Foto: Martin Braun

Cyber Security Risks in Power System Operation - How to address this issue as power system researchers

Philipp Linnartz, DigiSect 2023, 21st April 2023

IAEW High Voltage Equipment & Grids, Digitalization & Energy Economics

RWTH AACHEN UNIVERSITY

Introduction

Cyber attacks and power system operation

- **Increasing number of distributed energy resources (DERs) and controllable loads**
- **Deployment of ICT** to monitor and control these assets and to utilize flexibility for operational or market purposes

➢ **Increasing number of remotely controllable actuators**

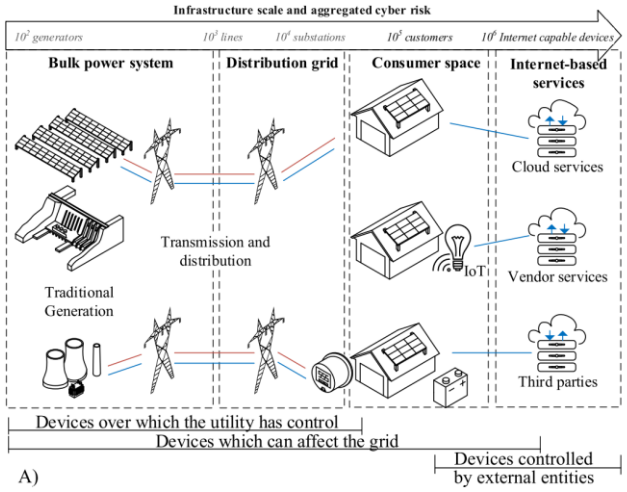
Increasing attack surface and impact potential

- **Cyber attacks** pose an **increasing threat** to the operation of cyberphysical systems, i.e. power systems
- **Already successful attack** that gained access to grid operator control system and led to **serious disruption of services** (Ukraine 2015)

➢ **Power system** as critical infrastructure has to be **resilient against cyber attacks**

How to develop methods to enhance resilience?

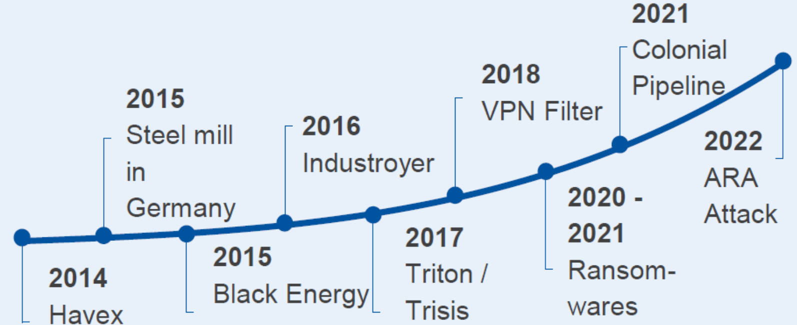
Increasing complexity



Infrastructure scale and aggregated cyber risk
10^2 generators
10^3 lines
10^4 substations
10^5 customers
10^6 Internet capable devices
Bulk power system
Distribution grid
Consumer space
Internet-based services
Transmission and distribution
Traditional Generation
IoT
Cloud services
Vendor services
Third parties
Devices over which the utility has control
Devices which can affect the grid
Devices controlled by external entities
A)

[1]

Cyber attacks on cyberphysical systems



2014 Havex

2015 Steel mill in Germany

2015 Black Energy

2016 Industroyer

2017 Triton / Trisis

2018 VPN Filter

2020 - 2021 Ransom-wares

2021 Colonial Pipeline

2022 ARA Attack

Flexible environment for cyberattack replication

Motivation

Main Issue

- Artificial cyberattacks cannot be applied to critical power system infrastructure
- No cyberattack benchmark data available
- No testing, verification or validation of mitigation strategies possible

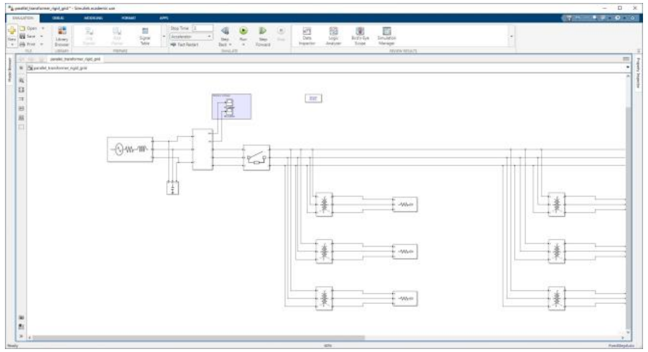
➢ Environment for cyberattack replication necessary

Requirements

- As close to reality as possible
- Flexible & Scalable
- Automated scenario generation, deployment and analysis
- Defined interfaces between hardware and simulation
- …

Suitable environments?

