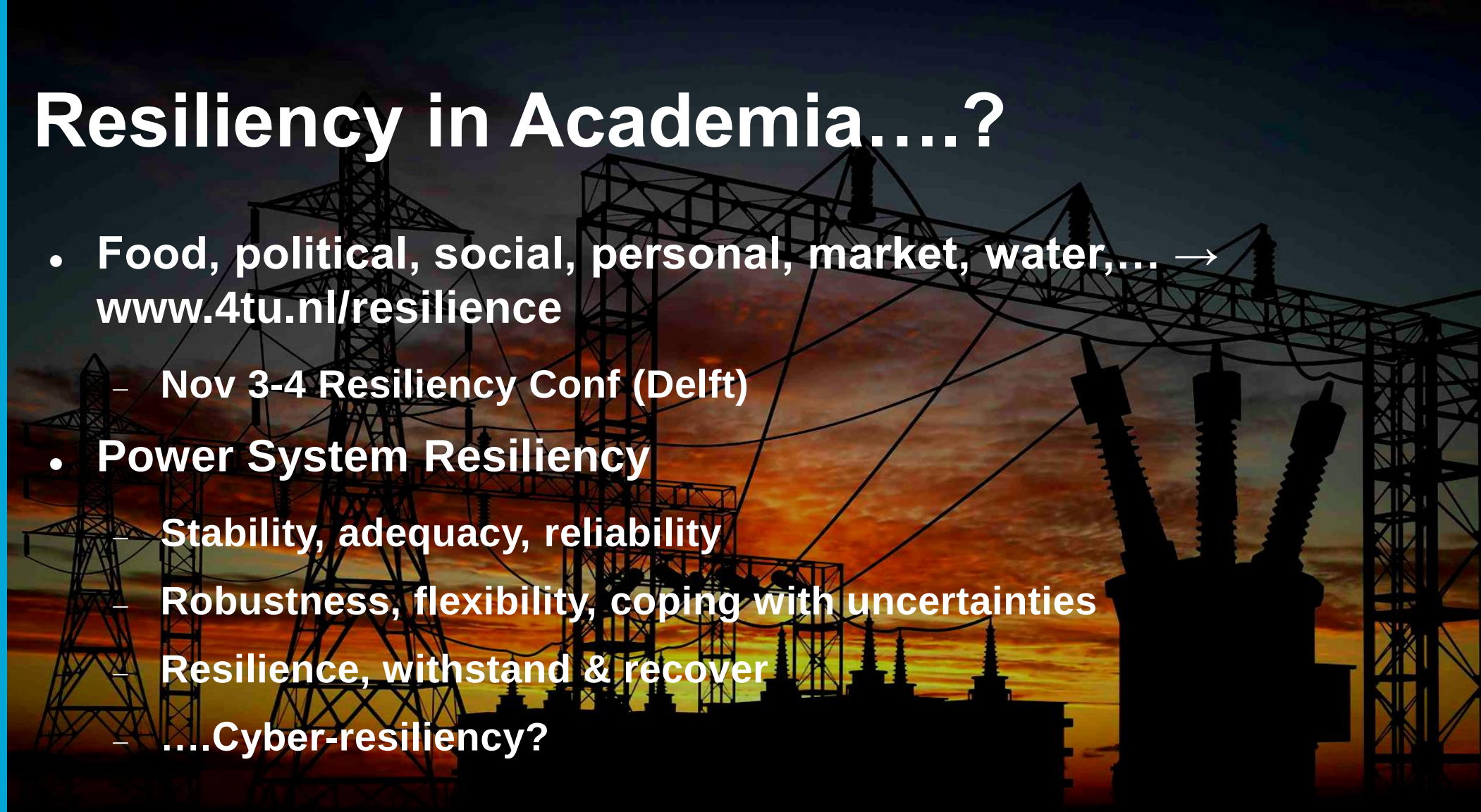
Academic view on resilience

CIGRE C0 Seminar 2022 on
critical infrastructure and cyber security

Peter Palensky
TU Delft

Resiliency in Academia….?

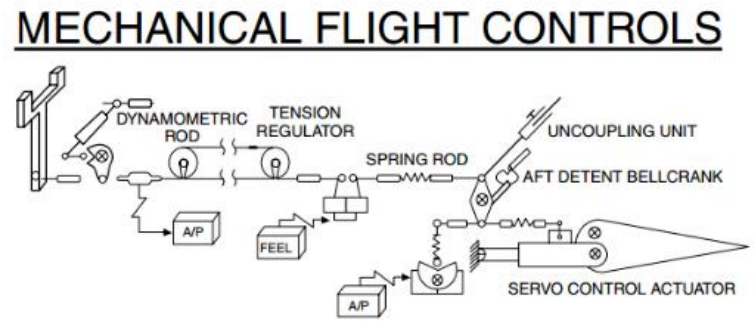
- Food, political, social, personal, market, water,… → www.4tu.nl/resilience
  - Nov 3-4 Resiliency Conf (Delft)
- Power System Resiliency
  - Stability, adequacy, reliability
  - Robustness, flexibility, coping with uncertainties
  - Resilience, withstand & recover
  - ….Cyber-resiliency?

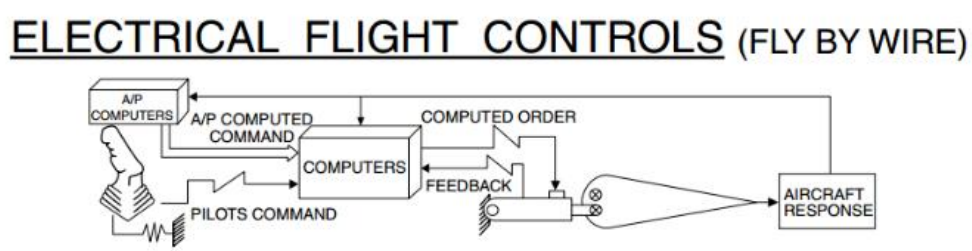


TU Delft

Crystal Ball for Power Sector!

- Mil, Avionics, Automotive, IT(?)
  - Cruise missile, A320, Tesla, AI/ML
- Fly-by-wire
- Redundancy
- Car2X communication
  - Cyber-sec?





Web3: flat, distributed, virtual?

Resilient!

Gold

Fiat

Crypto

Physical

Central Agreement

Distributed Agreement

Local Fuel

Power System

Energy Community

ICT: benefit or threat to resiliency?

