SCPS

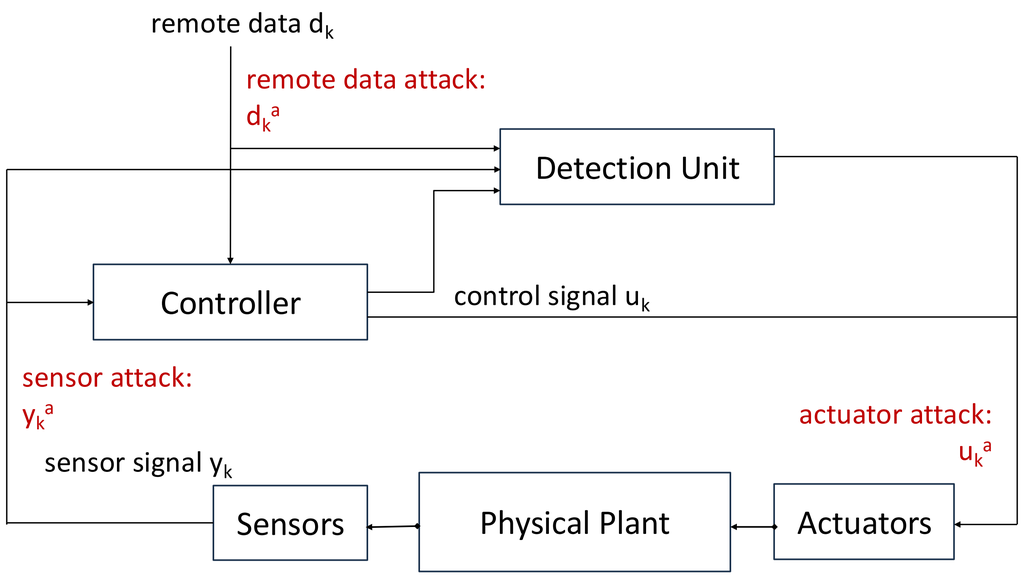
A Model-Based Safety and Security Analysis for Energy Systems

Sibylle Fröschle

Setting and Problem

- Energy systems such as wind farms are operated by SCADA systems, which comprise several layers of networks and control units for data acquisition, (remote) monitoring, and (remote) control.
- The great progress in data-centric methods has led to increasingly sophisticated anomaly detection systems, which typically work on the dynamical system level.
- **Challenge:** These techniques are typically decoupled from the technical level. But it is the latter where attacks are realized and shape what an attacker might be able to do at the dynamical system level.

Generic attack categories for feedback control systems

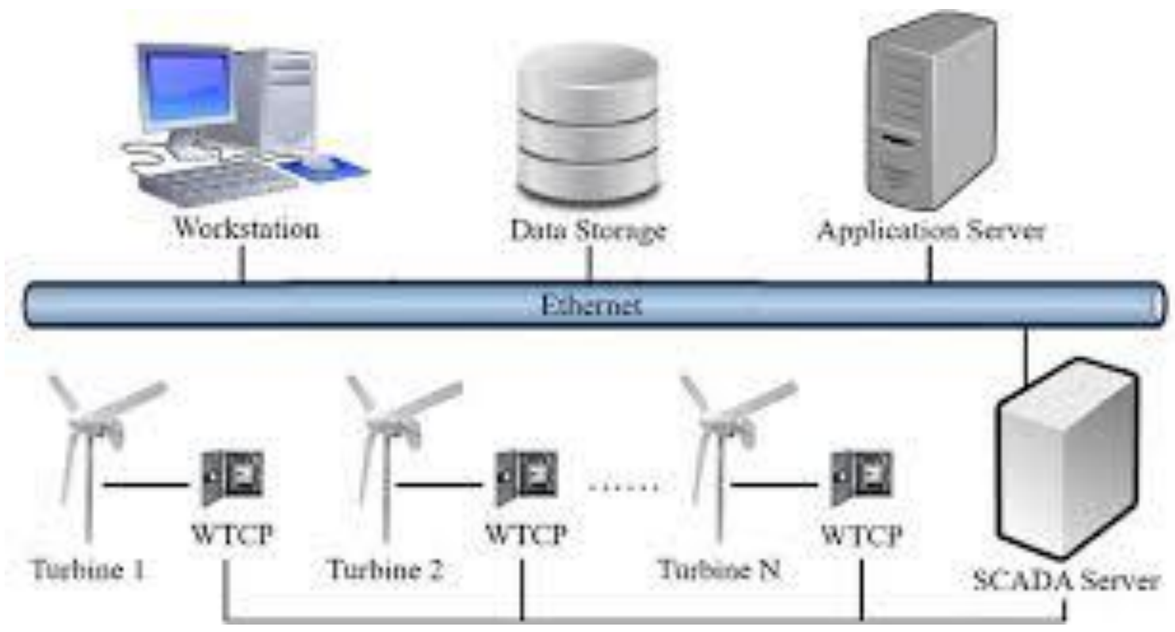


Examples of technical attacks and mitigation measures

CN	Attack	Signals	Mitigation Measures	Constraints	Feasibility
TA1					
FNC1	Wired PitM at C1	All left of C1	—	None	High
FNC1	Wired PitM at C1	All left of C1	Phys. access control	None	Low
TA2					
FNC1	Wired PitM at C1	All left of C1	Phys. access control	None	Low
WLAN1	Wireless PitM	All via AP1	—	None	High
WLAN1	Wireless PitM	All via AP1	Secure passwd & update process	None	Medium
WLAN1	Jamming	All via AP1	—	Only $\perp$ signal	High
TA3					
CAN1	Phys. Attacker	All on CAN1	Phys. access control	None	Low
CAN1	Remote Attacker	All on CAN1	SW Security	No stealthy write with simultaneous read	Medium
CAN1	Remote Attacker	All on CAN1	SW Security Debug lock-down + CAN filter at GW1	Write: only injection	Medium

Publications

- Sibylle Fröschle. The quest for a model-based safety and security analysis: a hybrid solution. Draft paper.
- Sibylle Fröschle and Martin Kubisch. Key establishment for maintenance with machine to machine communication in transportation: security process and mitigation measures. International Journal on Advances in Security, 17(3&4):142-155, 2024.
- Sibylle Fröschle and Martin Kubisch. Three taps for secure machine-to-machine communication: towards high assurance yet fully local machine pairing. In Proceedings of CPS&IoT Security and Privacy, CPSIoTSec'24, pages 125-133. Association for Computing Machinery, 2024.



Source: "Robustness of Short-Term Wind Power Forecasting against False Data Injection Attacks" by Yao Zhang, Fan Lin and Ke Wang is licensed under CC BY 4.0

Our Approach

1. Model generic attack categories for feedback control systems into a representation of the SUC (System under Consideration) as a hybrid system H (e.g. hybrid automaton). Result: the SUT under attack H^A.
2. Tie the analysis at the dynamical system level to an analysis at the technical level to resolve:
   - Relevancy of attack modes, feasibility of the attacker to reach an attack mode, constraints of the attacker on how to manipulate data

   Translate this into model parameters of H^A.
3. Explore whether and how the safety impact can be mitigated by detection measures. Thereby elicit new failure modes specific to attacks or new causes to existing failure modes.

The Overall Process

1. Identify all the computer networks and technical attacks relevant for the SUC H
2. For each technical attack A, evaluate and rate the feasibility of A
3. For each attack mode, evaluate the SUC under attack H^A with the corresponding model parameters, explore detection algorithms, and rate the safety impact.
4. Assess the overall risk based on steps 2. and 3.

Iterate until risk is at an acceptable level

TUHH
Technische Universität Hamburg

Technisch ist das möglich.

Technische Universität Hamburg
Am Schwarzenberg-Campus 1
21073 Hamburg

T. +49 40 428 78-4681
E. scps-sek@tuhh.de
W. https://www.tuhh.de/scps

Institut für Secure
Cyber-Physical Systems
Blohmstr. 15, HIPOne