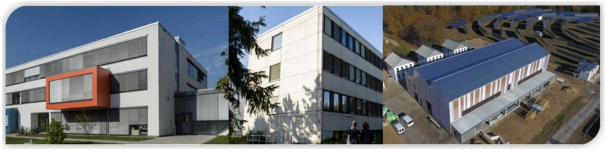
Karlsruhe Institute of Technology



Institute for Automation and Applied Informatics (IAI)

Student Thesis

Extension of Cyberrange CyDER by Operational Technology and Energy Systems Components

For research on nation-state cyber attacks on industrial and energy systems, we built our cyberrange CyDER (Cyber Distribution Experimentation Range). This cyberrange enables us to model realistic networks and systems in a separate environment for security testing, while being repeatable and featuring infrastructure for central audit log aggregation.

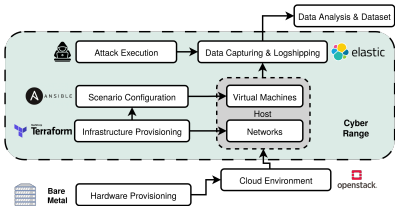


Figure 1: Underlying architecture of our Cyberrange CyDER

This thesis should make use of existing software provided by the LF Energy Sogno project and other open-source projects to implement a representative energy system covering the Purdue levels 3 to 1.

To emulate complete cyber attacks, including the transition from IT to OT and attacks targeting OT systems, we need to model such OT, energy systems and industrial automation components. This includes Control Centers, Substations and Field Controllers like PLCs, RTUs and IEDs. While simulators for many field devices already exist, we need implementations to run on Linux and Windows virtual hosts like they run on actual deployed hardware, so we can monitor network traffic and system audit logs.

Possible Research Questions:

- How can different energy systems be modeled in an abstracted but realistic and representative way?
- What is the smallest set of energy system components needed to model and re-create known attacks on energy systems?
- How can cyber ranges be used in combination with simulation models and real-time simulators for end-to-end attack emulation?

Main Tasks:

- Get an overview of industrial automation and energy systems architectures
- Set up an energy system and an industrial automation architecture that cover representative systems
- Implement your architectures within CyDER using FOSS like SOGNO and other open-source projects
- Set up communication between the components using IEC 61850, IEC 104, Modbus and OPC-UA
- Set up coupling with real-time Simulators like Opal-RT

Contact
Richard Rudolph
richard.rudolph@kit.edu

Skills

- Basic understanding of industrial automation and energy systems
- Basic knowledge of operating systems, system calls and network traffic
- Python and Bash
- Understanding of DevOps
- Container Orchestration

Studies

- Computer Science / Informatics

Languages

German or English

Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology
Campus North
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen