HydroLab: A Versatile Hydroelectric Power Lab for Security Research and Education

Sebastian Obermeier[1] [a], Giorgio Tresoldi[2] [b], Bernhard Tellenbach[2] [c] and Vincent Lenders[2] [d]

[1] *Hochschule Luzern Informatik, Campus Zug-Rotkreuz, Suurstoffi 1, 6343 Risch-Rotkreuz, Switzerland*

[2] *Cyber-Defence Campus, armasuisse Science and Technology, Feuerwerkerstrasse 39, 3603 Thun, Switzerland*

Keywords: Industrial Cyber Security, Substation Automation Systems, Cyber Security Testing Laboratory, Hydrolab.

Abstract: We present our experiences with designing, building and operating a lab for critical infrastructure consisting of a hydroelectric power plant for power generation and a substation automation system for the transfer of energy. The lab is unique in that it serves a double purpose, providing opportunities for both education and research. The paper outlines the architecture, hardware and software components of the lab and validates its effectiveness through classroom teaching and participation in two hackathons. The lab's ability to combine real-world applications with hands-on learning makes it an essential resource for students and researchers interested in critical infrastructure systems. The presented lab can aid in advancing the understanding and development of these systems for cyber security purposes.

1 INTRODUCTION

In order to make the national infrastructure more resilient, it is crucial for future engineers to receive education in cyber security and to conduct research on energy systems, especially on power generation and the automation of substations, which are responsible for the distribution of energy.

To enhance the learning experience and prepare students and professional engineers for real-world scenarios, we have designed and built a cyber security lab for critical infrastructure that can be used at the same time for education and research. The lab utilizes actual elements to simulate a hydroelectric power plant and a substation. This hands-on approach allows for a more practical and accurate understanding of the subject, as opposed to solely relying on simulated environments.

The main idea of the lab is to implement a modularized approach for cyber security controls within critical infrastructure environments. It has several components that resemble an end-to-end power scenario, ranging from power generation to transmission.

1.1 Contributions

Beyond a previous contribution (Obermeier et al., 2023), which focuses on recovery concepts for substation automation labs, the main contributions of this paper are:

- It presents the design, architecture and components for a novel cyber security focused energy lab that includes a hydroelectric and a substation automation system. The lab is built with real automation hardware and integrated by professional electrical engineers to ensure a maximum degree of realism.
- It shows which training scenarios and exercises have been integrated, including the setup of state-of-the-art intrusion detection systems as learning module.
- It evaluates the system through the use in two hackathons and through classroom lectures, thus showing the feasibility for both, education and research.

2 RELATED WORK

Lab approaches for education and research exist, e.g., (Holm et al., 2015) has conducted a meta study on in-

[a] https://orcid.org/0000-0003-2802-7427
[b] https://orcid.org/0000-0001-5148-6803
[c] https://orcid.org/0000-0002-5008-1107
[d] https://orcid.org/0000-0002-2289-3722

Obermeier, S., Tresoldi, G., Tellenbach, B. and Lenders, V.
HydroLab: A Versatile Hydroelectric Power Lab for Security Research and Education.
DOI: 10.5220/0012713800003767

In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024)*, pages 622-627
ISBN: 978-989-758-709-2; ISSN: 2184-7711

dustrial control system lab setups. (Frank et al., 2017) suggests a design life cycle concept for the creation and also maintenance of testbeds. Our evaluation confirms that maintenance should not be underestimated and resources should be planned.

In contrast to generic approaches like (Sauer et al., 2019), which has developed a low cost industrial testbed for research and education focusing on generic automation systems, our approach focuses on a real-world substation environment including real-world devices and software.

Another testlab is described in (Ruhe and Roesch, 2019), whereas (Rösch et al., 2020) is a movable extension to focus on cyber security aspects. However, the approach differs from our testlab as it is an all-in-one solution while our focus is on a modular approach.

A literature survey for critical infrastructure cyber training has been conducted by (Chowdhury and Gkioulos, 2021).