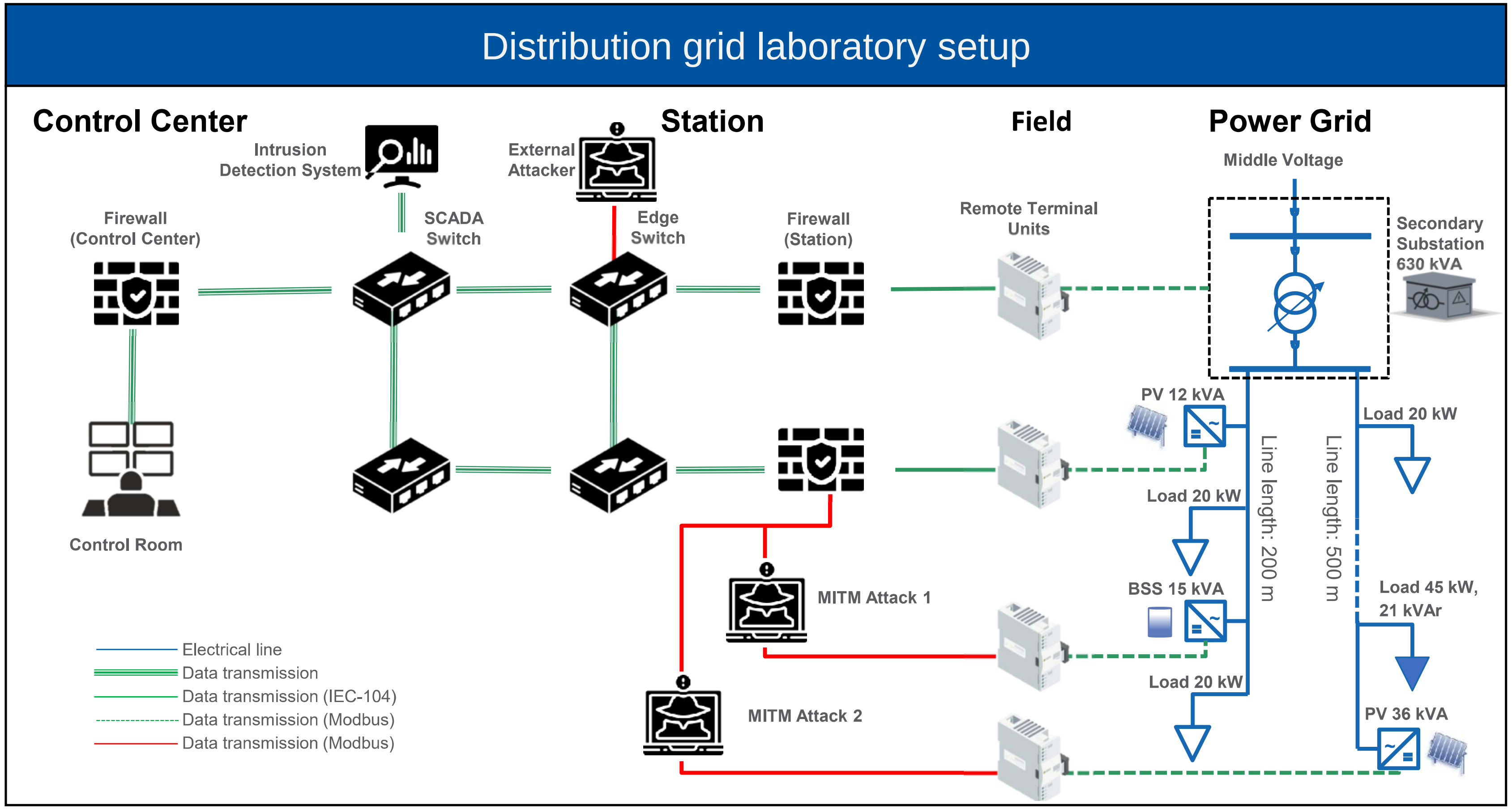
Foto: Martin Braun



Flexible environment for cyberattack replication

Laboratory

- Assets:
  - MV/LV grid with distribution substations
  - DER and loads remotely controllable via RTUs
  - Ring-shaped network topology of including switches and firewalls
  - Grid control room for monitoring and control
  - Communication using standard protocols (IEC 104, Modbus)
- Benefits:
  - Accessible (also for our attacker)
  - Real components, real data traffic
- Drawbacks:
  - Limited number of assets
  - Low flexibility