- Active assets ownership diversity
- Digital identity management
- Supply chain for digital assets (firmware update, patches)
- Admin, scalability,…
- …stay with centralized card-house?

Image: NREL

Question...

Digital Substations, IEC 61850, PMUs, …

good (GREEN) or

bad (RED)

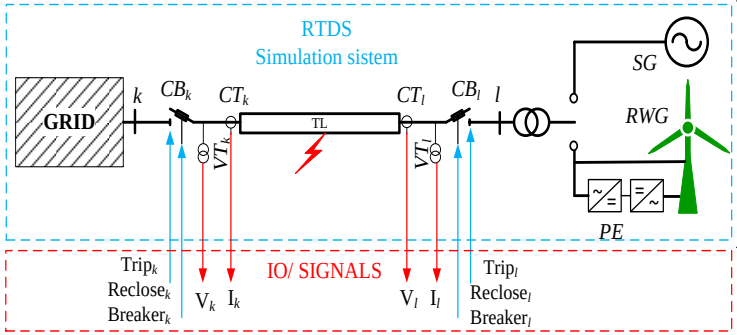
for power system resiliency?

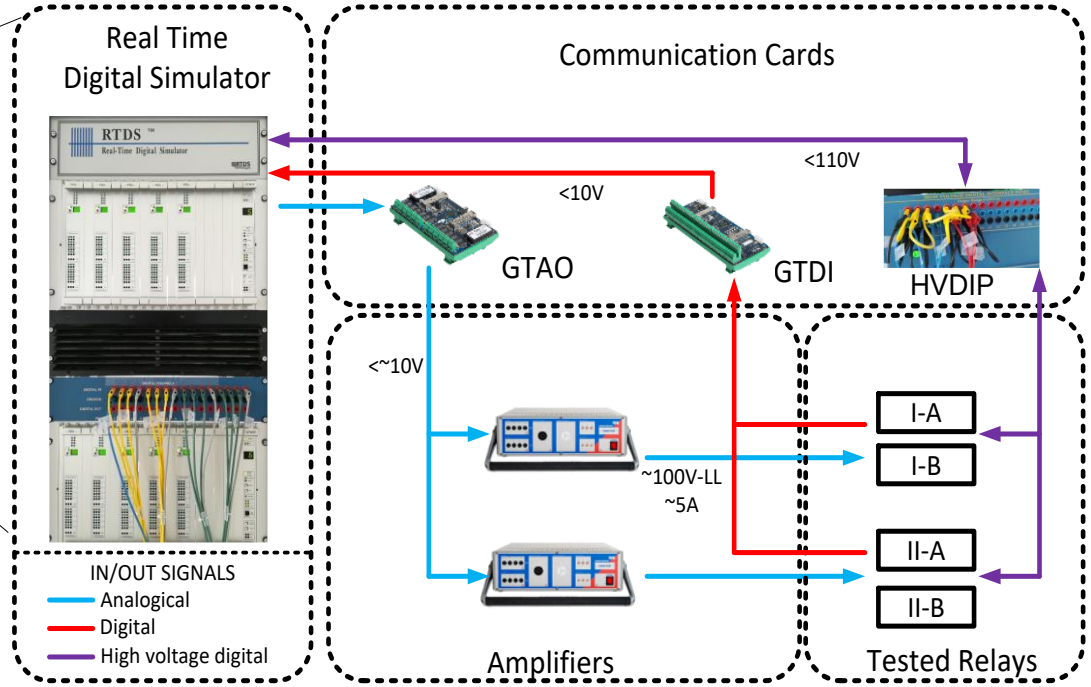
TU Delft

Activities in Academia

- Research
  - “Old”: risk assessment, stability, reliability,...
  - New: intrusion detection, swarm behavior, planning and operations under uncertainty, system-of-systems,...
  - Cyber-physical (social-stochastic-economic…) system
  - **Master complexity**: analytical, data-driven, numerical
- Education
  - Students, future and current workforce
  - Training with digital twins in labs