Concerning power systems, (Yang et al., 2015) presents an IEC 61850 based testbed for research purposes including cyber security tests. This testbed, however, does not include IEC 60870–5–104 communication towards a central SCADA system, which we have included in our lab. The investigation of (Yang et al., 2015) in 2015 revealed that several of the used Intelligent Electronic Device (IED)s exhibit vulnerabilities. This problem has not been completely solved until today - during a hackathon, we discovered three previously unknown vulnerabilities in our testbed of fully patched state-of-the-art IED.

In case of low budget, (Gunathilaka et al., 2016) has created a software-based smart grid testbed. However, our experiments show that the use of real-world hardware in testbeds is crucial, especially for cyber security research as the behavior of hardware under various attacks is difficult to assess and simulate.

The National Institute of Standards and Technology (NIST) recommends an industrial control system cyber security lab setup in (Candell et al., 2015). Their publication covers the lab setup and different scenarios which can be acted out on the proposed infrastructure.

3 DESIGN GOALS

The design goals of our energy laboratory are to create a mobile, miniaturized environment of a substation automation system that is realistic and extensible. The lab should be multi-purpose and capable of supporting multiple users simultaneously. One important aspect of the lab should be vulnerability research, allowing for the identification and analysis of potential weaknesses in the used energy systems. The lab should also be able to serve as a demonstration tool, showcasing the capabilities and features of various energy systems to decision makers and other stakeholders. To provide a comprehensive understanding of energy security, the lab should combine both, vulnerable components and the latest secure hardware and software, in order to allow users to find known weaknesses but also perform research on state-of-the-art systems.

Additionally, the lab should have automated recovery capabilities to ensure that it can quickly return to normal operation after any disruptions or attacks conducted by the users. Visual components, in our case a water tank, should demonstrate the results of successful attack scenarios that can be simulated within the lab. Overall, the energy laboratory should be designed to support a range of security awareness and training objectives, providing a valuable resource for engineers and decision makers working to secure energy systems.

4 LAB STRUCTURE

The lab consists of two parts, a Power **generation** system that is implemented through a hydroelectric power plant, and a Power **transmission** system that is implemented through a substation automation system.

While the Power generation part is a basic simulation environment with known security vulnerabilities, the Power transmission part, which is represented by the substation automation system, is a state-of-the-art system that is fully updated.

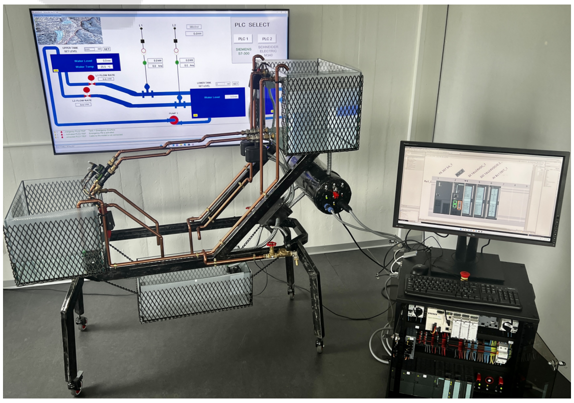

Figure 1: Picture of the hydro lab.

