Blog Post: Advancing Cybersecurity for Power Distribution – The New Testbed Developed by ELECTRICA, TRANSELECTRICA, and Politehnica University within the ELECTRON Project

The digital transformation of power distribution substations brings numerous advantages, such as enhanced control, monitoring, and efficiency. However, with this, increasing digitisation also comes a significant rise in cybersecurity risks. Recognising the critical need for robust security measures, ELECTRICA, TRANSELECTRICA, and the National University of Science and Technology Politehnica Bucharest have collaborated under the ELECTRON project (https://electron-project.eu/) to develop a cutting-edge laboratory testbed designed to enhance the cybersecurity of power substations.

A Game-Changing Testbed for Substation Cybersecurity

This testbed, a pioneering solution for testing and evaluating the cybersecurity of power distribution substations, integrates real Intelligent Electronic Devices (IEDs) with open-source tools to simulate real-world operational conditions. This allows cybersecurity experts to test, analyse, and improve security measures in a safe yet highly realistic environment.

This development has focused on safeguarding the critical **GOOSE (Generic Object Oriented Substation Event)** communication protocol. As a key component of the **IEC 61850** standard, GOOSE allows fast, efficient communication between IEDs, essential for the smooth operation and automation of electrical substations. However, it also presents cybersecurity vulnerabilities that could compromise power grid stability if left unchecked.

The Power of Real-World Simulation

Unlike previous test methods that relied on purely virtual models, this testbed uses **Technology Readiness Level 7 (TRL 7)** equipment, creating a realistic simulation environment for testing cyber threats without risking operational disruptions in live systems. The laboratory environment replicates the actual behavior of substations, ensuring that tests closely mimic real-world scenarios. This allows for more accurate results in identifying vulnerabilities and testing potential cyberattacks, such as **False Data Injection (FDI)** and others.

Through extensive testing, the project has demonstrated how potential attacks on GOOSE communication can be launched and mitigated. The insights derived from these tests are crucial for developing stronger, more resilient cybersecurity frameworks for modern power grids.

Open-Source Tools: A Flexible, Cost-Effective Approach

The testbed's use of open-source tools is another standout feature, offering flexibility and scalability at a fraction of the cost of traditional proprietary systems. Open-source platforms such as **OpenSCD**, **OpenServer**, and **LibIEC61850** were utilised to simulate substation environments, configure IEDs, and test communication protocols. This open approach ensures that the system is adaptable to evolving cybersecurity threats and can be expanded or modified as needed.

Additionally, tools like **Wireshark** and **Snort** were employed for network traffic analysis, allowing cybersecurity experts to monitor GOOSE communications and detect potential vulnerabilities in real time.

Ensuring the Security of Critical Infrastructure

This testbed marks a significant leap forward in protecting critical infrastructure within the energy sector. As substations and power grids become more interconnected and reliant on digital communication, the need for rigorous cybersecurity measures grows exponentially. The laboratory environment developed through this collaboration provides an essential platform for ongoing cybersecurity research, offering insights that will help safeguard substations against emerging threats.

Collaboration for the Future of Secure Energy Grids

The testbed is a testament to the power of collaboration between industry leaders and academic institutions. The joint efforts of **ELECTRICA**, **TRANSELECTRICA**, and **National University of Science and Technology Politehnica Bucharest** under the **ELECTRON** project No. 101021936 showcase a forward-thinking approach to addressing the cybersecurity challenges faced by modern power systems.

As the world moves toward smarter, more automated energy grids, this project sets a new standard for cybersecurity testing and development. It ensures that distribution substations remain resilient to cyber threats, helping to protect the stability of national power networks.

Fig. 1 The main rack of the testbed