Ex 1: numerical experiments with power system protection

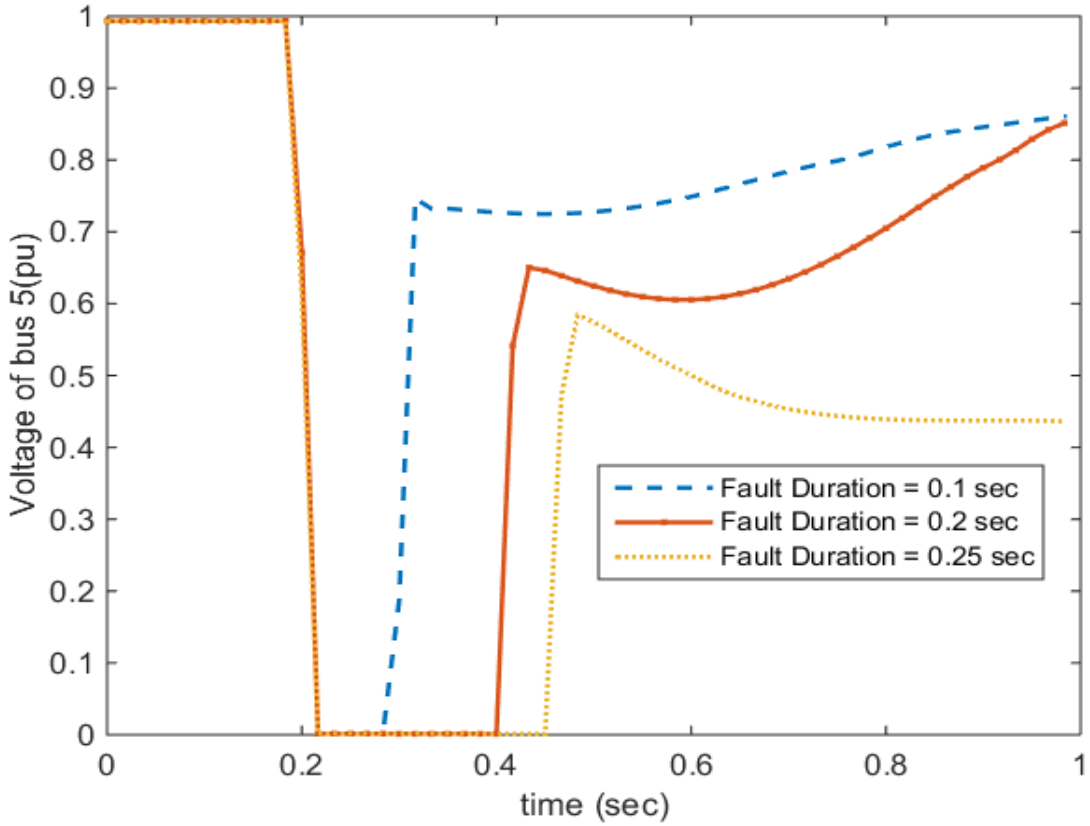


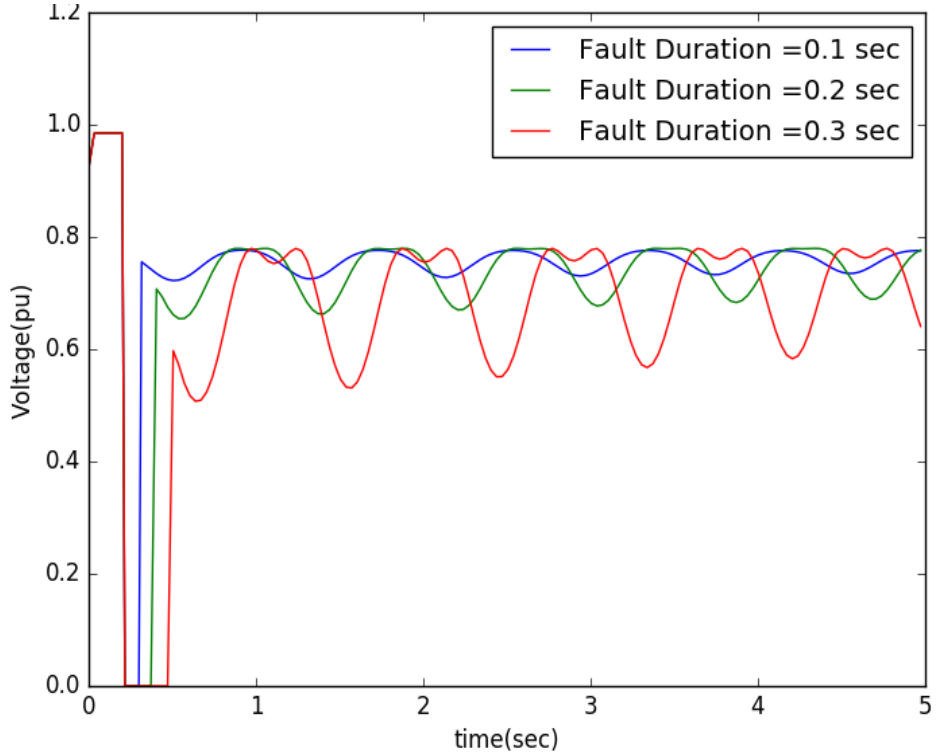


- Massive batch processing
- Interfacing?
- Open Benchmark Cases?
- Open Data Sets?
- Confidentiality?

HIL: Hardware-in-the-Loop

Ex 2: Forecasting Voltage Stability

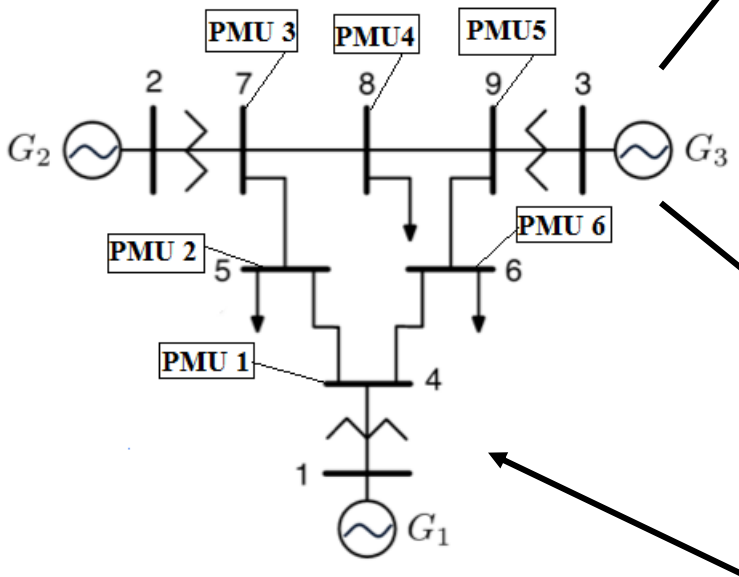




Faster-than-real-time twins?

validation?
coverage?

Real System



Identification → Model

AI/ML

Signatures

Surrogate

Offline Learning

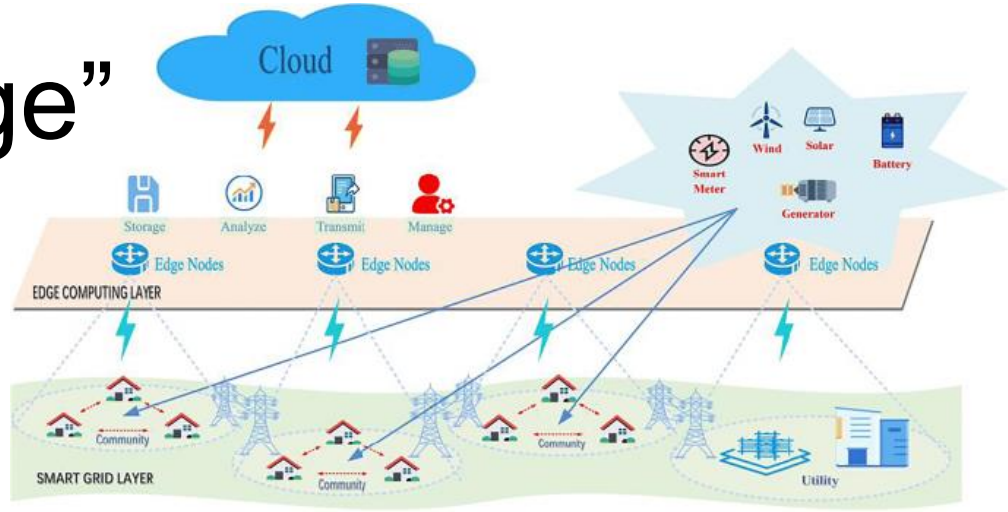
Non-RT

Detection → (smart) Forecast → Scenario

incl. remedial actions?

Classification → Robust Decision

Ex 3: Smart “Grid Edge”



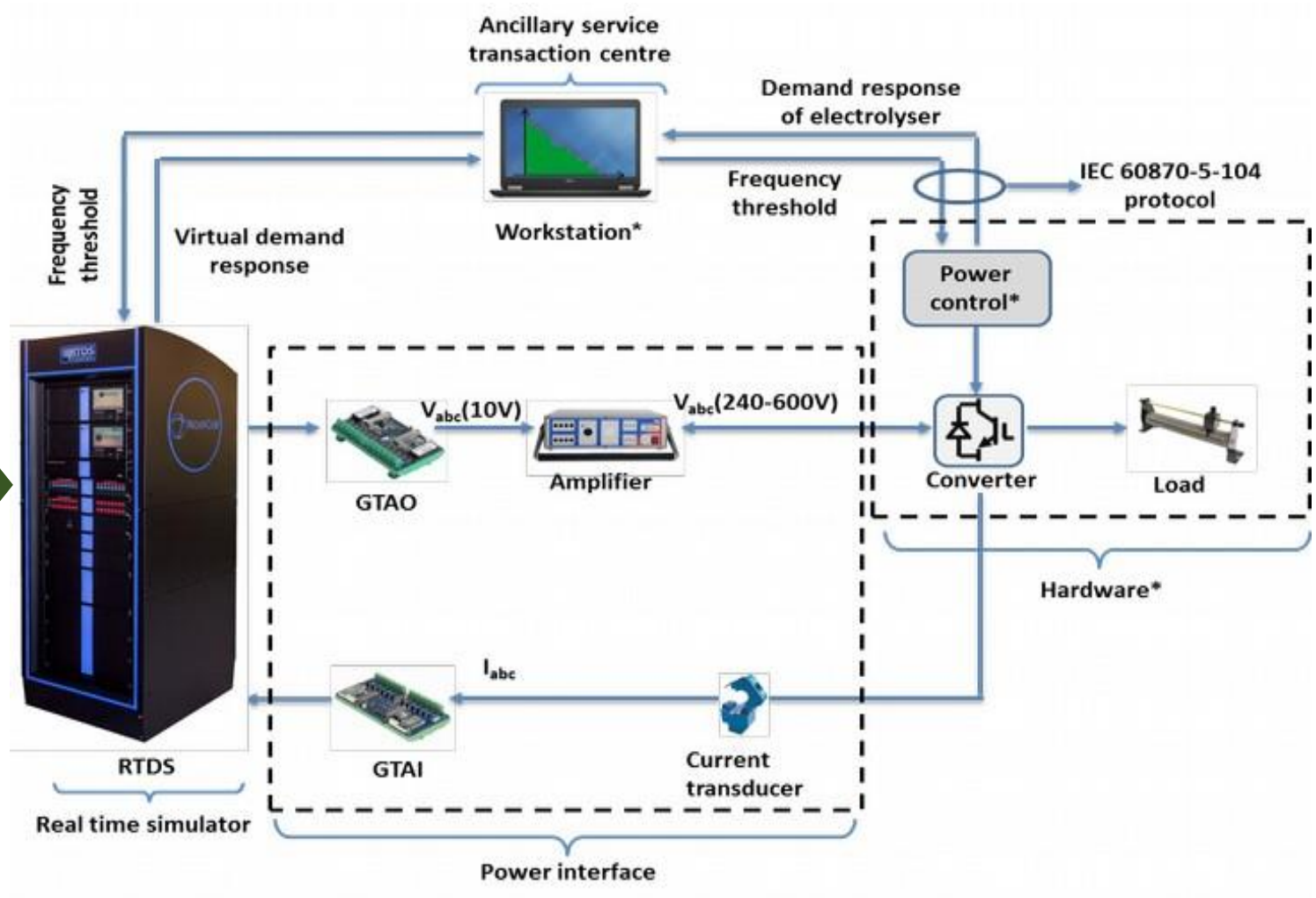
- IoT-enabled
  heat-pump, PV panel,
  EV charging pole,
  A/C, batteries,…
- Contribute to ancillary and local services
- Reliability? Statistical methods...
- Ownership of data, functions,…?
  - EU “Data Act” in preparation (GDPR for IoT)
  - New role for grid companies?

IoT: Internet of Things
PV: Photovoltaics
EV: Electric Vehicle
A/C: Air Conditioning
GDPR: General Data Protection Regulation

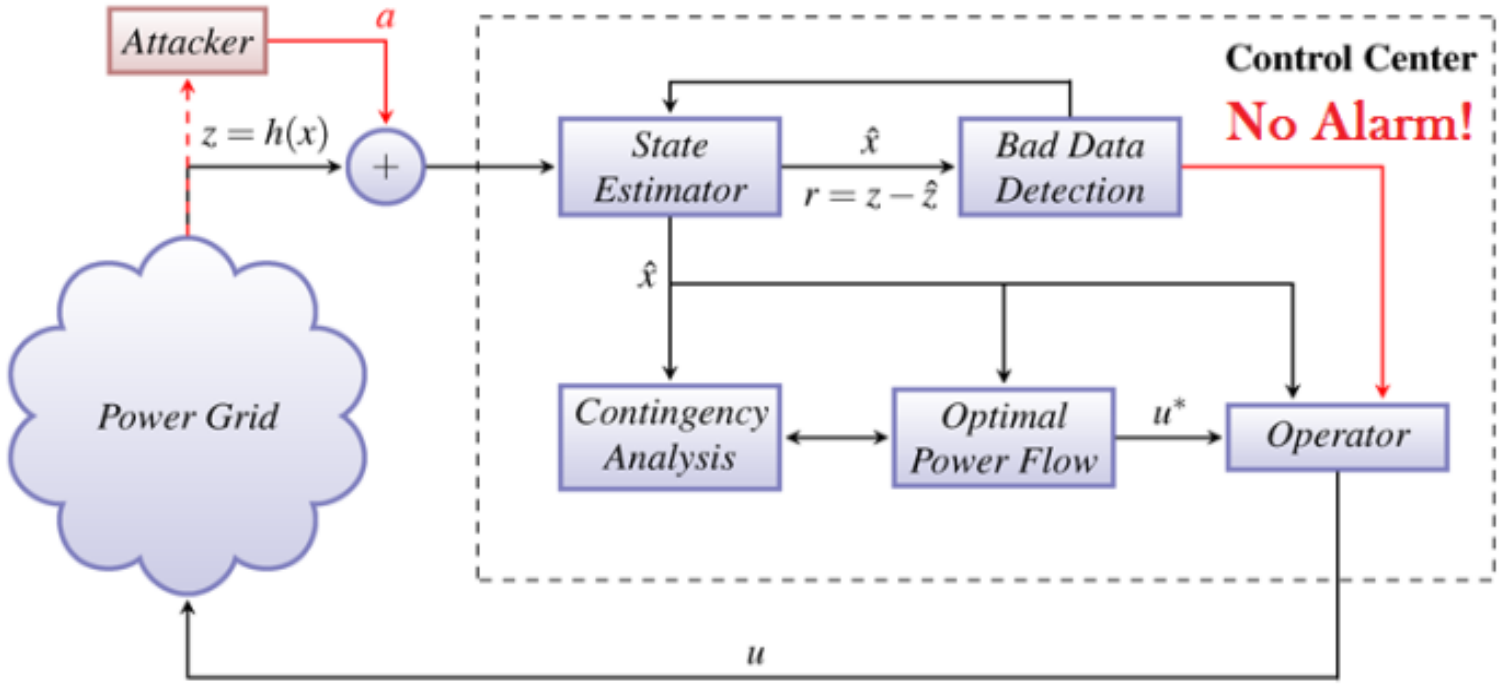
Ex 4: Ancillary Services of Hydrolyzers

EMT system model

North Netherlands (year 2030)

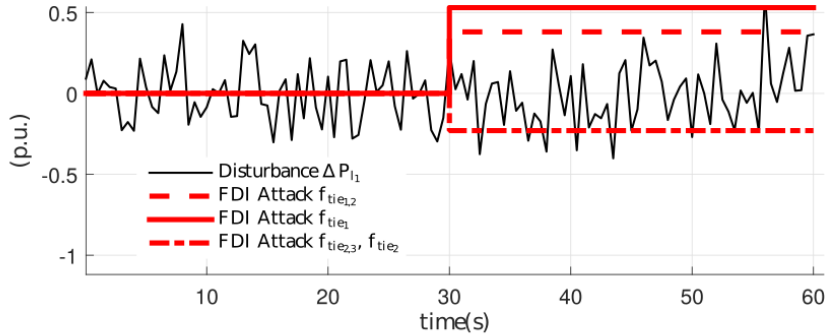


Ex 5: Sophisticated attacks coming...



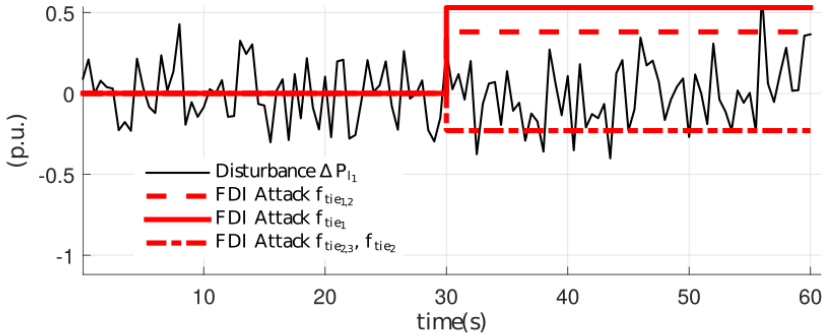
- Energy Management System
- Stealthy Attacks
- Theft, vandalism warfare
- Cascading effect

Cyber-physical attack

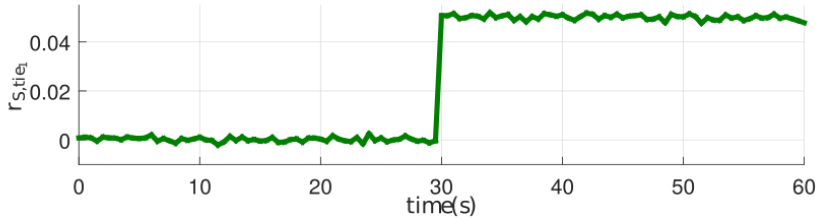


FDI: false data injection

Cyber-physical attack



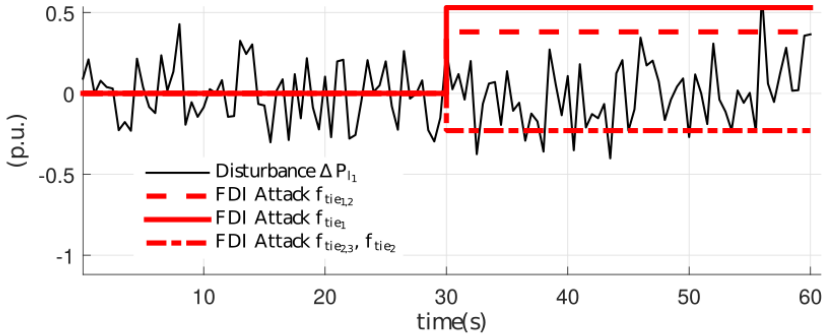
(a) Load disturbance and unstealthy attack



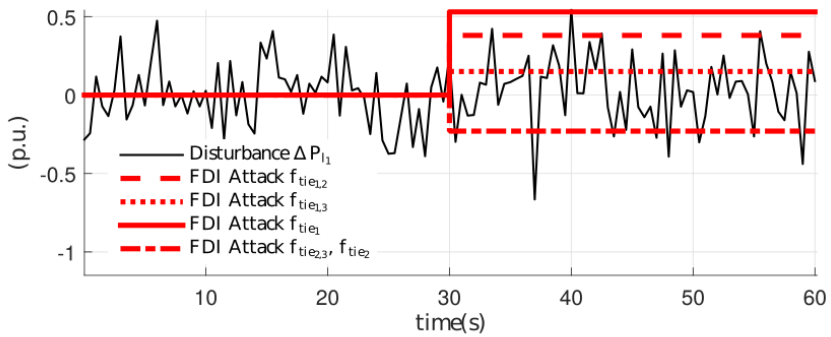
(c) Residual of static detector under unstealthy attack

FDI: false data injection

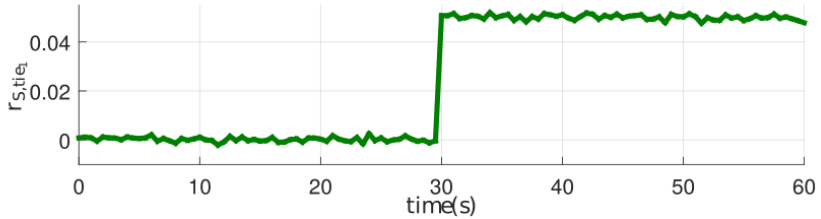
Cyber-physical attack: undetected



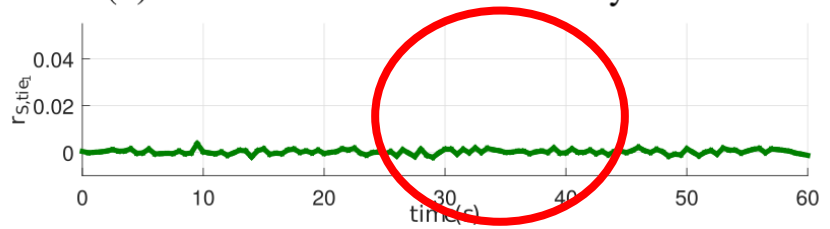
(a) Load disturbance and unstealthy attack



(b) Load disturbance and stealthy attack



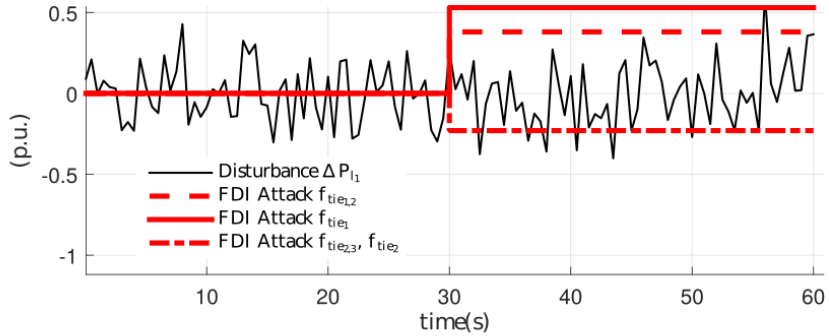
(c) Residual of static detector under unstealthy attack



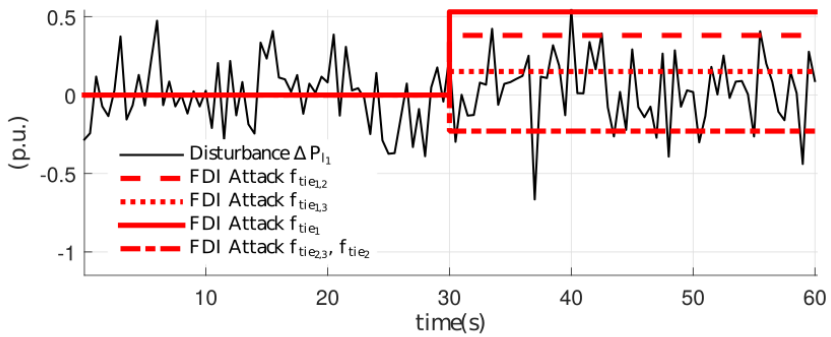
(d) Residual of static detector under stealthy attack

FDI: false data injection

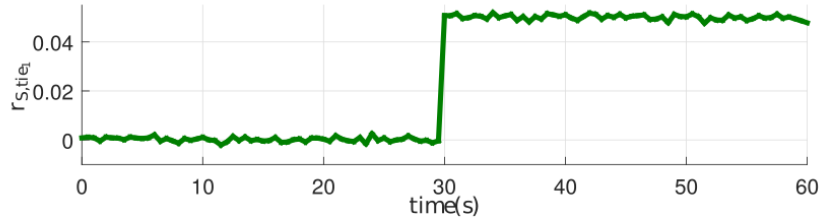
Cyber-physical attack: detected (analytically!)



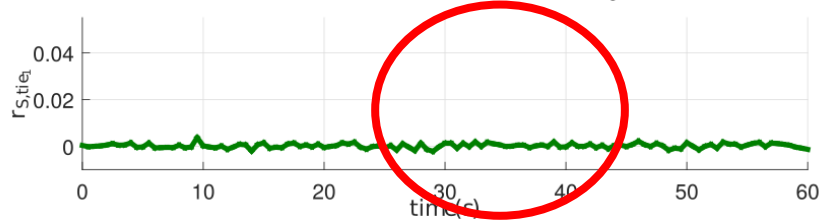
(a) Load disturbance and unstealthy attack



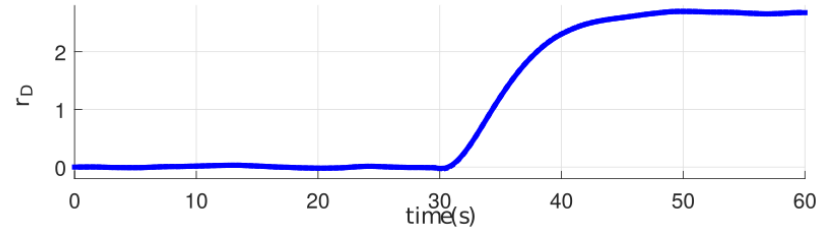
(b) Load disturbance and stealthy attack



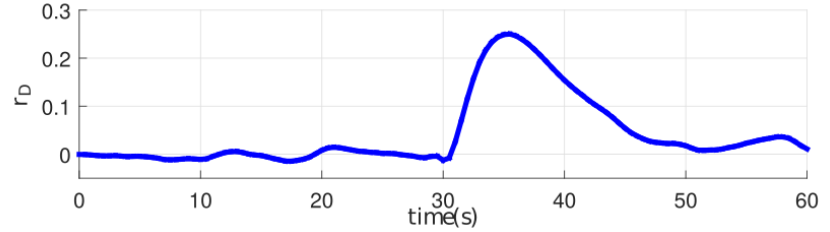
(c) Residual of static detector under unstealthy attack



