Cybersecurity Research and Training for Power Distribution Grids: A Blueprint

Fraunhofer FKIE
lennart.bader@fkie.fraunhofer.de
martin.henze@fkie.fraunhofer.de

Motivation

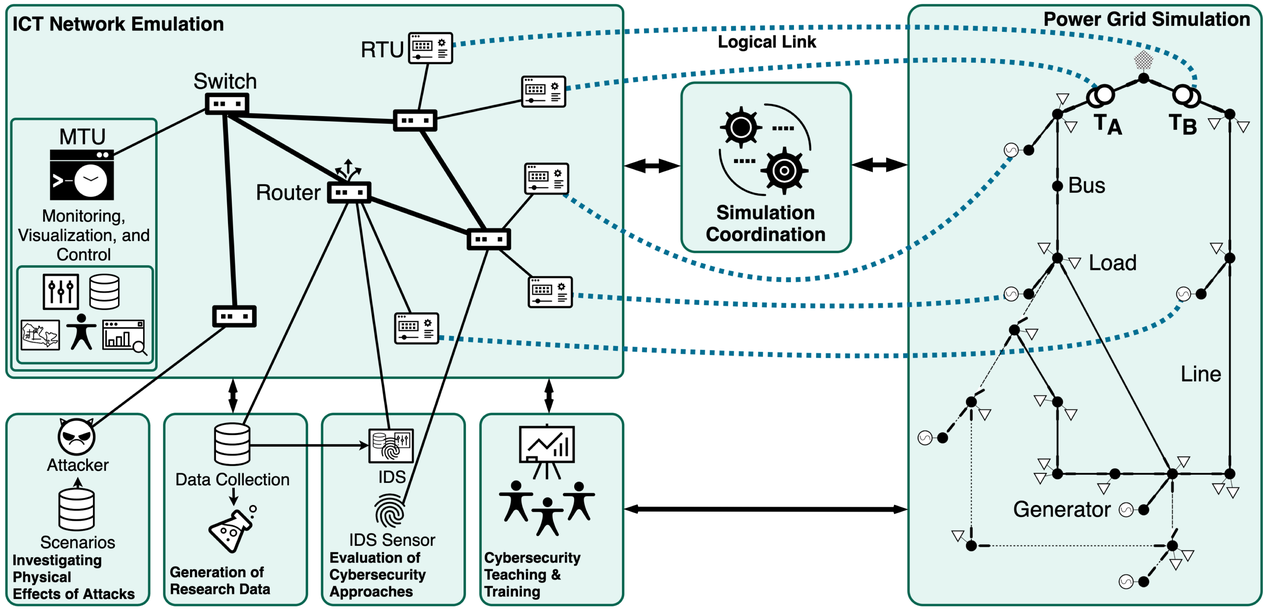
Ongoing Digitalization in Power Grids

- Increased susceptibility to cyberattacks
- Especially relevant for power *distribution* grids
  - Heterogenous environment
  - Direct interaction with prosumers

Attack Prevention and Reaction Mechanisms

- Potentially disastrous consequences
  - Physical interactions increase complexity
- **Required: Sophisticated research and training environment**
  - Covering power grid and ICT

Cybersecurity Research and Training Architecture



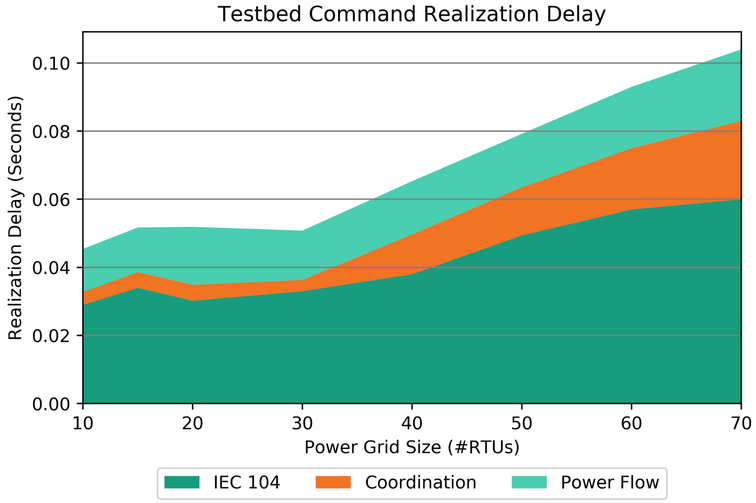
Co-Simulation Framework

- Network emulation (Mininet + Open vSwitch)
- Power grid simulation (Pandapower)
- Dedicated coordination

Realistic Networking

- Virtual links and interfaces
- Realistic traffic and protocols (e.g., IEC 60870-5-104)
- RTUs, MTUs, switches, routers, control center, monitoring, attackers, …

Early Results



ICT Emulation Feasible for Current Systems

- Less than 65 MiB RAM per RTU
- Mininet evaluation promises sufficient scalability
  - Hundreds of switches and hosts
- Architecture currently under advanced evaluation

Low Latency for Power Grid Simulation

- Power flow computations take a few milliseconds
  - About 20 ms for a 70 bus grid
- Influence of grid structure and size under active evaluation

Outlook

Full Implementation

- Docker containers
- Scalable and distributed multi-host setup

Additional Use Cases

- Real-world intrusion detection systems
- Attacker scenarios

Performance Evaluation

- Communication network scalability & throughput
- Real-time capabilities

Validation of Realism

- Validate against physical distribution grid
- Iterative improvements