatory requirements. The mapping between NIST CSF and RAs is illustrated in Table 2.

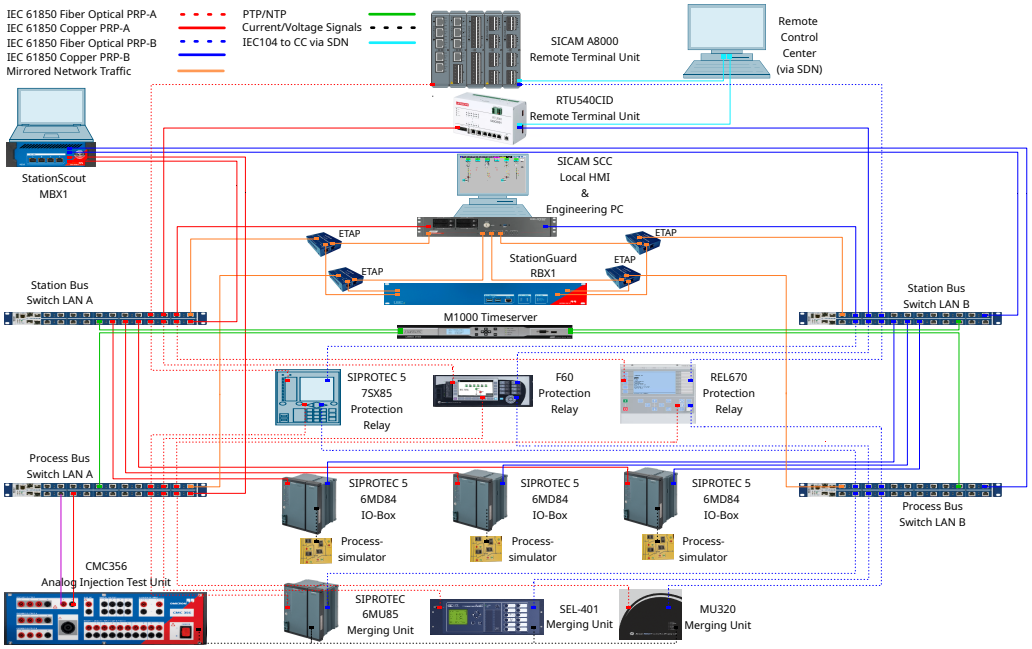


Figure 2: Overview of Subsystem 2 — a digital substation.

During the *Protect* phase, vulnerability analysis is crucial to implement controls to address identified weaknesses. At the same time, threat modeling guides the design of security controls to mitigate potential threats. SDN improves network security through flexible controls and configurations, and compliance ensures that protective measures adhere to regulatory standards. In the *Detect* phase, Intrusion Detection and Prevention Systems (IDPS) actively monitor and identify suspicious activities and potential threats, while SIEM aggregates and analyzes data to detect security incidents and anomalies. For the *Respond* phase, IDPS provides critical alerts and information for an effective incident response, and SIEM offers detailed logs and insights to manage and respond to incidents. In the *Recover* phase, compliance and standardization ensure that recovery processes meet regulatory requirements and incorporate lessons learned to improve future resilience. Finally, the *Govern* function focuses on structures and processes to manage cybersecurity risks.

4.2 Interdisciplinary Across Research Areas

In the context of security standards for energy systems, IDSs are discussed in relation to IEC 62351-6. Integrating standards' recommendations in the developed IDS solution is emphasized, along with bridging the gap between norms and practical applicability. Specific attack identification methods targeting energy protocols have already been proposed [13]. In section 3, the research aims to create adversarial attack-resistant IDSs while incorporating current security recommendations for energy protocols. By evaluating the response of ML-based IDSs to simulated threats, it identifies vulnerabilities and enhances resilience against future attacks. A risk assessment of adversarial attacks will also focus on specific areas in the lab such as 61850 protocols. The risk assessment aims to correlate known vulnerabilities in hardware systems to obtain a

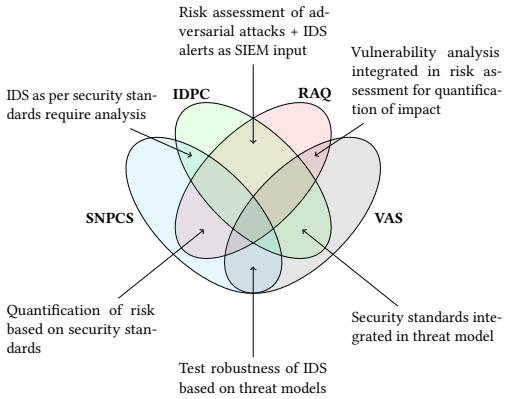


Figure 3: Venn diagram to represent interconnected RAs. Legend: Securing Network Protocols and Communication Structure (SNPCS), Vulnerability Analysis in Software, O.S. of PLCs and Other Energy Control Components (VAS), Intrusion Detection and Prevention Concepts (IDPC), Risk Analysis and Quantification/Qualification (RAQ).

comprehensive grid-wide risk assessment for specific types of hardware attacks. Vulnerability analysis uncovers unknown vulnerabilities in software by analyzing architecture, design assumptions, and software code. Software vulnerability assessments are crucial for understanding security risks in energy systems, alongside broader risk assessments. Network-based attack detection systems have limited detection rates since many attacks do not change communication patterns significantly. Traditional IDPS can be challenged

Table 2: Mapping of NIST CSF Functions to Security Measures.