(d) Residual of static detector under stealthy attack



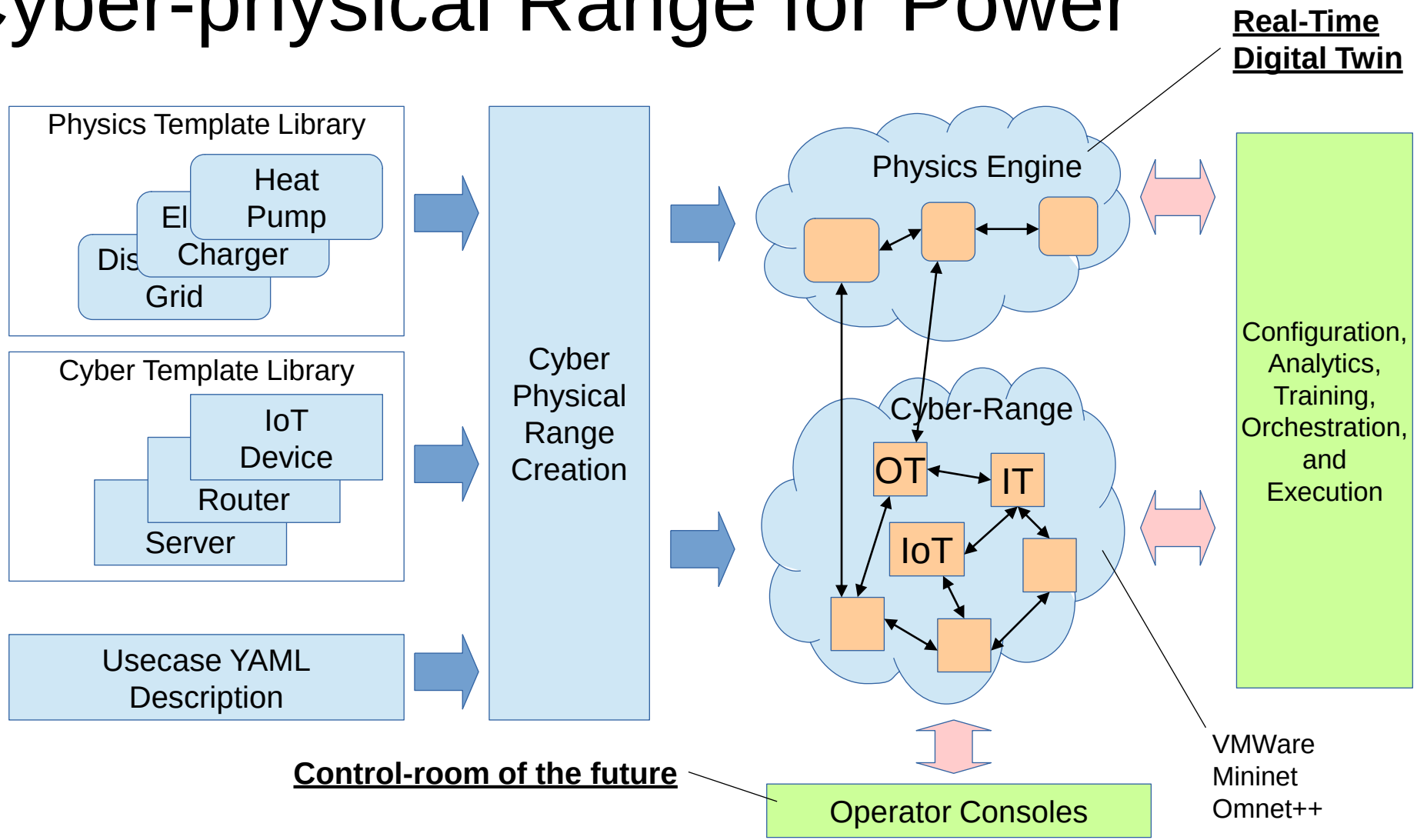
(e) Residual of dynamic detector under unstealthy attack