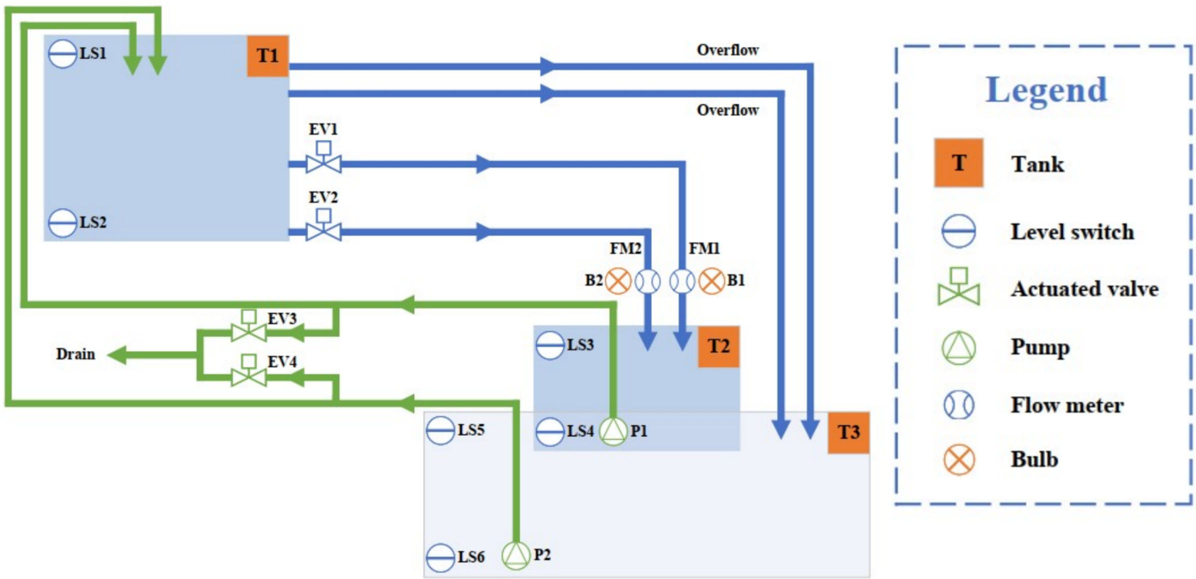

Figure 2: Schematics of the hydro lab.

4.1 Hydroelectric Power Plant

The hydroelectric part of the energy laboratory offers an introduction to Operational Technology (OT) and a picture is shown in Figure 1. It consists of a model of a hydroelectric power station where water is stored in a elevated reservoir. Upon release, the water travels through pipes, turns a turbine, and generates electricity. When excess energy is available, the water is pumped back up to the reservoir.

The physical setup using water tanks allows to experience the consequences of an attack, e.g. the overflowing of one of the water tanks.

The schematics are illustrated in Figure 2. The model includes three tanks which represent the lower (T2) and higher elevation reservoirs (T1) plus an overflow tank (T3).

The water in the higher reservoir can be released by two separate electric gate valves (EV1 & EV2). Water then flows to the lower tank (T2) through flowmeters (FM1 & FM2), which simulate the turbine through lighting bulbs (B1 & B2). The water can be pumped from the lower tank (and from the overflow tank) to the upper tank using a pumps (P1 & P2). Both tanks are equipped with level sensors (LS3 & LS5) to sense overflows. To avoid that water spills on the ground during cyber attacks, we have added separate overflow pipes.

4.1.1 Architecture

The overall architecture is illustrated in Figure 3. The sensors and actuators are connected to a Siemens S7-300 (PLC1 in the image) and a Schneider Electric Modicon M340 (PLC2) which are programmed with the same logic. Both PLCs are used to control two pumps that control the water flow. Both PLCs, as well as the engineering workstation (Engg), the HMI (based on Allen-Bradley FactoryTalk) and the substation automation system (SAS) are connected through a Siemens SCALANCE XB208 Network switch.

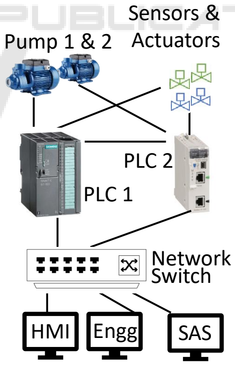

Figure 3: Hydro lab architecture.

The system is designed to support two distinct communication protocols to provide participants with an opportunity to experience diverse implementations while comprehending a single physical process. The used protocols are Modbus for the M340 PLC and S7comm for the S7-300.

The substation automation system (SAS) is connected through the network switch, as illustrated in the bottom right corner of Figure 3.

