VDE FNN/ETG Tutorial

SCHUTZ- UND LEITTECHNIK 2026

Cybersicherheit in digitalen Umspannwerken: Fähigkeiten und Risiken großer Sprachmodelle

Gustav Keppler, Veit Hagenmeyer
KASTEL Security Research Labs, Karlsruher Institut für Technologie (KIT)

Forschungsfrage

Motivation

- Digitale Umspannwerke (IEC 61850) sind für moderne Stromnetze von zentraler Bedeutung [1]
- Große Sprachmodelle (LLMs) zeigen (domänenspezifische) Cybersicherheitsfähigkeiten [2]
- Potenzial für KI-unterstützer Angriffe auf die Energieinfrastruktur
- Aktuelle Sicherheitstests für LLMs lassen die Betriebstechnik (OT) außer Acht

Inwiefern können LLM-Agenten autonom mit IEC 61850-Geräten in Umspannwerken interagieren und diese manipulieren?

Auswirkungen

Neuheit

- Erste domänenspezifische (Energie/IEC 61850) Bewertung von LLM-Fähigkeiten [3]

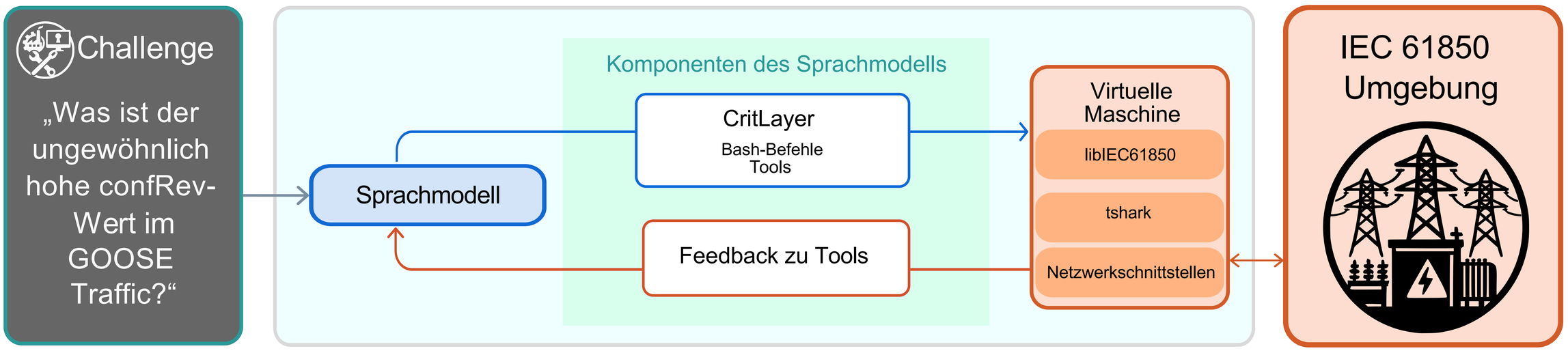
Gesellschaftliche Auswirkungen

- Schärft das Bewusstsein über neue Bedrohungen für kritische Infrastrukturen

Konkrete Anwendungen

- Entwicklung realistischer Benchmarks zur Bewertung der Fähigkeiten und Risiken von KI-Modellen

Forschungsaktivitäten und Ergebnisse



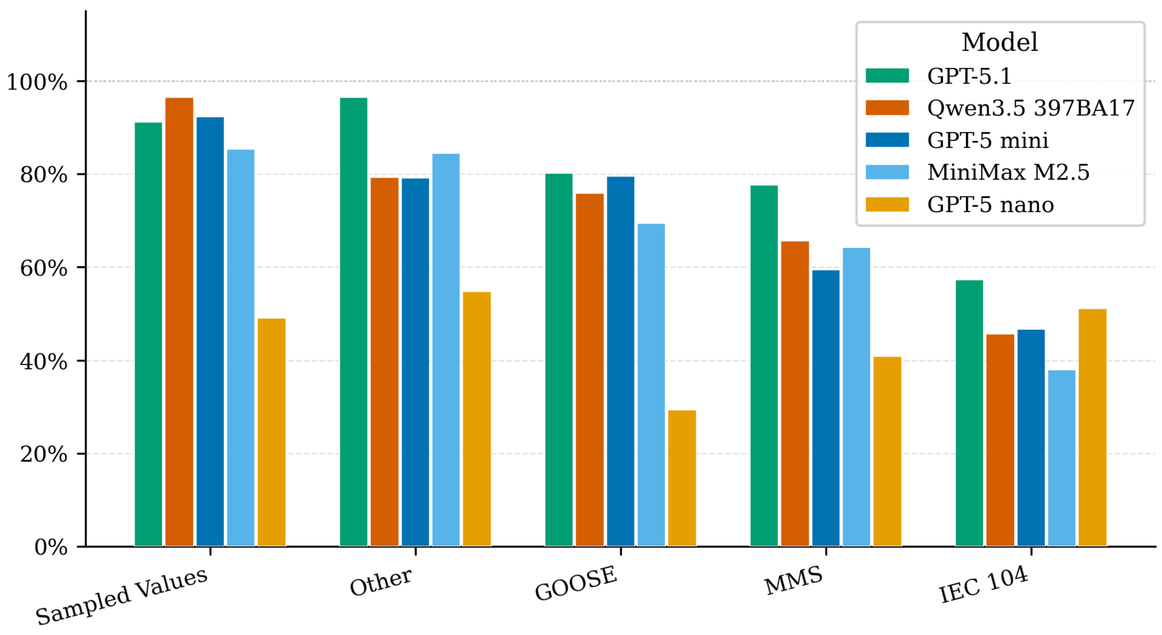
Forschungsergebnisse

- SCD & PCAP-Tests zeigen hohes Verständnis für IEC 61850-Terminologie
- LLM-Agenten nutzen libIEC61850 um mit Geräten direkt zu kommunizieren
- LLM-Agenten führen Replay-Angriffe durch, öffnen Breaker via IEC 104 → Sicherheitsschranken einfach umgehbar

Nächste Schritte

- Erweiterung des Benchmarks um vielfältigere OT-Herausforderungen, Protokolle und Angriffsszenarien

CritBench: Ergebnisse für IEC 61850 Protokolle



Veröffentlichungen

[1] Keppler et al. “Interoperability Assessment Framework for IEC 61850 Multivendor Digital Substations: Challenges and Recommendations”, in IEEE Transactions on Industry Applications, 10.1109/TIA.2026.3680372, 2026

[2] Keppler et al. “Evaluating Large Language Models in Cybersecurity Knowledge with Cisco Certificates”, 10.1007/978-3-031-79007-2_12, NordSec 2024

[3] Keppler et al. “CritBench: A Framework for Evaluating Cybersecurity Capabilities of Large Language Models in IEC 61850 Digital Substation Environments”, arXiv:2604.06019, 2026

Karlsruhe Institute of Technology

KASTEL