Cyber-Physical System Resiliency and Cyber Security

Dr. Alex Stefanov

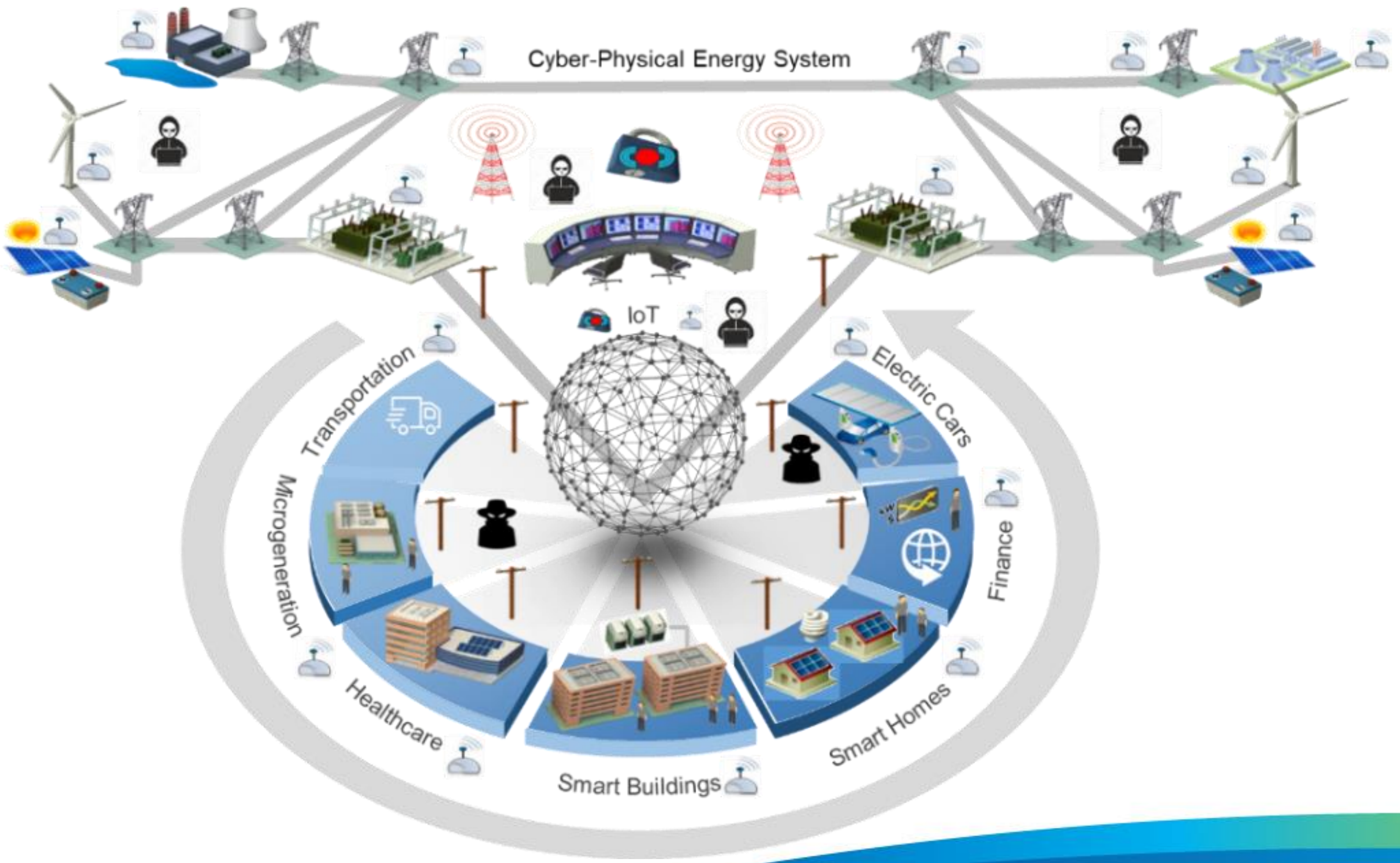
Assistant Professor, Chartered Engineer