Flexible environment for cyberattack replication

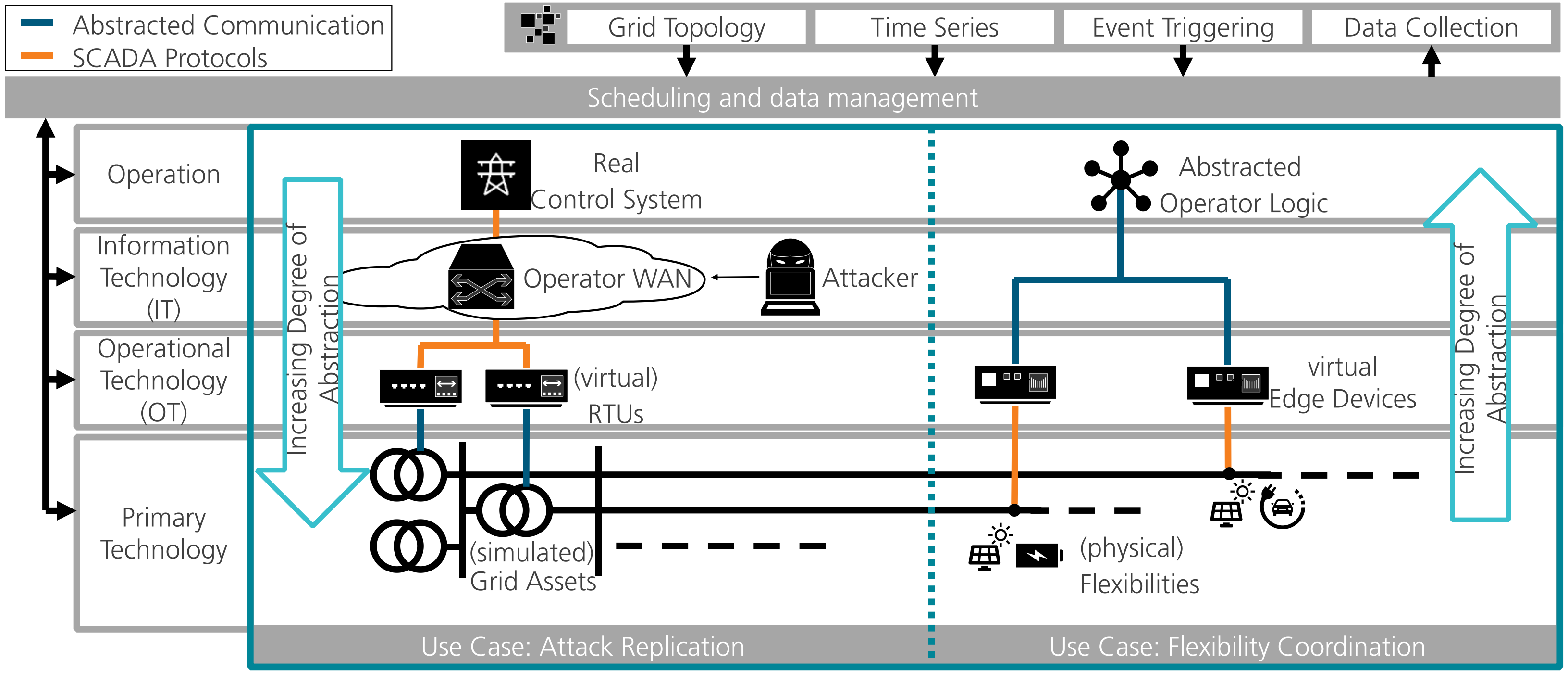
Co-Simulation

- Simulating the power system, operation logics, and (emulating) ICT processes in a common environment
  - Central scheduler synchronizes multiple simulations during operation time
  - Scenario configuration based on infrastructure modeling
  - Various OT and IT devices integrated
- Modularity to depict various use cases