NIST CSF	VAS	SNPCS	IDPC	RAQ
Identify	Vulnerability analysis in SW/HW, threat modeling	Protocol weaknesses identification, compliance with IEC 62351/62443	Analysis of cyber-physical threats in SCADA systems	Risk analysis and quantification of system-wide threats
Protect	Secure SW development based on risks	SDN-based mitigation	IDS development	Risk mitigation strategies
Detect	Formal methods for SW vulnerabilities	Monitoring network anomalies	Hybrid IDS for detecting anomalies	IDS integration into SIEM
Respond	N/A	Incident response via SDN reconfiguration	Automated response through IDS alerts	SIEM-based response and post-incident analysis
Recover	N/A	N/A	N/A	Resilience strategies and post-incident assessment
Govern	Govern informs how an organization will implement the other five Functions.			

with specific attacks like data injection, highlighting the need to develop HIDS to enhance effectiveness. Addressing these challenges necessitates a comprehensive understanding of both fields. The security recommendations explored in Section 3 for securing the network protocols and communication structure will be integrated into the threat modeling approach. Incorporating relevant security recommendations from the IEC 62351 and IEC 62443 standards into a comprehensive threat model aids in identifying potential vulnerabilities in the energy system and provides guidance on mitigation strategies, such as SDN techniques against DDoS attacks.

The Security Lab Energy facilitates research and experimentation at the intersection of various research domains. It enables simulation of real-world scenarios, fostering research into cybersecurity in energy systems through interdisciplinary collaboration including computer science, electrical engineering, and energy informatics. Partnerships with academia and industry, alongside a planned lab demonstrator, will facilitate exploration of security issues and future risks in energy systems.

5 Future Research Directions and Further Lessons Learned

In VAS research area, current investigations into inverter firmware for renewable energy plants face practical limitations due to the lack of physical power plants for experimentation. Nonetheless, this area presents a valuable opportunity for future research, emphasizing the need to explore inverter firmware development and its implications for enhancing the efficiency and reliability of renewable energy systems.

In SNPCS research area, our future work will focus on examining the applicability of security recommendations outlined in standards such as IEC 62351 and 62443. This research will be conducted in collaboration with industrial partners in controlled laboratory settings, facilitating the collection of empirical data. We intend to relay feedback to relevant standardization committees, thereby contributing to the enhancement of security protocols within the energy sector.

In IDPC research area, we aim to leverage network-based measurements alongside explicit feedback from supervisory control systems to improve detection performance and optimize the training processes of IDS. Additionally, future investigations will prioritize the exploration of problem-space adversarial attacks, particularly focusing on their implications within the framework of IEC 61850 protocols, enhancing the resilience of SG operations against emerging threats.

Finally, in research area RAQ, our future initiatives will strive to integrate the MITRE ATT&CK framework to bolster threat identification processes and develop a SIEM system specifically designed for energy infrastructure. This integration will allow for exposure to simulated threats, thus refining the threat model and fortifying the IDS against both current and potential sophisticated attacks in the future.

As a potential additional research area, our focus includes addressing security and privacy concerns within advanced metering infrastructure. Specifically, our goal is to mitigate cryptographic-related security issues such as chosen-message attacks and adaptive chosen-ciphertext attacks. Thus, we plan to develop lightweight cryptosystems. Furthermore, our future approach will also involve designing and implementing attribute-based access control for substations. This will enable role/rule-based lightweight and post-quantum secure malleable access control authentication, encryption, and signcryption techniques to address security concerns within substations and their associated protocols with the well-known real-time solid requirements. Together, these research directions collectively aim to enhance security, reliability, and resilience within the energy sytems. Besides the interdisciplinary collaboration, which is one of the key lessons learned from this initiative, we identify other important lessons as checkpoints for the research community:

- ✓ Establishing specific research goals/outcomes, identifying key areas of focus within cybersecurity for energy systems.
- ✓ Creating a realistic simulation and HIL setup that allows testing cybersecurity measures under real-world conditions.
- ✓ Implementing realistic case studies and simulating actual cyber attacks on energy systems to quantify their impact, understand vulnerabilities, and test responses.
- ✓ Ensuring the necessary physical and virtual infrastructure (including dedicated servers and secure networks) is available.
- ✓ Conducting regular assessments to schedule periodic checks of the infrastructure.