4TU.Resilience Engineering, DeSIRE Conference 2022

November 3, 2022

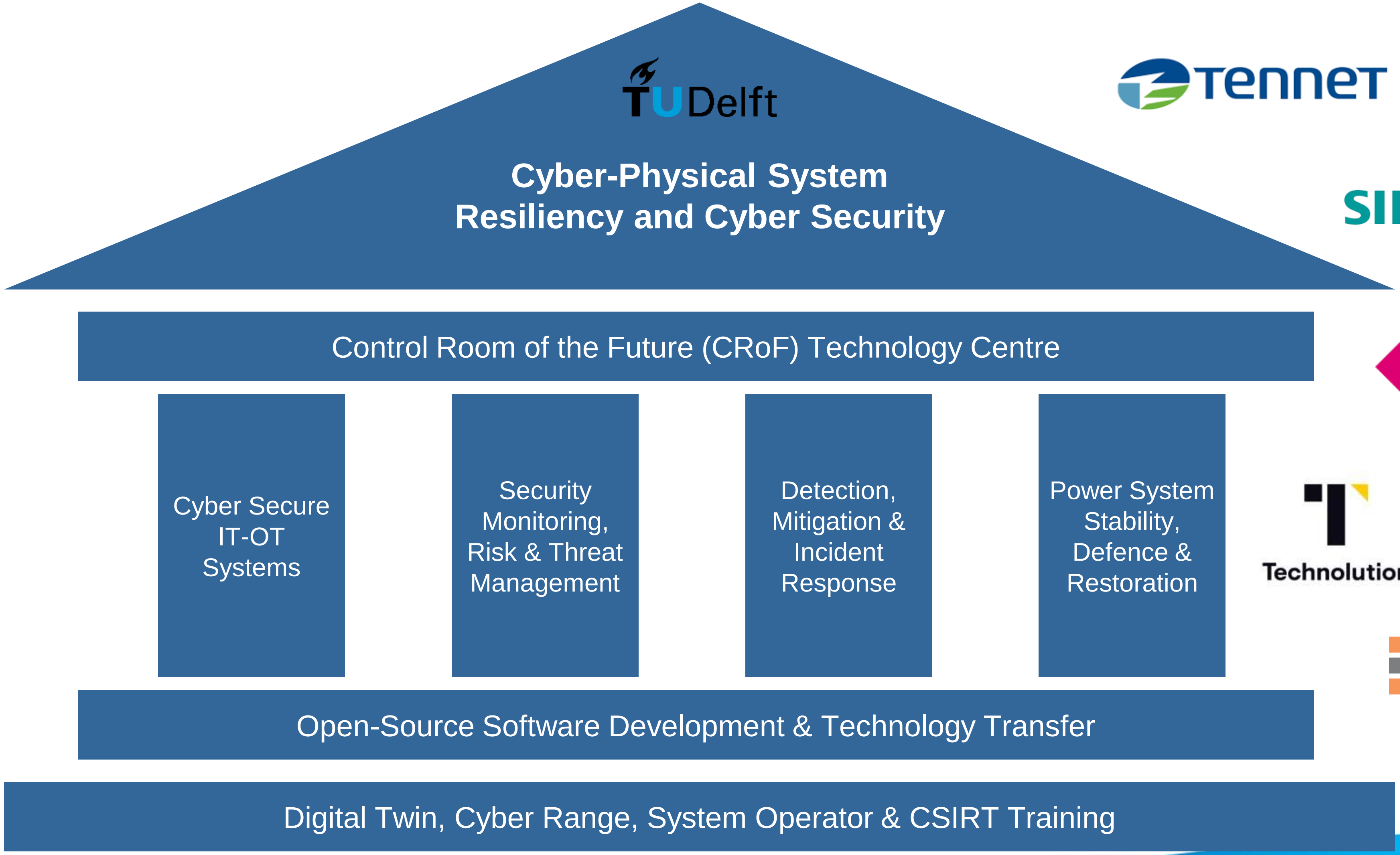
Cyber Security and Resilience of Power Grids