➢ Flexibility and scalability

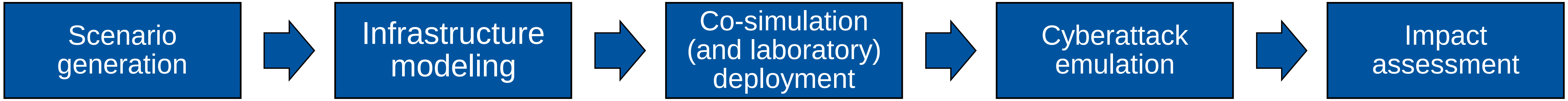
➢ Interfaces to connect hardware

Co-simulation structure and exemplary use cases

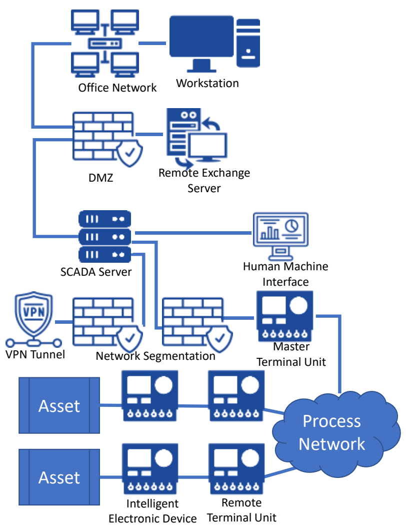


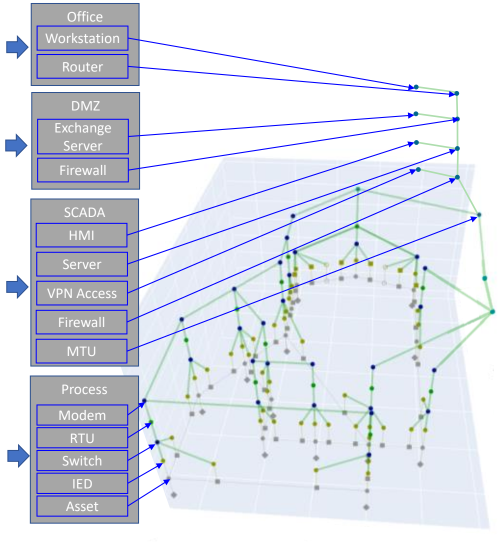
Flexible environment for cyberattack replication