✓ Implementing mechanisms for continuous learning and skill sharing, as well as maintaining comprehensive documentation. We use a dedicated wiki to document technical specifications, experimental methodologies, and consolidate lessons learned.

✓ Involving energy stakeholders—including technology vendors and regulators—early in the planning phase to ensure the lab meets industry needs.

✓ Ensuring dedicated lab personnel are available to manage and run the infrastructure.

✓ Building an interdisciplinary team that includes cybersecurity experts, energy engineers, and policy specialists.

✓ Forming and fostering partnerships with academic institutions, standardization groups, national labs, and private industry to share knowledge, resources, and best practices.

✓ Encouraging experimentation and innovation by providing resources to explore further research topics and funding.

6 Conclusion

This work has presented an exploration of cybersecurity challenges within energy systems through the lens of our specialized testbed. By integrating targeted threat models with realistic experimental scenarios, we have gained valuable insights and learned lessons that extend beyond conventional technical details. Our interdisciplinary approach has paved the way for a clearer understanding of the vulnerabilities and resilience strategies necessary to safeguard the Smart Grid (SG). The design of the testbed, which emphasizes practical experimentation, has enabled us to identify actionable strategies that are directly transferable to real-world energy systems. Our findings not only demonstrate the potential of advanced methods such as Software-Defined Networking (SDN) and intrusion detection but also highlight the importance of collaboration across research disciplines and with industry partners. Looking forward, our vision is to further enhance cybersecurity for critical infrastructures by refining these insights into robust, deployable solutions. Future work will include the development of a demonstrator and the organization of cyber range exercises. We will extend our work through newly developed case studies as part of our planned future work.

Acknowledgments

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

References

[1] 2021. *Cybersecurity risk management: Mastering the fundamentals using the NIST cybersecurity framework.*
[2] Sridhar Adepu, Nandha Kumar Kandasamy, and Aditya Mathur. 2019. Epic: An electric power testbed for research and training in cyber physical systems security. In *ESORICS '18 Workshops*. Springer, 37–52.
[3] Hossein Ghassempour Aghamolki, Zhixin Miao, and Lingling Fan. 2015. A hardware-in-the-loop SCADA testbed. In *NAPS '15*. IEEE.
[4] Univ. Grenoble Alpes. 2014. G-ICS lab (GreEn-ER8 Industrial Control systems Sandbox). Accessed: 2024-06-05.
[5] Tamara Becejac, Crystal Eppinger, Aditya Ashok, Urmila Agrawal, and James O'Brien. 2020. Prime: a real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond. *IET Cyber-Physical Systems: Theory & Applications* 5, 2 (2020).
[6] Sine Canbolat, Ghada Elbez, and Veit Hagenmeyer. 2023. A new hybrid risk assessment process for cyber security design of smart grids using fuzzy analytic hierarchy processes. *at-Automatisierungstechnik* 71, 9 (2023).
[7] Sine Canbolat, Clemens Fruböse, Ghada Elbez, and Veit Hagenmeyer. 2024. Assessing GNSS Vulnerabilities in Smart Grids. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 545–555.
[8] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz. 2021. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors* 21, 14 (2021).
[9] Edward R Griffor, Christopher Greer, David A Wollman, and Martin J Burns. 2017. Framework for cyber-physical systems: Volume 2. (2017).
[10] Prageeth Gunathilaka, Daisuke Mashima, and Binbin Chen. 2016. Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions. In *CPSS '24*.
[11] Eman Hammad, Mellitus Ezeme, and Abdallah Farraj. 2019. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *International Journal of Electrical Power & Energy Systems* 104 (2019).
[12] Nandha Kumar Kandasamy, Sarad Venugopalan, Tin Kit Wong, and Nicholas Junming Leu. 2022. An electric power digital twin for cyber security testing, research and education. *Computers and Electrical Engineering* 101 (2022).
[13] Gustav Keppler, Andrea Bonetti, Sine Canbolat, Aneeqa Mumrez, Veit Hagenmeyer, and Ghada Elbez. 2024. Interoperability Assessment of IEC 61850 Devices in a Multivendor Digital Substation. In *GPECOM '24*.
[14] KIOS. 2018. *KIOS Testbeds for critical infrastructure systems.*
[15] Georgia Koutsandria, Reinhard Gentz, Mahdi Jamei, Anna Scaglione, Sean Peisert, and Chuck McParland. 2015. A real-time testbed environment for cyber-physical security on the power grid. In *CPS-SPC '15*.
[16] Aneeqa Mumrez, Gustavo Sánchez, Ghada Elbez, and Veit Hagenmeyer. 2023. On Evasion of Machine Learning-based Intrusion Detection in Smart Grids. In *SmartGridComm '23*. IEEE.
[17] Anand Narayan, Carsten Krueger, Andre Goering, Davood Babazadeh, Marie-Christin Harre, Bertram Wortelen, Andreas Luedtke, and Sebastian Lehnhoff. 2019. Towards future SCADA systems for ICT-reliant energy systems. In *ETG '19*. VDE.
[18] National Institute of Standards and Technology (NIST). 2022. *National Vulnerability Database, December 2022.* https://nvd.nist.gov/
[19] Felix Neumeister and Martina Zitterbart. 2022. The Smart Grid: A Use-Case for Large-Scale SDN Deployment. In *3. KuVS Fachgespräch "Network Softwarization"*.
[20] Ibukun Adesile Oyewumi. 2019. *ISAAC: The Idaho Cyber-physical System Smart Grid Cybersecurity Testbed.* University of Idaho.
[21] Sven Peldszus, Frederik Reiche, Kevin Hermann, Sophie Corallo, Thorsten Berger, and Robert Heinrich. 2024. Can I Check What I Designed? Mapping Security Design DSLs to Static Code Analyzers. to be published.
[22] Flavio Quizhpi-Palomeque, Freddy Jiménez, Pedro Rivera, Mateo Quizhpi-Cuesta, and Francisco Gómez-Juca. 2022. Implementation of an iec61850 virtual relay network in a protection laboratory. In *ROPEC '22*. IEEE.
[23] Stephan Ruhe, Steffen Nicolai, and Peter Bretschneider. 2018. Modelling and simulation of electrical phenomena in a real time test bench. In *UPEC '18*. IEEE.
[24] Gustavo Sánchez, Ghada Elbez, and Veit Hagenmeyer. 2024. Attacking Learning-based Models in Smart Grids: Current Challenges and New Frontiers. In *e-Energy '24*.
[25] Siddharth Sridhar, Aditya Ashok, Michael Mylrea, Seemita Pal, Mark Rice, and Sri Nikhil Gupta Gourisetti. 2017. A testbed environment for buildings-to-grid cyber resilience research and development. In *RWS '17*. IEEE.

