Portable cybersecurity training and research platform for power grids - Testbed report

Dennis Rösch[1], Adam Bartusiak[2], and Stephan Ruhe[1]

[1] Fraunhofer IOSB, IOSB-AST Ilmenau, Germany
[2] Fraunhofer IOSB, IOSB-AST Görlitz, Germany
dennis.roesch@iosb-ast.fraunhofer.de

Fig. 1: Physical Setup of Training and Research Platform

Critical infrastructures and in particular energy supply have undergone significant developments, such as decentralisation and digitalisation, which push a significant amount of innovation and movement in the networking of many distributed IT and OT-based energy systems. These advancements bring substantial benefits but also expose the underlying systems to a number of risks at the same time. In this report, a portable platform is presented which allows examining various aspects of cybersecurity on an electrical process and, as a result, provides an interactive hardware environment for conducting technical trainings for the employees of energy supply organisations.

The main purpose of the portable platform shown in Figure 1 is to demonstrate the importance of applying security recommendations defined in e.g. IEC 62351 and IEC 62443 illustrated with a voltage transformer process, which is implemented using common automation technologies and miniaturized electrical equipment. In addition, this platform provides a research environment to address and test contemporary security solutions within an OT infrastructure as an extention to our stationary testbed [1]. Figure 2 shows the process, IT-network structure, and overlying virtual infrastructure for investigating the early stages of coordinated attacks.

The aim of the attacks is to demonstrate their harmful influence on a dynamic process by setting it into an unsafe state. Defence strategies that can be applied on the platform rely on the chosen aspects of the Defence-in-Depth approach

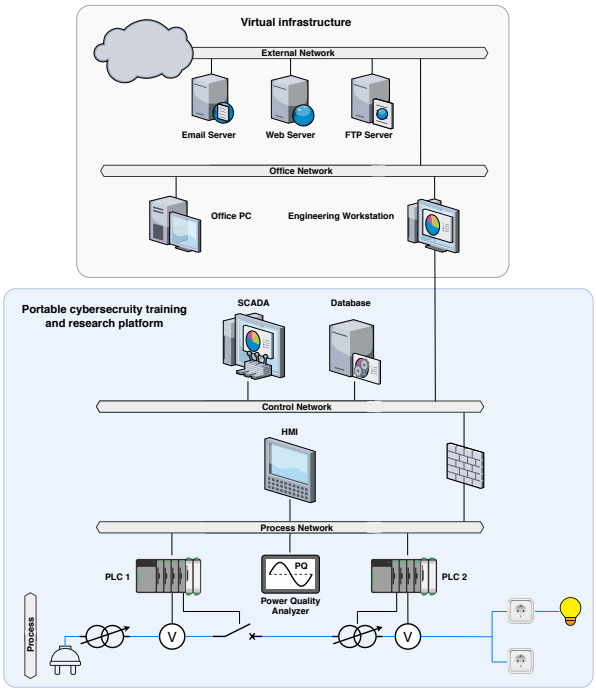

Fig. 2: Abstract process view

according to IEC 62443. Table 1 summarizes possible security measures that can be applied on the platform to counter to the implemented attacks.

Table 1: Defence-in-Depth concepts and security measures

Attack type	**Defence-in-Depth concept**	**Possible security measures**
Password Cracking	Policies, Processes, Security Awareness	Hardening, Secure System Configuration
Denial-of-Service	Network Security	Network Segmentation and Monitoring
Man-in-the-Middle	Network Security	Network Segmentation and Monitoring
	Software Security	Encryption, Access Control

References

1. Ruhe, S., Rösch, D.: Design of a cyber-physical energy laboratory. International ETG-Congress 2019; ETG Symposium pp. 1–6 (2019)