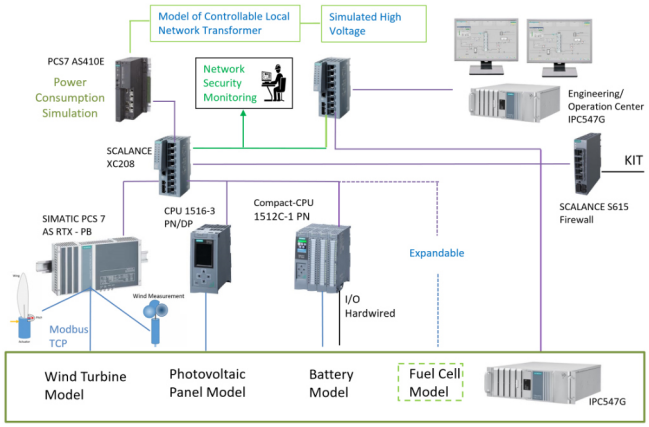
SecLabE investigates potential threats against future energy systems and aims to develop countermeasures.

The Security Lab Energy (SecLabE)

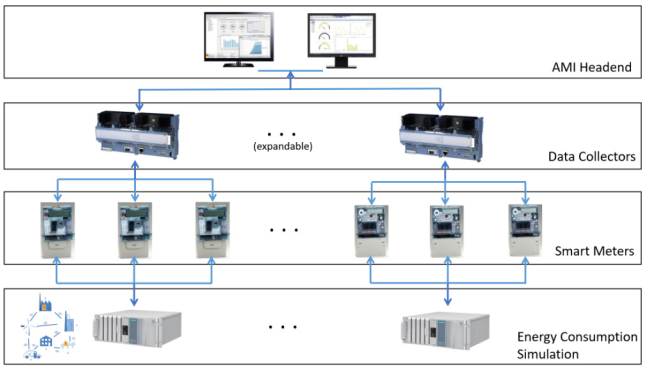
A small-scale Smart Grid (SG) with an energy supply part (wind turbine, battery and PV) and a transmission substation are implemented as Matlab / Simulink models. Some sensors and actors are installed physically. The three Siemens PLCs and the three IEDs are responsible for controlling the dynamic behavior of the four models and taking corrective actions. One engineering and monitoring workstation is directly located in the E-Lab 2.0 and the second one, which is located in the building 445, is connected through VPN to the SecLabE, so that supervisory actions can be carried out remotely. The Network Security Monitoring (NSM) station provides a continuous collection, attack detection, and analysis of communication data. The testbed will be extended with integration of further energy consumption simulation models to provide data for Advanced Metering Infrastructures (AMI).

- Cyber-Physical Security (CPS) is a substantial concern in critical infrastructures.
- The interconnected structure of SGs increases considerably its exposure to cyber-attacks as in our model more than 40 variables are transmitted for control and monitoring.
- Man-in-the-Middle, data theft, false data injection and other manipulations.
- Such attacks can have severe consequences on the stability of the electric grid and might lead to blackouts.
- To defend against those threats, designing and developing effective countermeasures for the CPS for the transition to future energy systems.

The architecture and the communication network of the SecLab is represented by the following diagram. Several PLCs and IEDs are used as hardware-in-the-loop components together with power generation and transmission simulations.



Security Lab Energy (SecLabE)



A further extension of SecLabE with an AMI is planned. The structure of the AMI is presented in the following diagram where hardware components such as smart meters and data collectors will be directly connected to a simulation of the energy consumption.

The SecLabE Expansion

For data exchange, as a substantial "intelligent" subsystem of the SG, the AMI provides bidirectional communication between energy consumers and providers for monitoring and demand-response systems. A broad variety of new communication technologies emerge and constantly evolve in AMI, which contribute to integration of a great number of intelligent appliances into the SG.
Communication in AMI is often grouped into communication in LAN (between energy prosumers and smart meters), NAN (between smart meters and data collectors) and WAN (between data collectors and headend system). However, this very high accessibility may cause increased cyber-attacks due to unsecure system design, vulnerabilities in communication protocols, software and programming languages. Hence, the extension of SecLabE by AMI testbed is essential.

Preventing Cyber-Attacks

As a high-level control system for cyber-security research for future energy systems, the SecLabE facilitates implementation of attack scenarios and manipulation of hardware and software components. This enables the analysis of the risks and possible malfunctions in the electric system caused by cyberattacks.

SecLabE Objectives

SecLabE is used for development of efficient methods and algorithms for detection and prevention of cyber-attacks. This includes the development of supervision tools, the design of security features in protocols, software and systems as well as recovery strategies.

Dr. Kaibin Bao
Insitute for Automation and
Applied Informatics

Hermann-von-Helmholtz-Platz 1
76433 Eggenstein-Leopoldshafen

kaibin.bao@kit.edu

Federal Ministry
for Economic Affairs
and Energy

Baden-Württemberg
MINISTERIUM FÜR WISSENSCHAFT, FORSCHUNG UND KUNST

Federal Ministry
of Education
and Research