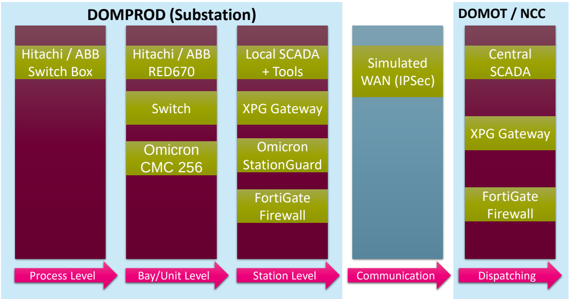

Figure 4: Conceptual Overview of the Substation System.

4.2 Substation Automation System

The goal of the substation automation system is to create a complex, realistic system that mimicks a real-world installation. It does not contain a physical visualization, but utilizes an accurate configuration and system. It is secure-by-design through the use of latest standards, firewalls, segmentation, IDS, etc. It involves recovery and reset options into defined states according to (Obermeier et al., 2023). Therefore, the system allows for reproducible, complex, and realistic exercises.

Figure 4 illustrates an overview of our substation system. The left blue box denotes the substation (DOMPROD), while the right box symbolizes the network control center (DOMOT/NCC). The left-most red box illustrates the process level, simulated through an ABB Switch Box, which is capable of replicating the states of circuit breakers, switchgears and other field components. The RED670 IED on Bay Level is employed for the protection, monitoring, and control of overhead lines and cables. The Omicron CMC256 is connected to the RED670 to simulate overcurrents, which may arise from lightning strikes on power lines. The managed switch, equipped with a monitoring port, mirrors all traffic to the Omicron StationGuard IDS on the station level. That level also accommodates the local SCADA system, as well as supplementary tools. The Fortigate Firewall safeguards the substation from the wide area communication network, which is simulated through IPSec as VPN technology. The counterpart symbolizes the network control center, inclusive of the central SCADA system.

4.2.1 Architecture

The lab network layout is illustrated in Figure 5. Each computer icon represents a virtual machine. The Omicron CMC 256 is not included in this figure because it is not connected to the network but directly to the IED.

While we have virtualized the IT hardware, the industrial components are bound to their dedicated hardware.

5 EVALUATION AND LESSONS-LEARNED

To evaluate the lab, we created two scenarios: a classroom setting and a hackathon experience. To answer the question whether it is possible to master a complex, multi-component technology, we have utilized lab exercises. To examine the extent to which participants are able to apply their knowledge independently and perform research, we have utilized a hackathon setting. Furthermore, we evaluated the potential of combining vulnerable components for early success (e.g. known vulnerabilities through the use of weak protocols) with more sophisticated state-of-the-art security challenges.

5.1 Evaluation in Classroom

The use of a substation laboratory in a classroom setting allows students to apply theoretical concepts to real-world situations, leading to a deeper understanding of the system. Furthermore, the hands-on experience in the lab also improves problem-solving skills, as students are able to experiment and test different solutions.

Concretely, we have implemented several exercises in our lab:

Protection of the Power Grid. In this exercise, students focus on the general operation of the power grid and start with learning about the different protection functions and their use in power networks. In the practical part, they we will use the Omicron CMC256 to test the protection functions and evaluate the reclosing feature that can automatically re-establish a power grid.

Operation. Students learn about how to switch, recognize alarms, and set parameters. In the practical portion, focus is on the IEC61850 protocol and how Layer 2 Messages are used. Tools for monitoring OT protocols and how to interpret the data are introduced as well. Additionally, the use and monitoring of IEC60870-5-104/101 is covered.

Cyber Security Maturity Assessment. In this exercise, students focus on evaluating the cyber security maturity and creating a catalog of cyber measures. First, they analyze the IP concept and network diagram, create a maturity table and risk assessment following the NIST framework (Barrett, 2018).