- Energy transition: decarbonisation, decentralisation and digitalisation
- Digitalisation introduces new cyber security threats in smart grids



[Stefanov *et al*. Probabilistic Reliability Analysis of Power Systems, Springer, 2020]

Brand New Research Programme at TU Delft



TU Delft

Cyber-Physical System Resiliency and Cyber Security

Control Room of the Future (CRoF) Technology Centre

Cyber Secure IT-OT Systems

Security Monitoring, Risk & Threat Management

Detection, Mitigation & Incident Response

Power System Stability, Defence & Restoration

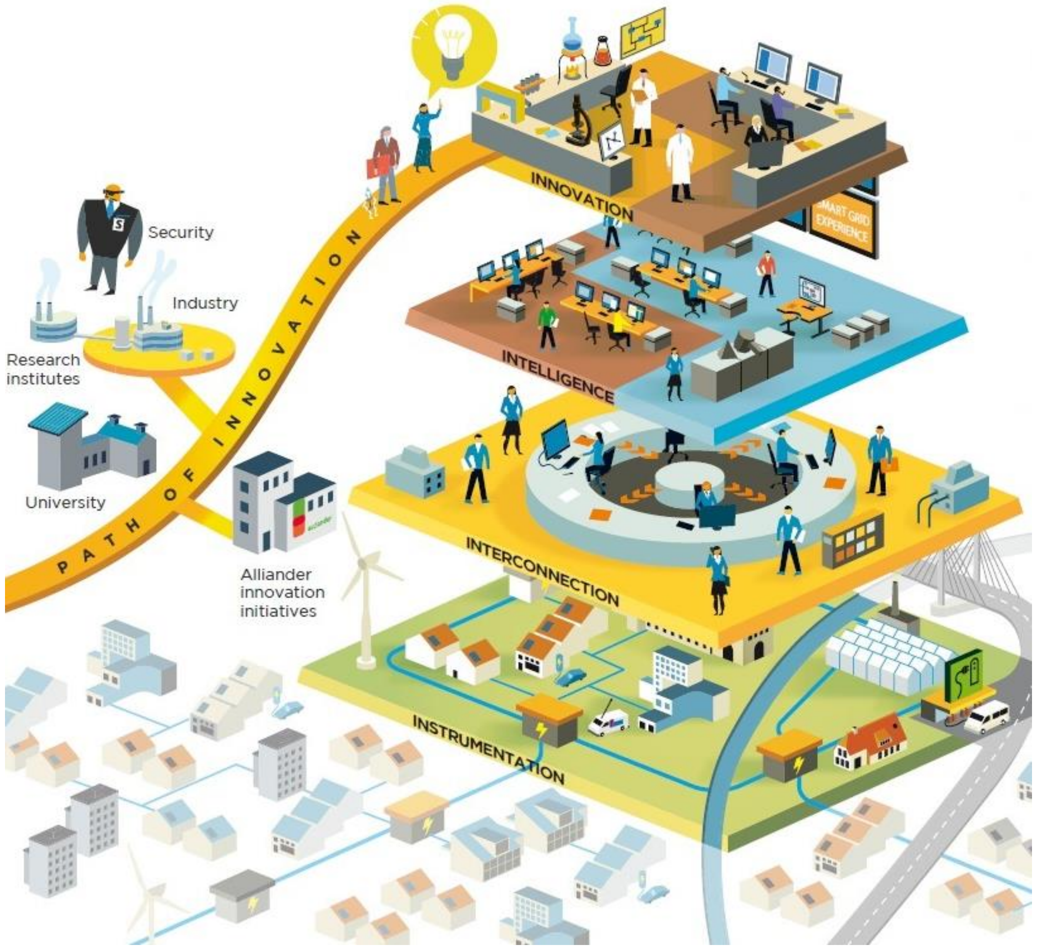
Open-Source Software Development & Technology Transfer

