Karlsruhe Institute of Technology

Contact:

HELMHOLTZ

Compromising Time Synchronization in an Electrical Substation: Cyber Threats and Impact Analysis

Clemens Fruböse*, Sine Canbolat Kaya*, Eva Hetzel*, John Seiquera, Ghada Elbez, Veit Hagenmeyer

Motivation & Research Approach

Motivation:

- **Monitoring** and **protection** with ~1 µs measurement accuracy
- Time synchronization usually done using **GNSS satellite signals**
- **Reported GNSS incidents** (e.g. Finland, Poland)
- **Impact** of time synchronization attack on the power grid **still open**
- **Mitigation** of time-related risks

Research Approach:

- KIT possesses **Realistic Smart Grid Testbed** (hardware-based) [2]
- Conduct **risk quantification** taking into account: difficulty, success ratio, attacker's trade-offs [1]
- **Mitigation** of time-related risks

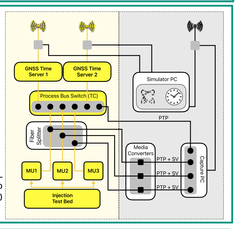
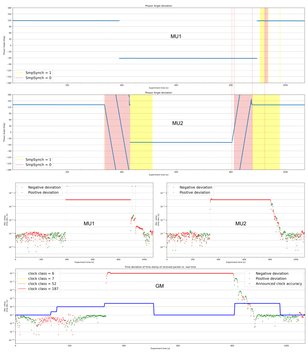


Fig. 1: GNSS time spoofing setup at KASTEL Security Lab Energy, yellow parts correspond to realistic electrical substation fulfilling IEC 61850 standard

Selected Experimental Results

Time jump attack



- (Short) blocking of some protection functions
- Interoperability issues (possible trips)
- Phasor angle change of 180°
- Detectable in standard monitoring

- No immediate blocking of protection functions
- No interoperability issues
- Phasor angle change of only $3.6 \cdot 10^{-5} deg\ s^{-1}$
- Not detectable in standard monitoring

Fig. 2: IEC 61850 Sampled Values (SV) and PTP impacts of time jump attack

Time drift attack

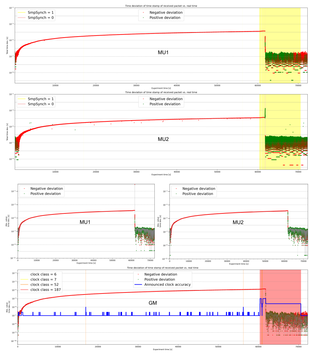


Fig. 3: SV and PTP impacts of time drift attack

Risk Analysis and Conclusion

Risk analysis:

- To assess risk, **flags have to be considered** (not every jump is blindly accepted)
- Real hardware from **different manufactures reacts differently** (dependent on GM behavior: SmpCnt jumps, Ramp-Ups, SmpSynch values)
- Impacts are **incorrect phasors** (WAMS), **possible differential protection trips**, **blocking of protection functions**

	Jamming	Time Jump attack	Time drift attack	Internal PTP attack (APT)
Required skill & access	Low	Low	Medium	High
Detectable in standard monitoring	Yes	Yes	No	No
Mitigation	Medium	Medium	Hard	Hard
Impact Magnitude	Medium	High	Low	High
Timing of impact	Easy	Medium	Hard	Easy

Fig. 4: Overview matrix of time synchronization attacks on an electrical substation.

Conclusion:

- Real world dangers occur if **different time bases are compared** (differential protection between substations, different MUs within substation)
- Impacts **require modern substation design and substantial insider knowledge**
- Risk quantification must **consider ease of coordination and scalability**

Publications

[1] Canbolat, Sine, et al. "Assessing GNSS Vulnerabilities in Smart Grids." *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Cham: Springer Nature Switzerland, 2024.

[2] Elbez, Ghada, et al. "Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research." *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems*, 2025.

* clemens.fruboese@kit.edu
* sine.canbolat@kit.edu
* eva.hetzel@kit.edu

KASTEL

EIE

ITSF 2025

I · T · S · F