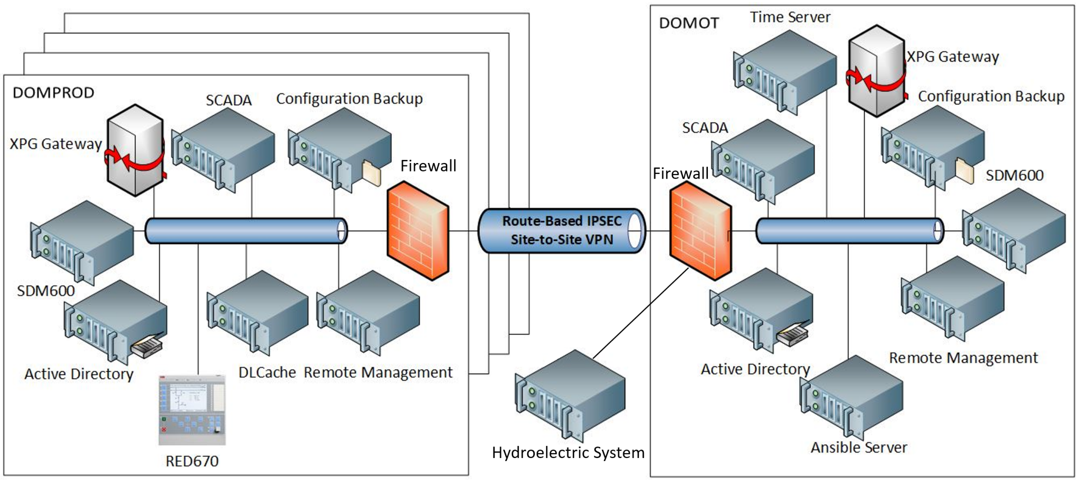

Figure 5: Network Layout of the Substation System.

Cyber Measures. A catalog of cyber measures is created in this exercise including a revision of the network segmentation. In the practical portion, the defined measures in the network are implemented, including a proper segmentation. Additionally, the configuration of the affected components is improved and verified.

IDS. After evaluating different concepts of IDS and methods integration, students integrate the Omicron StationGuard IDS practically and test its detection capabilities by executing the following attacks: Packet Injection, DoS, and Password Brute Force.

After the classroom has been completed, which consisted of 6 days with 6 lectures each, we have conducted a survey among the 15 participating students. We have received feedback from 8 participants. All students reported that the lab was worth their time and effort. Some students felt that the workload was high, due to the required preparation and reading before and after the lab sessions. Three students would like to have even more exercises. Despite this, the results of the lab indicate that the students learned a significant amount from the experience. Overall, the lab was deemed completely satisfactory by seven participants.

Anecdotal evidence also supports the benefits of a substation laboratory in the classroom. For example, students who have participated in laboratory sessions in a substation setting have reported a greater understanding of the material and a higher level of engagement in the class. One student went on to a career as a cyber security engineer for a utility. His employer reported that the on-boarding was exceptionally short. In addition, students who participated later in the hackathon and had experience in a substation lab demonstrated higher levels of success and were better able to apply their knowledge to the competition.

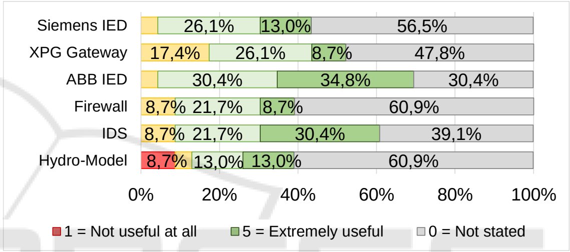

Figure 6: Usefulness of the Infrastructure.

5.2 Evaluation at Hackathons

The complete lab was evaluated through two 4-5 day hackathons, which took place in September 2022 and 2023, respectively, with more than 30 participants from various private, military and governmental organizations. The participants were split up into cross-functional teams, each with different focal points in the area of attack, digital forensics & intrusion detection, and reverse engineering.

The laboratory was used throughout the hackathons, allowing its participants to identify different vectors of attack on industrial control systems and carry out attacks themselves in the different parts of the laboratory. The participants appreciated the opportunity to be able to work on a concrete system resembling a real world setup.