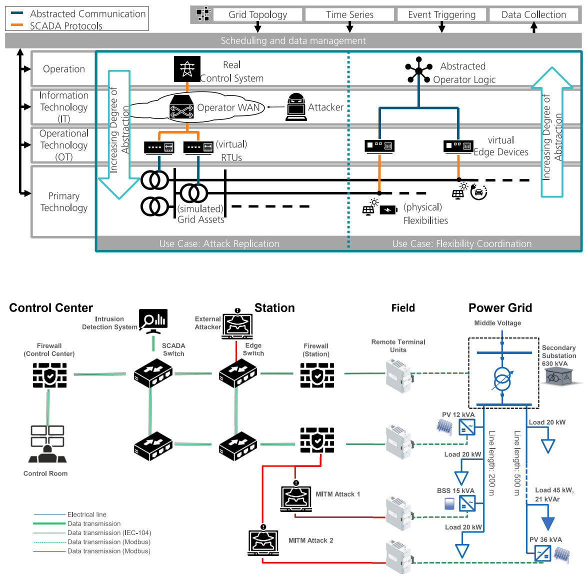
Overview of environment

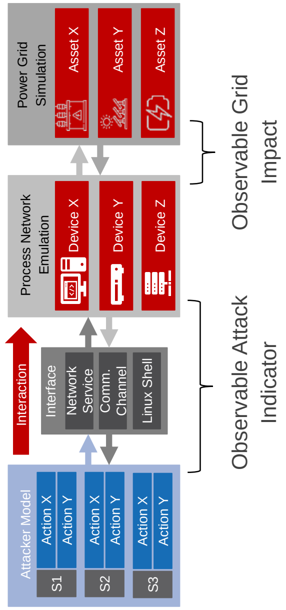


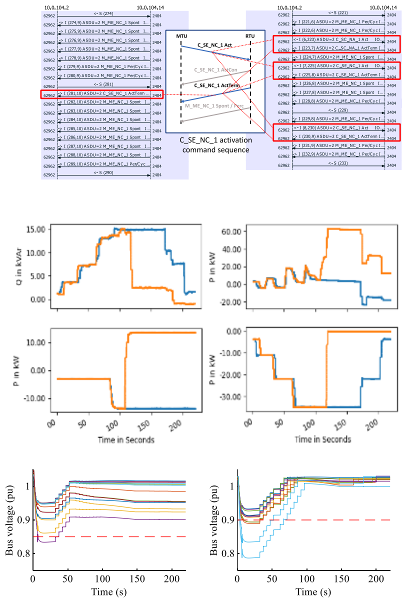
Scenario generation → Infrastructure modeling → Co-simulation (and laboratory) deployment → Cyberattack emulation → Impact assessment











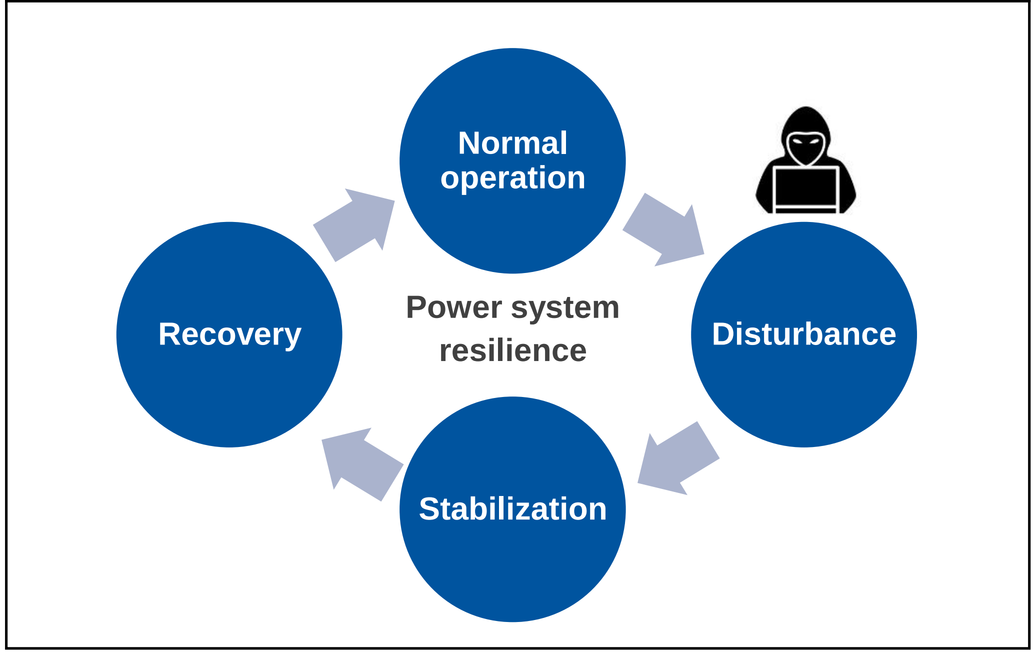
Environment enables flexible and scalable analysis of multi-staged cyber-attacks

Flexible environment for cyberattack replication

Use cases

- Flexible environment for cyberattack replication can be used for:
  - Development and verification of concepts and systems (e.g., intrusion detection systems)
  - Generation of attack data / datasets
  - Training (e.g. response of operator personnel) and teaching
  - Testing of operational and control concepts and strategies
  - …
- **Goal:** Develop and implement concepts to make power system operation resilient against cyberattacks

Power system resilience



Normal operation

Disturbance

Stabilization

Recovery

Power system resilience

Looking forward to the discussion

Philipp Linnartz

Chief Engineer
Active Energy Distribution Grids
IAEW at RWTH Aachen University

p.linnartz@iaew.rwth-aachen.de

References & Acknowledgements

[1] D. J. S. Cardenas, A. Hahn and C. -C. Liu, "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations," in *IEEE Access*, vol. 8, pp. 61161-61173, 2020, doi: 10.1109/ACCESS.2020.2983313

Funded by (excerpt):

BEAUTIFUL

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

MEDIT
Prävention, Detektion und Reaktion
bei IT-Angriffen und -Ausfällen

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

PHOENIX
Electrical Power System's Shield
against complex incidents and
extensive cyber and privacy attacks

European
Commission
Horizon 2020
European Union funding
for Research & Innovation

Research environment developed in close cooperation with experts from:

Fraunhofer
FIT