Digital Twin, Cyber Range, System Operator & CSIRT Training

Control Room of the Future (CRoF) Technology Centre at TU Delft

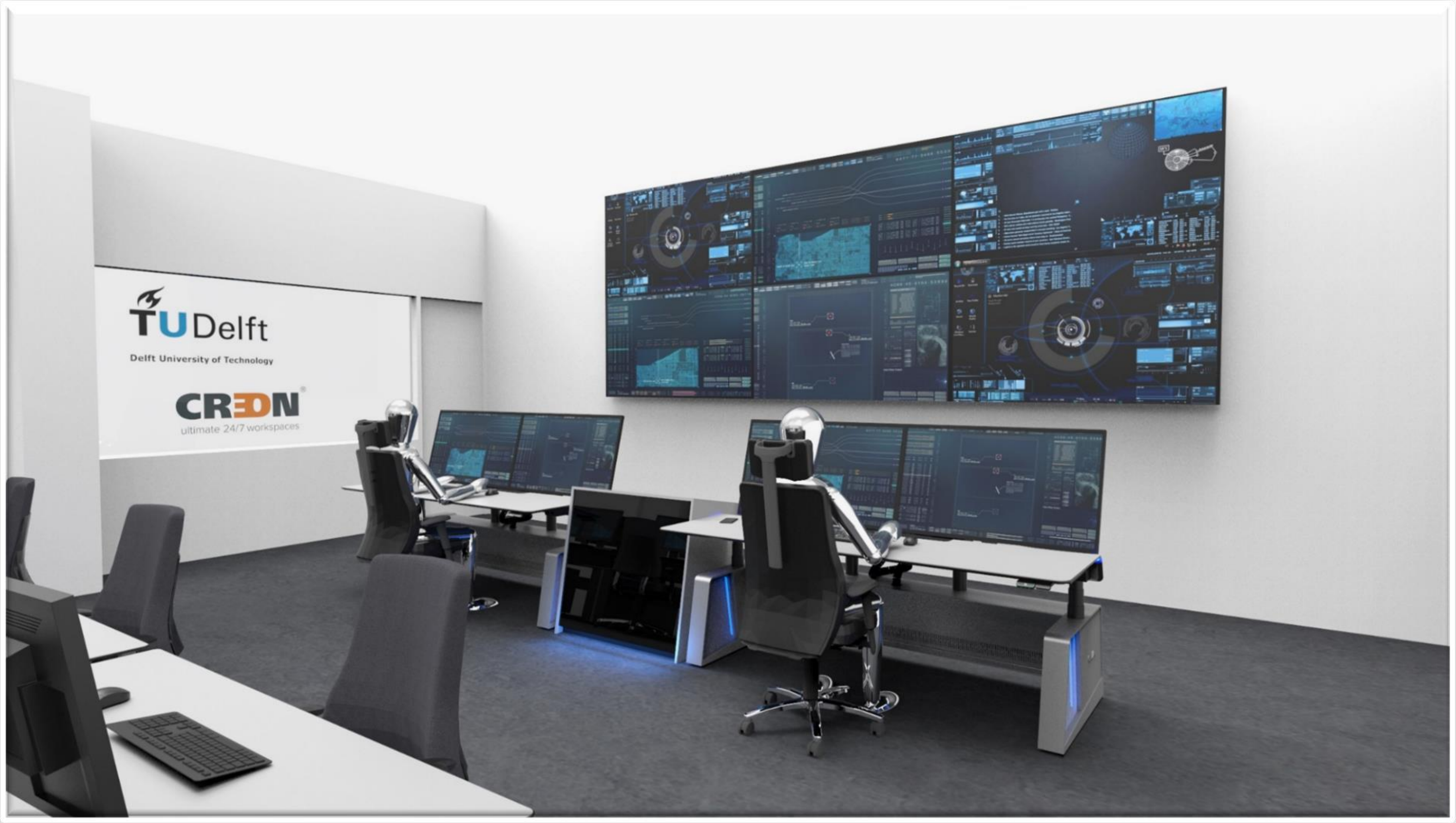
Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