A PLC Setup

The lab has evolved significantly to align with energy sector research, transitioning from a general PLC-based automation system to three specialized subsystems with tailored hardware and software. Further details on the lab's current structure are below. It is important to note that since the initial concept encompasses general automation components widely used in the industry; this configuration has been retained within the lab and will henceforth be referred to as the PLC setup, depicted in Figure 4.

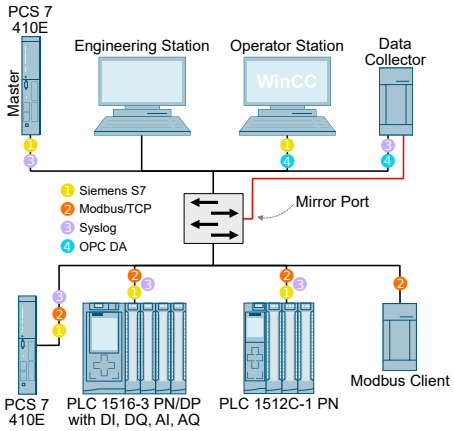


Figure 4: Overview of the PLC setup.

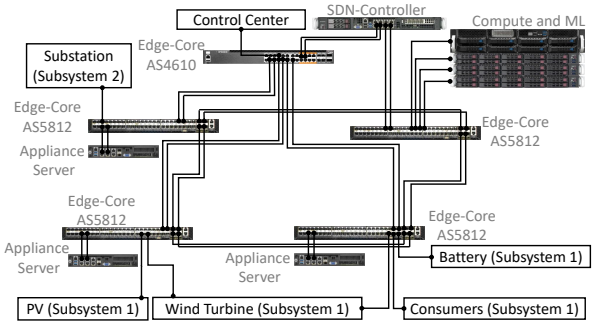


Figure 5: Overview of the SDN Network and its respective connections to the rest of the lab.

Uniqueness of PLC Setup. This lab setup represents a general automation systems with PLCs widely used in industry. It provides the opportunity to investigate the security of WinCC, the modbus TCP and the S7 protocols, and the PLC/PCS firmware.

B SDN Subsystem

The SDN Subsystem, depicted in Figure 5, serves as a connection between Subsystems 1 and 2, with the control center located in Subsystem 1 acting as the remote SCADA for Subsystem 2.

Uniqueness of SDN Subsystem. The SDN Subsystem aims to model and develop a highly resilient network. To achieve this, we created a unique testbed for a distributed, co-located SDN control plane that integrates real industrial components. We are not aware of any existing publications on similar systems in the realm of industrial SDN.