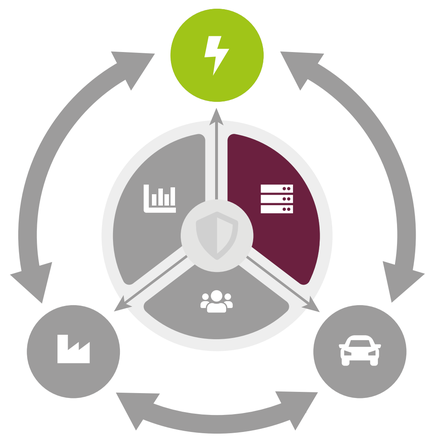
Karlsruhe Institute of Technology

P1T3

FENCE: Future ENergy Cybersecurity Evaluation



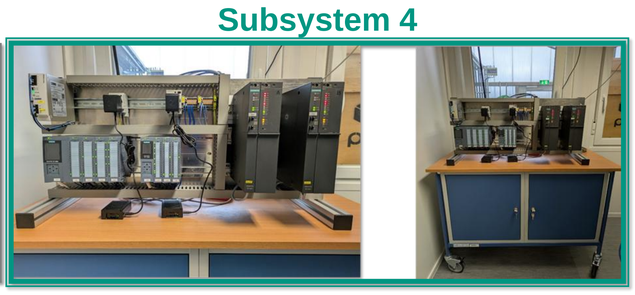
H.C. Alberto, S. Canbolat Kaya, S. Corallo, G. Elbez, C. Fruböse, E. Hetzel, N. Kellerer, G. Keppler, F. Lanzinger, F. Neumeister, G. Sanchez, B. Beckert, A. Koziolek, J. Müller-Quade, M. Zitterbart, V. Hagenmeyer
(Cryptography Quantification, Dependability Verification, Energy Systems Security, Modeling Software Engineering, Network Security)

Motivation and Research Questions

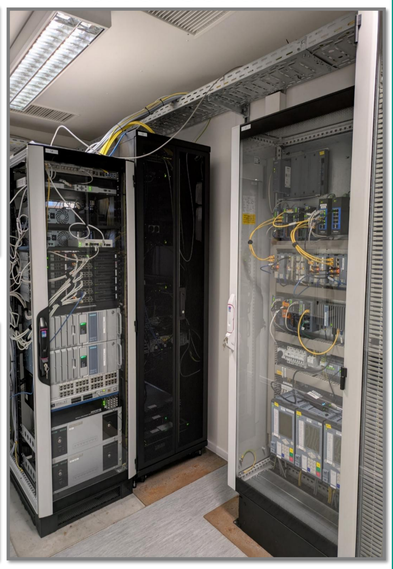
➡ What novel security approaches leveraging cutting-edge tools and techniques can be developed to enhance the cybersecurity of power grids ?

Subsystem 2

Subsystem 4



Server Container



Subsystem 1 & SDN

Office Container

Impact

- Strengthen energy system cybersecurity through advanced defense strategies
- Leverage cutting-edge tech. to respond to threats and vulnerabilities in energy systems

Helmholtz Program ESD

ESD

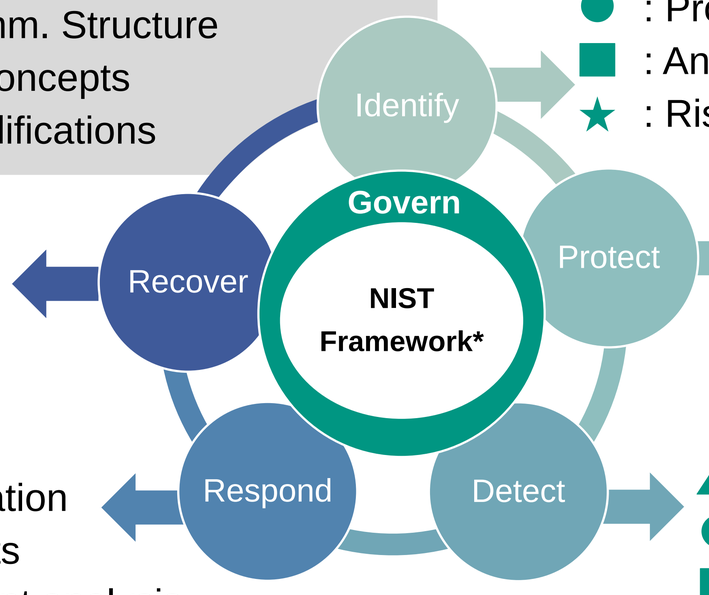
Other Partners

SIEMENS energy, NTNU, OMICRON, SAFRAN, SUTD Singapore University of Technology and Design, DTU Technical University of Denmark, University of Illinois Urbana-Champaign, Australian National University, ADSC Illinois at Singapore Pte Ltd

Research Activities and Results

- The power grid heavily relies on Information and Communication Technology (ICT), making it vulnerable to cyber-attacks.
- Interdisciplinary research tailored for energy systems at ST2.

▲ : Vulnerability Analysis in Software, O.S. of PLCs and Comp.
● : Securing Network Protocols and Comm. Structure
■ : Intrusion Detection and Prevention Concepts
★ : Risk Analysis and Quantification/Qualifications



▲ : Vulnerability analysis, threat modeling
● : Protocol weaknesses, compliance with standards
■ : Analysis of cyber-physical threats in SCADA sys.
★ : Risk analysis and quantification of threats

▲ : Secure software development
● : SDN-based mitigation
■ : IDS development and robustness
★ : Risk mitigation strategies

★ : Resilience and post-incident assess.

● : Incident response via SDN reconfiguration
■ : Automated response through IDS alerts
★ : SIEM-based response and post-incident analysis

▲ : Formal methods for software vulnerabilities
● : Monitoring network anomalies
■ : Hybrid IDS for detecting anomalies
★ : IDS integration into SIEM

*Source: https://www.nist.gov/cyberframework

Publications

- Evaluating Large Language Models in Cybersecurity Knowledge with Cisco Certificates. In: NordSec 2024.
- Attacking Learning-based Models in Smart Grids: Current Challenges and New Frontiers. In: e-Energy 2024.
- Extended Abstract: Assessing GNSS Vulnerabilities in Smart Grids. In: DIMVA 2024.

links to:

How can industrial protocols be protected, and ML-based IDS robustness tested?

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

KASTEL