- Vision
  - ➢ Future power grid is intelligent (AI), resilient and cyber secure
- Facility for Research, Development & Demonstration
  - ➢ CRoF is unique, future-ready and multi-domain experimental setup
    - ✓ Neutral ground for TSOs, DSOs & vendors
    - ✓ Hub for future power grid technologies
- Research
  - ➢ Intelligent power system operations
    - ✓ Future control of power systems
    - ✓ Cyber security
    - ✓ Digital twins
    - ✓ Artificially intelligent assistants
  - ➢ Reliability and operational resilience



Source: alliander.com

Control Room of the Future (CRoF): AI for Cyber Resilience of Power Grids



Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Cyber Resilient Power Grids (CRPG) Team

Projects

- NWO RESCUE (PI): *Resilience and cyber security of integrated cyber-physical energy systems*
- Stedin BRILLIANT (PI): *Cyber resilient electric vehicle charging in smart grids*
- EU Horizon eFORT (Demo Leader): *Establishment of a framework for transforming current power systems into a more resilient, reliable and secure system all over its value chain*
- EU H2020-MSCA-ITN InnoCyPES: *Innovative tools for cyber-physical energy systems*
- EU Horizon HVDC-WISE: *HVDC-based grid architectures for reliable and resilient widespread hybrid AC/DC transmission systems*
- EU H2020 ERIGrid2.0: *European research infrastructure supporting smart grid and smart energy systems research. technology development, validation and roll out – 2nd edition*

- Total research funding of 3.5 M€

Cyber Resilient Power Grids (CRPG) Team

Name: Dr. Raifa Akkaoui (Postdoc)
Research Topic:
Blockchain for a cyber-secure and resilient control of DERs at grid edge

Name: Vetrivel Subramaniam Rajkumar (PhD)
Research Topic:
Cyber security of power grids: cascading failure analysis and mitigation

Name: Yigu Liu (PhD)
Research Topic:
Synthetic cyber-physical systems and vulnerability assessment

Name: Ioannis Semertzis (PhD)
Research Topic:
Intrusion detection of cyber attacks on cyber-physical energy systems

Name: Ali Abedi (PhD)
Research Topic:
Cyber-physical smart grid intrusion detection

Name: Alfan Presekal (PhD)
Research Topic:
Cyber resiliency of power grid operational technologies

Cyber Resilient Power Grids (CRPG) Team

Name: Sjors Hijgenaar (PhD)
Research Topic:
Resilience of power systems against cyber attacks on EV charging infrastructure

Name: Mehran Hashemian Ataabadi (PhD)
Research Topic:
Decision support for operational technology and power system restoration

