technische universität dortmund

Fakultät für Elektrotechnik und Informationstechnik

Institut für Energiesysteme, Energieeffizienz und Energiewirtschaft

Master Thesis for X

Benchmarking and Testing of an AI-Driven Anomaly Detection Algorithm in Smart Grids

---

The operation of modern transmission power systems is characterized by a high degree of automation and extensive use of digital control and monitoring infrastructure. Extending comparable levels of automation to distribution and low-voltage grid levels requires a significant increase in communication interfaces and data exchange. While this ongoing digitization enables advanced control strategies and improved system efficiency, it simultaneously increases the exposure of power systems to cyber threats, data manipulation, and communication failures.

Consequently, the reliable detection of anomalies in measurement and control data becomes a critical requirement for secure power system operation. Data-driven approaches, including machine-learning-based anomaly detection methods such as those implemented in the EnerGuard pipeline, represent promising tools to address these challenges. In addition, control and protection algorithms must be systematically evaluated with respect to their robustness against corrupted, delayed, or maliciously manipulated data.

The objective of this thesis is to investigate the detection and impact of cybersecurity threats in digitized power systems. For this purpose, a test suite will be established in the Smart Grid Technology Laboratory and complemented by simulation-based studies to reproduce representative cyber-related disturbances and to assess the impact of erroneous or manipulated data on measurement signals and control stability. Finally, the EnerGuard anomaly detection pipeline will be evaluated and benchmarked with respect to its detection capability and reliability under the considered scenarios.

The work can proceed as follows:

- Familiarization with the topic, literature review, and requirements analysis about the topic of cybersecurity and testing procedures in power systems
- Exemplary setup of a simulation for a typical substation with the integration of EnerGuard’s detection pipeline
- Implementation of a testing system and scenario definition of attacks and failures
- Benchmarking of detection reliability and impact of cyber attacks in predefined scenarios
- Documentation of the results

Schedule:

- Start of the thesis work on March 1, 2026

At the end of this thesis work, the results achieved shall be presented to wider audience along with open discussions.

Supervisor @ ie3: Prof. Dr.-Ing. Christian Rehtanz
Aaron Eicker, M.Sc.
Maurice Raetsch, M.Sc.