To evaluate its usefullness, we created a survey of 24 quantitative and qualitative questions. 23 participants of the ICS Hackathon completed the survey.

Figure 6 shows the results of the perceived usefulness of the provided infrastructure: ”Please indicate below on a scale from 1 (not useful at all) to 5 (extremely useful) how you would rate the usefulness of the infrastructures provided at the hackathon?". In general, the mean index MD of the satisfaction rate was high, with the exception of the hydroelectric model as this part has not been used by many participants. Note that we have employed an additional standalone Siemens Siprotec device in the hackathon, which is not part of the regular setup.

Another result of the hackathon was the discovery and reporting following a responsible disclosure process of three vulnerabilities (CVE-2022-4778, CVE-2022-4779, CVE-2022-4780), which were discovered through analysis of the Gateway Applicance and its firmware. CVE-2022-4778 concerns a path traversal vulnerability in the gateway that allows authenticated users to get unauthorized access to files on the server's filesystem. CVE-2022-4780 concerns hardcoded crendentials in the gateway. The identified vulnerabilities show that the use of state-of-the-art hardware for cyber security research is essential because it provides a more realistic and accurate representation of the actual devices and systems being targeted by potential cyber attacks, unlike simulated devices which may not accurately reflect real-world scenarios and vulnerabilities.

An additional result of the hackathons was a test suite for IDS in substation environments developed by the defense team. The authors plan to report about it in a separate paper.

6 SUMMARY AND CONCLUSION

We have presented the design and use of a lab dedicated to cyber security in critical infrastructures that models a hydroelectric power plant to produce energy and a substation automation system to transfer it. The lab is unique in its double use for both teaching and research purposes. The lab features a combination of old and new devices and systems to cater to both basic and advanced research and teaching needs, enabling hackathons with a broad audience. Going forward, we will focus on the integration of additional critical infrastructure components, e.g., for building automation, to enable an even more holistic research and learning experience.

REFERENCES

Barrett, M. (2018). Framework for improving critical infrastructure cybersecurity version 1.1.

Candell, R., Zimmerman, T., and Stouffer, K. (2015). An industrial control system cybersecurity performance testbed. *National Institute of Standards and Technology. NISTIR*, 8089.

Chowdhury, N. and Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40:100361.

Frank, M., Leitner, M., and Pahi, T. (2017). Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology*, pages 38–46.

Gunathilaka, P., Mashima, D., and Chen, B. (2016). Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, CPS-SPC '16, page 113–124, New York, NY, USA. Association for Computing Machinery.

Holm, H., Karresand, M., Vidström, A., and Westring, E. (2015). A survey of industrial control system testbeds. In Buchegger, S. and Dam, M., editors, *Secure IT Systems*, Lecture Notes in Computer Science, pages 11–26. Springer International Publishing.

Obermeier, S., Jösler, T., Renggli, S., Unternährer, M., and Hämmerli, B. M. (2023). Automating recovery in mixed operation technology/it critical infrastructures. *IEEE Secur. Priv.*, 21(5):43–54.

Ruhe, S. and Roesch, D. (2019). Design of a cyber-physical energy laboratory. In *International ETG-Congress 2019; ETG Symposium*, pages 1–6.

Rösch, D., Bartusiak, A., and Ruhe, S. (2020). Portable cybersecurity training and research platform for power grids - testbed report. In *The 15th International Conference on Critical Information Infrastructures Security 2020 (CRITIS), 2-3 September 2020, Bristol, UK*.

Sauer, F., Niedermaier, M., Kießling, S., and Merli, D. (2019). LICSTER - A low-cost ICS security testbed for education and research. *CoRR*, abs/1910.00303.

Yang, Y., Jiang, H. T., McLaughlin, K., Gao, L., Yuan, Y., Huang, W., and Sezer, S. (2015). Cybersecurity test-bed for iec 61850 based smart substations. In *2015 IEEE Power & Energy Society General Meeting*, pages 1–5.