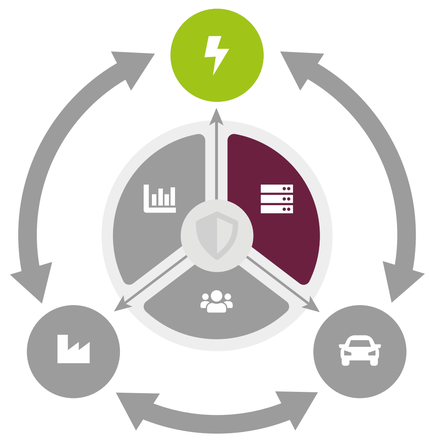
Karlsruhe Institute of Technology

**P1T3**

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

N. Kellerer, G. Sánchez, H.C. Alberto, G. Elbez, V. Hagenmeyer
(Energy Systems Security)



## Motivation and Research Questions

- Improve security of existing infrastructure, including legacy systems, without costly upgrades
- Understand cybersecurity threats in a safe environment before they are exploited by malicious actors

➡ How well do learning-based Intrusion Detection Systems (IDS) detect cyberattacks against industrial protocols and how robust are they against poisoning attacks?

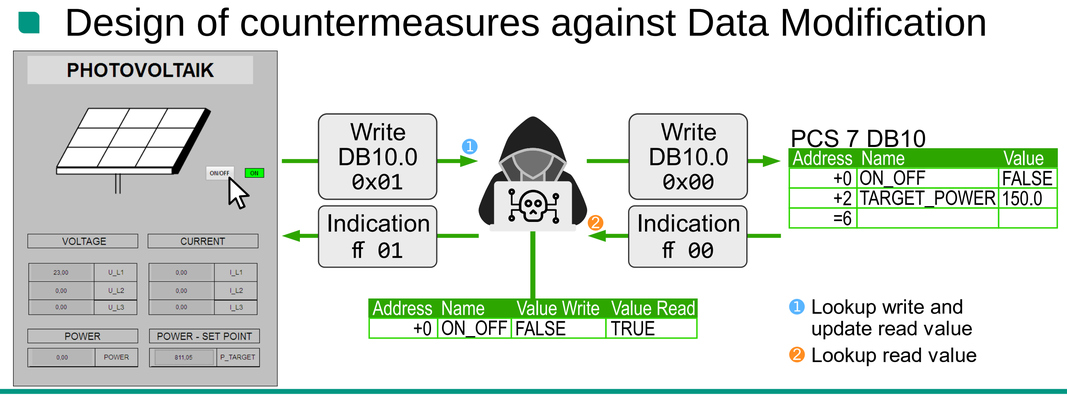
## Impact

### Novelty

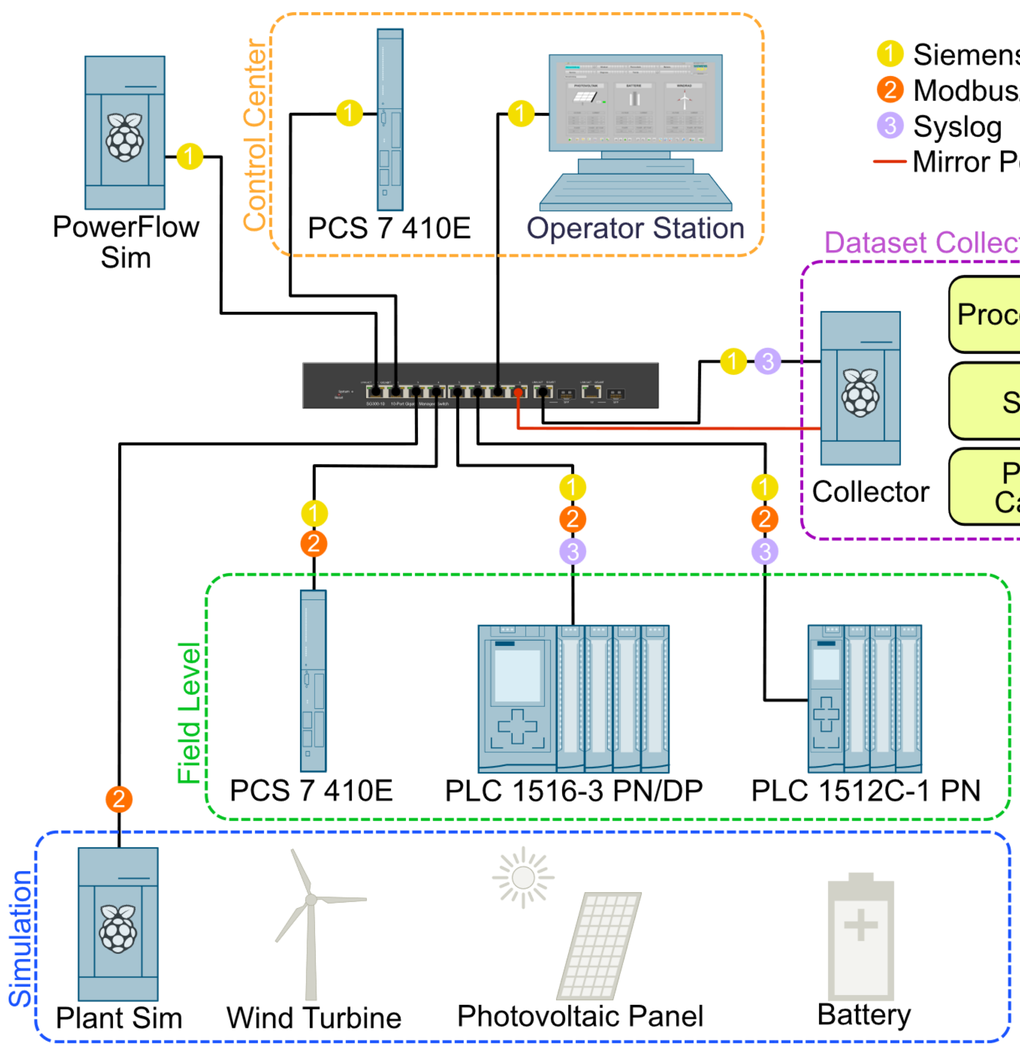
- Open Source attack scripts, IDS and dataset

### Social and Economic Impact

- Design of countermeasures against Data Modification




## Research Activities and Results




- No protection in S7 against data modification
- ➡ Stealthy multi-stage attack: Modify values displayed to the operator in the SCADA HMI to hide an attack on the field level
- IDS help increase security of S7
- ➡ But ML-based IDS are vulnerable to evasion and poisoning attacks; we investigate this using eXplainable Artificial Intelligence (XAI) methods
- Future work: Increase the robustness of learning-based IDS against adversaries that exploit data poisoning and evasion attacks

| Model | Clean | 1% Poison | 2% Poison | 3% Poison | 4% Poison |
|---|---|---|---|---|---|
| **RF** | 98.86 | 92.39 | 86.89 | 70.06 | 68.44 |
| **RF+MLP+SVM** | 98.38 | 93.85 | 86.73 | 72.81 | 68.28 |

RF: Random Forest, MLP: Multi Layer Perceptron, SVM: Support Vector Machine

## Publications


- Attacks on the Siemens S7 Protocol Using an Industrial Control System Testbed. In: e-Energy 2025 (in press).
- Attacking Learning-based Models in Smart Grids: Current Challenges and New Frontiers. In: e-Energy 2024.
- On Evasion of Machine Learning-based Intrusion Detection in Smart Grids. In: IEEE SmartGridComm 2023.


KASTEL