(f) Residual of dynamic detector under stealthy attack

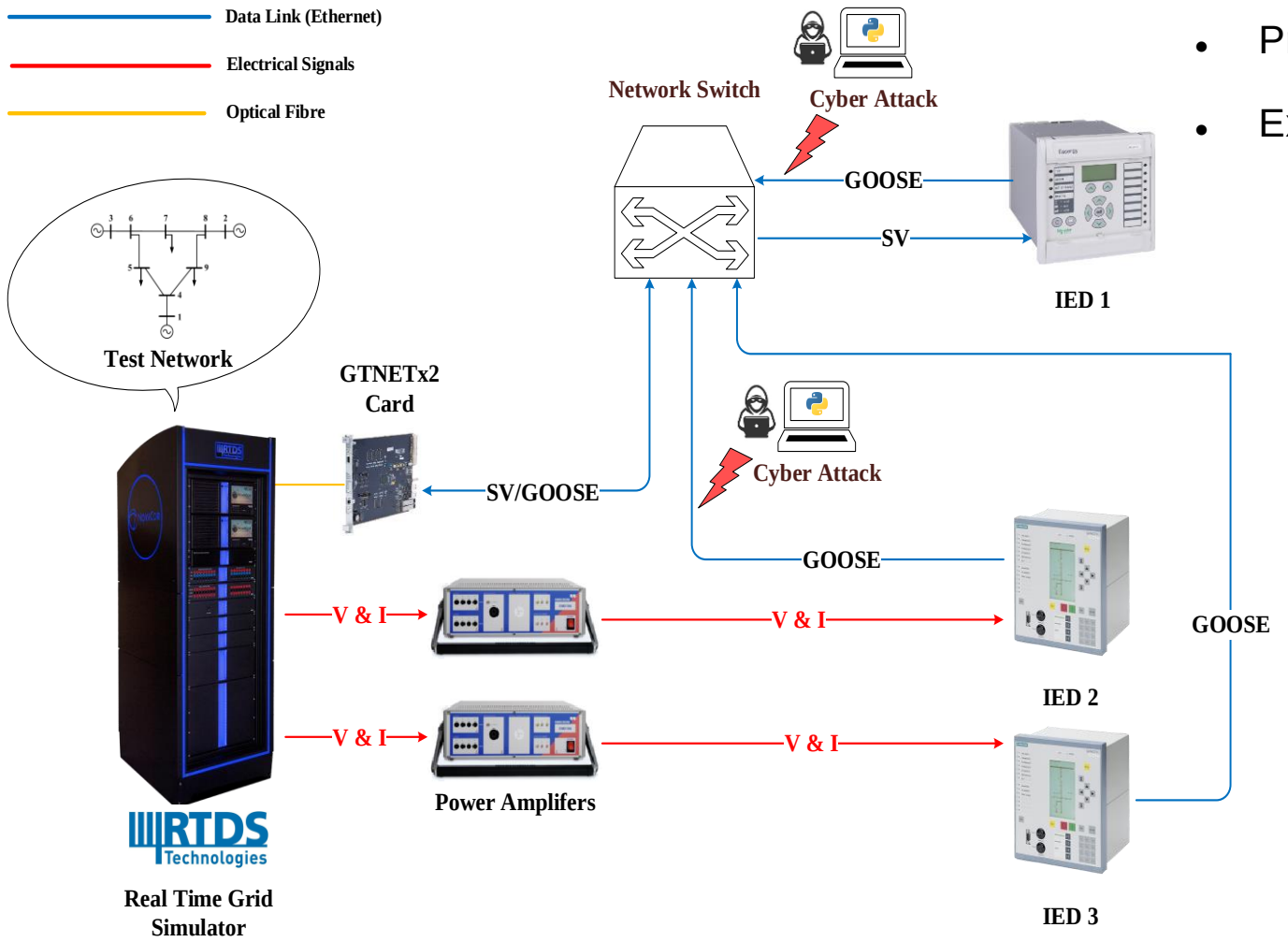
FDI: false data injection

Cyber-physical Range for Power



Cyber Attack Analysis

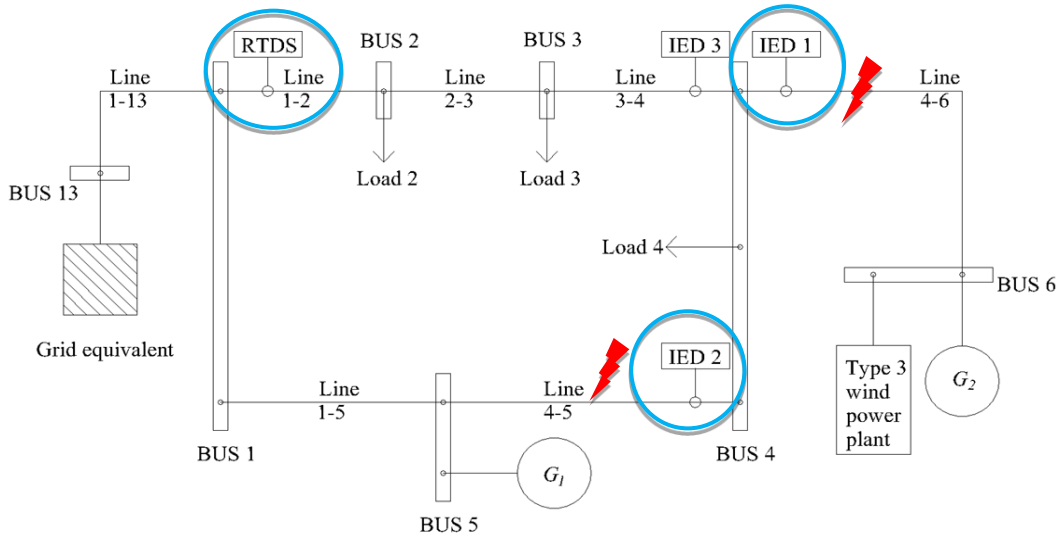
- Reconnaissance
- Preparation
- Execution



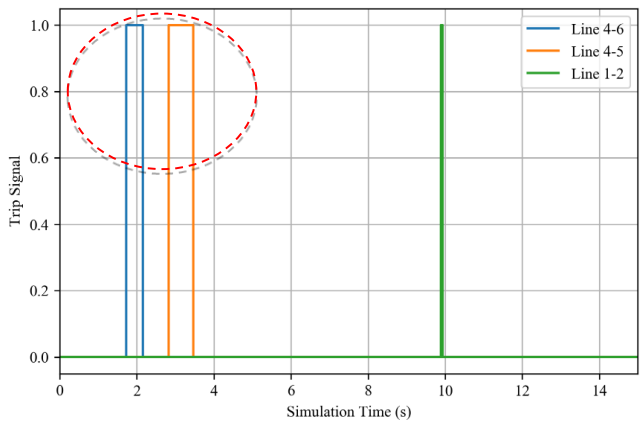

```
    Type: IEC 61850/GOOSE (0x88b8)
GOOSE
    APPID: 0x8000 (32768)
    Length: 156
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  goosePdu
      gocbRef: P446_SVSystem/LLN0$GO$gcb01
      timeAllowedtoLive: 2001
      datSet: P446_SVSystem/LLN0$OPGOOSEDataset
      goID: P446_GOOSE
      t: Mar 17, 1994 22:13:49.941999971 UTC
      stNum: 1
      sqNum: 23628
      test: False
      confRev: 3
      ndsCom: False
```

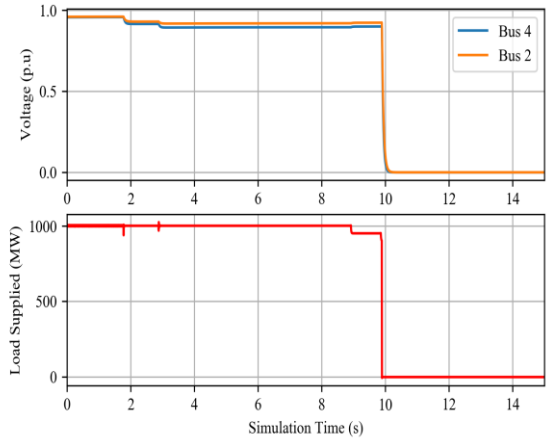
Wireshark snippets GOOSE data frame

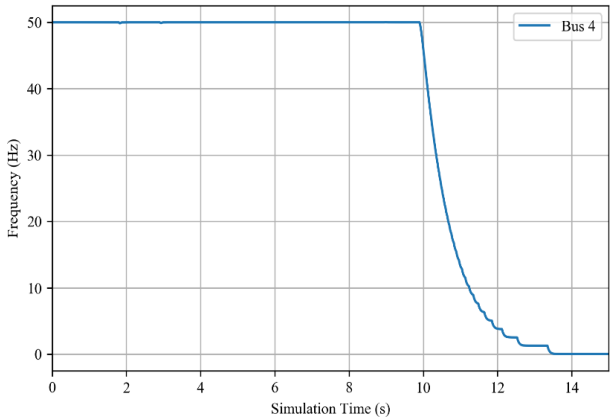
Coordinated Attacks (N-1 anyone?)



- Coordinated GOOSE cyber attack on IEDs 1 and 2, type “Flevoland” ;-)
- Lines 4-6, 4-5 disconnected. G1 lost
- Voltage drops below limit of 0.92 p.u
- Overload protection trips line 1-2 (1.1 p.u, delay 7s) after cyber attack
- Leads to cascading failure and blackout







TU Delft

TU Delft

Take aways

- Academia is neither army nor consultant
- Academia is a partner that grows with you
- Resilient digital transformation “done right”?
  - Security by design, auditable
- Complexity: there is help!

Question...

Self-organization, distributed control, market-based control,…

good (GREEN) or

bad (RED)

for power system resiliency?


TECHNISCHE UNIVERSITEIT DELFT
MDCCCXLII