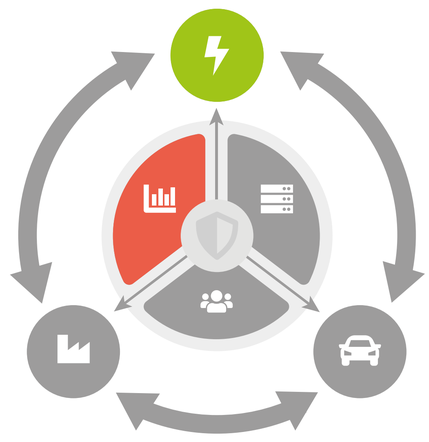
Karlsruhe Institute of Technology

P1T3

GPS & Co.: Danger of Attacks on the Smart Grid

C. Fruböse, S. Canbolat Kaya, E. Hetzel, G. Elbez, J. Müller-Quade, V. Hagenmeyer
(Energy Systems Security, Quantification)



Motivation and Research Questions

- Modern grid control requires time-synchronized measurements (~ 1 µs)
- Time sync. is usually done using **GNSS satellite signals**
- GNSS **incidents have been reported** (e.g., Finland)

➡ How vulnerable is the Smart Grid to time synchronization attacks?

Impact

Novelty

- Realistic setup at the KASTEL Security Lab Energy

Social and Economic Impact

- Awareness of disruptions and risk quantification

Applications

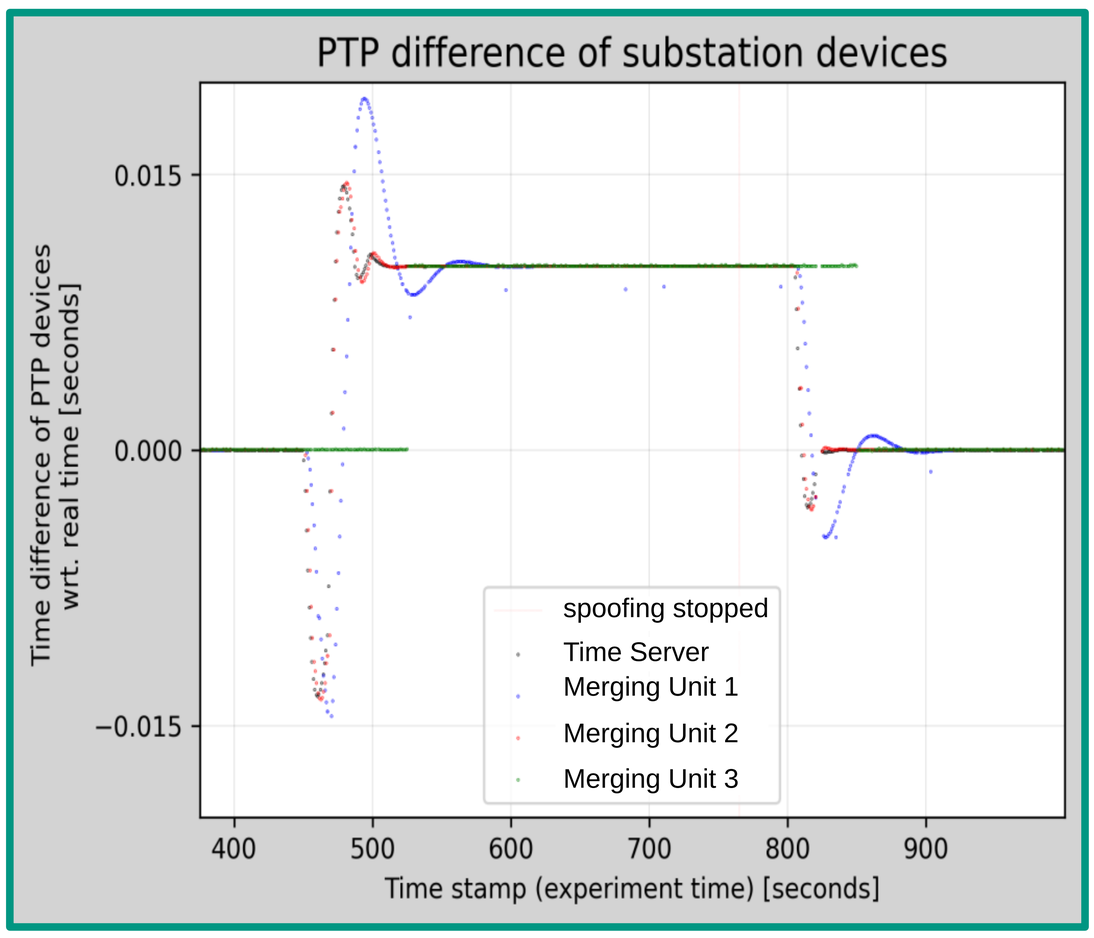
- Hardening of Smart Grids against GNSS attacks

Research Activities and Results

- Approach
  - **Conduct GNSS spoofing attacks** with real hardware, estimate success / difficulty [DIMVA 2024]
  - Simulate impact on grid with help of **energy informatics at KIT**
  - Combine findings for risk evaluation

Results of GNSS attacks

- Jamming- Attacks: High impact, not stealthy
- Jump-Attacks: High impact, not stealthy
- Drift-Attacks: Stealthy but more difficult to conduct
- Devices from different manufacturers react differently to time shift



- Future Development
  - Monitoring to **eliminate blind spots**
  - **Voting on internal clocks** to detect drifts
  - Security recommendations such as authenticated GNSS signals

Publications

- Extended Abstract: Assessing GNSS Vulnerabilities in Smart Grids. In: DIMVA 2024.

links to:

FENCE: Future ENergy Cybersecurity Evaluation

KASTEL