VDE FNN/ETG Tutorial

SCHUTZ- UND LEITTECHNIK 2026

Wie beeinflussen GNSS Angriffe die Smart-Grid Stabilität?

Clemens Fruböse, John Seiquera, Veit Hagenmeyer
KASTEL Security Research Labs, Karlsruher Institut für Technologie (KIT)
Kontakt: clemens.fruboese@kit.edu

Motivation & Herangehensweise

Motivation:

- **Monitoring** und **Schutz** mit ~1 µs Messgenauigkeit
- Zeitsynchronisation erfolgt üblicherweise mittels **GNSS-Satellitensignalen**
- **Bekannte GNSS-Vorfälle** (z. B. Finnland, Polen)
- **Auswirkungen** von Zeitsynchronisations-angriffen auf Stromnetz **weiterhin offen**
- **Vorbeugung** zeitbedingter Risiken

Herangehensweise:

- KIT verfügt über **realistisches Smart Grid-Testsysten** (hardwarebasiert)
- **Quantifizierung von Risiken** unter Berücksichtigung: Schwierigkeit, Erfolgsquote, trade-offs des Angreifers [1]
- Bewertung zeitbedingter Risiken: **"Was ist realistisch?"** [2]

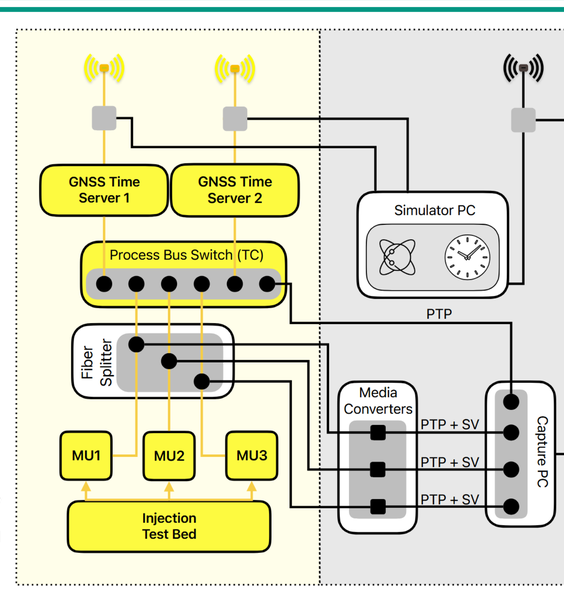

Abb. 1: GNSS-Zeit-Spoofing-Setup im KASTEL Security Lab Energy, gelbe Teile entsprechen einem realistischen Umspannnwerk, das IEC 61850-Standard erfüllt.

Ausgewählte Ergebnisse

Zeit-Sprung-Angriff

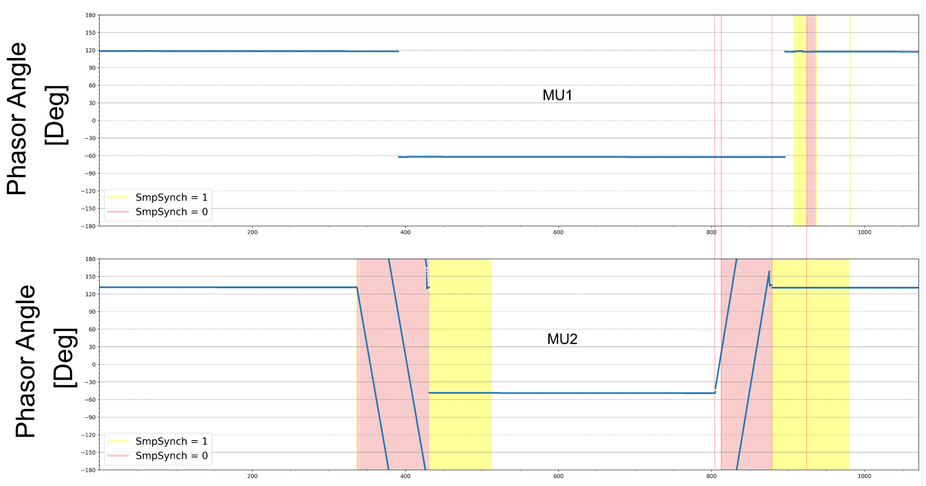

Abb. 2: IEC 61850 Sampled Values (SV) bei einem Zeit-Sprung-Angriff

- (Kurzzeitiges) Blockieren von Schutzfunktionen
- Interoperabilitätsprobleme (Fehlauslösungen)
- Winkeländerung Phasoren um 180°

- Kein Blockieren der Schutzfunktionen
- Keine Interoperabilitäts-probleme
- Winkeländerung Phasor nur $3.6 \cdot 10^{-5} deg\ s^{-1}$

Zeit-Drift-Angriff

Abb. 3: SV bei einem Zeit-Drift-Angriff

Risikoanalyse und Fazit

Risikoanalyse:

- **Flags müssen berücksichtigt werden** (nicht jeder Sprung wird akzeptiert)
- Echte Hardware **verschiedener Hersteller verhält sich unterschiedlich** (abhängig vom GM-Verhalten)
- Auswirkungen: **falsche Phasoren** (WAMPACS), **mögliche differenzielle Schutzauslösungen, Blockade von Schutzfunktionen**

	Jamming	Zeit-Sprung-Angriff	Zeit-Drift-Angriff	Interner PTP-Angriff (APT)
Erforderliche Fähigkeiten und Zugang	Niedrig	Niedrig	Mittel	Hoch
Erkenntlich im Standard-monitoring	Ja	Ja	Nein	Nein
Vorbeugung	Mittel	Mittel	Schwierig	Schwierig
Schadens-größe	Mittel	Hoch	Niedrig	Hoch
Timing des Shifts	Leicht	Mittel	Schwierig	Leicht

Abb. 4: Übersichtsmatrix der Zeitsynchronisationsangriffe auf ein Umspannwerk.

Conclusion:

- Echte Gefahren treten nur auf, wenn **verschiedene Zeitbasis verglichen werden** (diff. Schutz zwischen Umspannwerken, unterschiedliche MUs innerhalb der Umspannwerke)
- Auswirkungen **erfordern modernes Umspannwerksdesign und großes Insiderwissen**
- Risikoquantifizierung muss **Koordination** berücksichtigen

Publikationen

[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] Fruböse, Clemens, et al. „Compromising Synchrophasor Data by Attacking Time Synchronization: A Hardware-Lab Study." *5th International Conference on Smart Grid Synchronized Measurements and Analytics 2026* – in press

Karlsruhe Institute of Technology

HELMHOLTZ

KASTEL