

## Support in configuring and testing a GNSS simulator environment at the KASTEL Security Lab Energy

### Description:

The highlighted objective of “Secure Energy Systems (SES)” working group is about the cyber-physical security of energy systems. The working topics cover a broad range from hardware to the communication structure in Smart Grids (SGs). New concerns about risks of security threats have emerged with the implementation of SGs infrastructure. Since Precision Time Protocol (PTP) has a vital role to enhance high precision time synchronization for time-critical applications, conducting PTP related attack scenarios is planned to investigate interoperability and analyze grid stability. A simplified representation of PTP-related attack scenarios is shown in Figure 2.

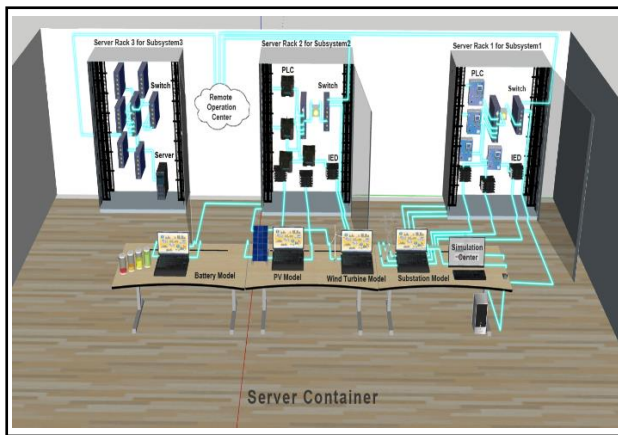


Figure 1: Projection of KASTEL Security Lab Energy

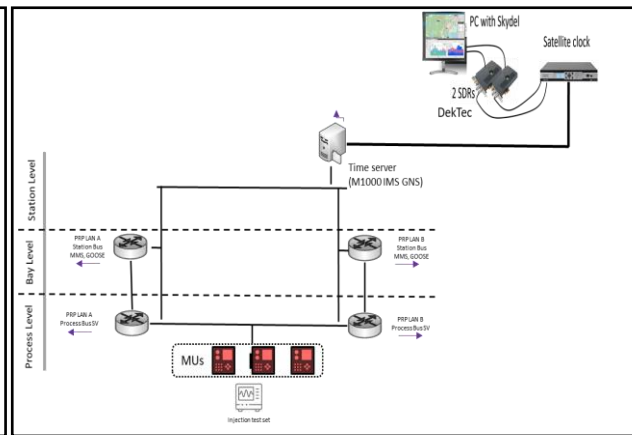


Figure 2: Simplified representation of attack scenario regarding Heterogeneous Subsystem

Genuine and spoofing signals are created by a computer using the software Skydel GNSS Simulator Environment by the company Orolia.

- Helping to configure and test Skydel GNSS Simulator environment for attack scenarios such as jamming and spoofing attacks.
- Assistance with documentation of the outcomes.

### Requirements:

- Bachelors or Masters at Computer Science.
- Familiar or motivated to work with GNSS Simulator environment.

### Contact:

Clemens Fruböse  
Phone: +49 721 608-45764  
e-mail: [clemens.fruboes@kit.edu](mailto:clemens.fruboes@kit.edu)

Sine Canbolat  
Phone: +49 721 608-24913  
e-mail: [sine.canbolat@kit.edu](mailto:sine.canbolat@kit.edu)