LEARNING LAB CYBERSECURITY
ENERGY AND WATER SUPPLY

Cyber security and digitalization
The massive attack on the state-owned Ukrainian electricity supplier Ukrenergo or the distribution of blackmail software such as “Wannacry” or “Petya” are only some examples why cybersecurity is currently the focus of public attention. In this context, the IT security of critical infrastructures plays an outstanding role, since they secure the daily supply of our society. With a unique learning laboratory, direct knowledge transfer from the accompanying IT security research and a specially tailored training offer, we guarantee your company the right offering for all enterprise levels:

Decision makers
Creating awareness for cybersecurity, information about current standards, norms and dangers

Information security officer
Best practices and state of the art of communication architectures for critical infrastructures, information on the current legal and guideline situation

Planer / Developer
State of the art and best practices in the area of security and safety, weaknesses of communication interfaces and protocols

Users
IT threat situation and handling of critical infrastructure data and systems
Trainings

We offer a wide range of training courses on IT security and IT security management for companies and critical infrastructures. Our training courses offered by the Fraunhofer Academy include the following topics:

- Current legal situation
- Attack examples and how they work
- IT security management
- Security awareness
- Employee awareness
- Standardization (ISO 2700x, BSI IT-Grundschatz, VDE 3473)
- IT security management tools
- Preparation and procedure of certifications
- Comparison of IT security management tools
- Practical attack examples and case studies

More information on our trainings (German only):

https://www.academy.fraunhofer.de/kritis

In addition to our training courses, we offer independent and individually tailored R&D services in the field of IT security for companies, municipal and public institutions and in the context of critical infrastructures.

Learning lab “cybersecurity energy and water supply”

In our learning laboratory, complete IT and hardware infrastructures can be flexibly replicated. The core piece is an OPAL-RT test stand for hardware-in-the-loop tests. From simple office computers to firewalls and VLANs, most heterogeneous and diverse IT system landscapes can be simulated.

In addition, a wide range of R&D test scenarios are possible, such as the triggering of protection systems without physical network overload, the simulation of current and transformer signals and any sensor signals. The learning laboratory also comprises a control system and engineering and power quality monitoring workstations.

The illustration of a real motor-generator combination, with which consumers, generators and the control of industrial and power plants can be simulated, is unique. The learning laboratory does not only serve as part of our training portfolio but also as a tool for applied research in the field of IT cybersecurity, from which you can already benefit in our today’s offers.

Technical data sheet for the learning lab

Protocols in control technology:
- IEC 60870-5-104
- IEC 61850
- DNP 3.0 via Ethernet
- Modbus
- OPC-UA
- Profibus

Remote maintenance and remote accesses:
- Physical: DSL, WLAN, 3G/4G
- Logical: VPN, FTP, SFTP, TLS/SSL, RDP
- TeamViewer, Putty, MobaXterm

Hardware-in-the-loop stand:
- Simulation of causes and triggers of the protection systems without physical network overload
- Simulation of current and voltage transformer signals
- Simulation of any sensor signals

Figure 1: View of the learning laboratory with real guidance system