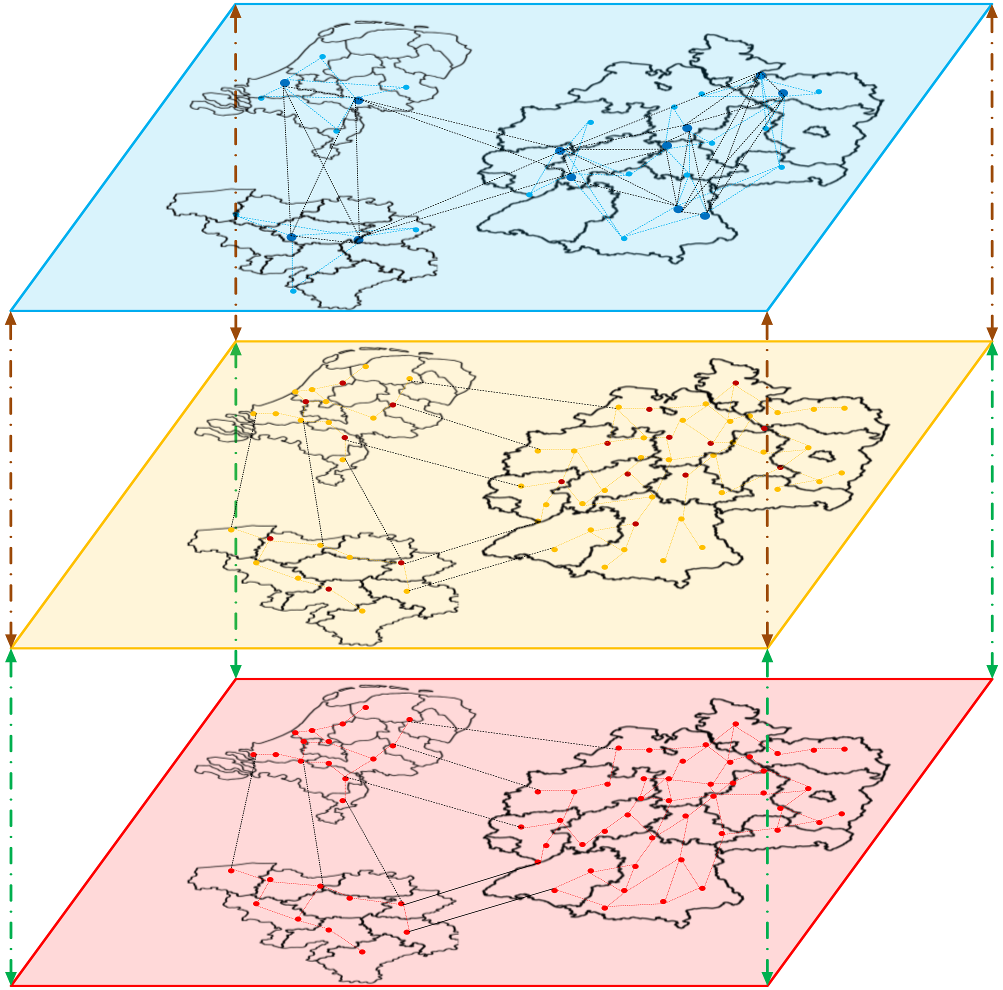
Name: Dr. Mohsen Jorjani Damghani (Postdoc)
Research Topic:
Cyber security of high-voltage AC/DC power grid architectures

Name: Sho Cremers (PhD CWI-TUD)
Research Topic:
Incident response using security games

Name: Ali Mollaiee (PhD)
Research Topic:
Self-healing power grid capabilities to defend against cascading effects

Name: To be recruited (Postdoc)
Research Topic:
Power system self-healing and defence against cyber attacks

Generating Large-Scale Synthetic Communication Topologies for Cyber-Physical Power Systems



Logical Control Network

II. Generating LCN

- ➢ **Choose optimal communication hubs for each area**
  - ✓ Minimize traffic volume and consider the node degree of corresponding substation node
  - ✓ Use Algorithm 2 to identify the optimal communication hubs
- ➢ **Form logical communication topology among Communication Hubs (CHs) and Control Centers (CCs)**
  - ✓ Generate topology between CHs and CCs
  - ✓ Generate topology between CCs

Physical Communication Network

I. Generating PCN

- ➢ **Generate the backbone topology based on power topology**
  - ✓ Consider the construction cost of communication infrastructure
  - ✓ Use minimum spanning tree to solve model and ensure connectivity
- ➢ **Increase redundancy to enhance the network resilience:**
  - ✓ consider betweenness distribution and eigenvalue of graph Laplacian when increasing the network redundancy
  - ✓ Use Algorithm 1 to determine the added redundancy

● communication hub

● Substation nodes (Physical)

● control center

● Substation nodes (Cyber)

◄· – ·► PC-PP interdependency: **“partially one-to-one”**

◄· – ·► LC-PC interdependency: **“one-to-one”**

Modelling Cyber-Physical Systems for Smart Grid Intrusion Detection

Research Goal

- Develop Intrusion Detection System (IDS) for Cyber Physical power Systems (CPS)

Problem

- ICT and physical power grid are entangled in CPS
- Most works ignore or simplify one of 3 layers in CPS

Approach

- Mathematically model CPPG
  - ➢ Use Hybrid Dynamical Systems theory

State variable

$$\Sigma : \begin{cases} x \in C, & \dot{x} = f(x) \\ x \in D, & x^{+} = g(x) \end{cases}$$

C : flow set

D : jump set

f : flow map

g : jump map

Model of each cyber or physical component:

Internal states

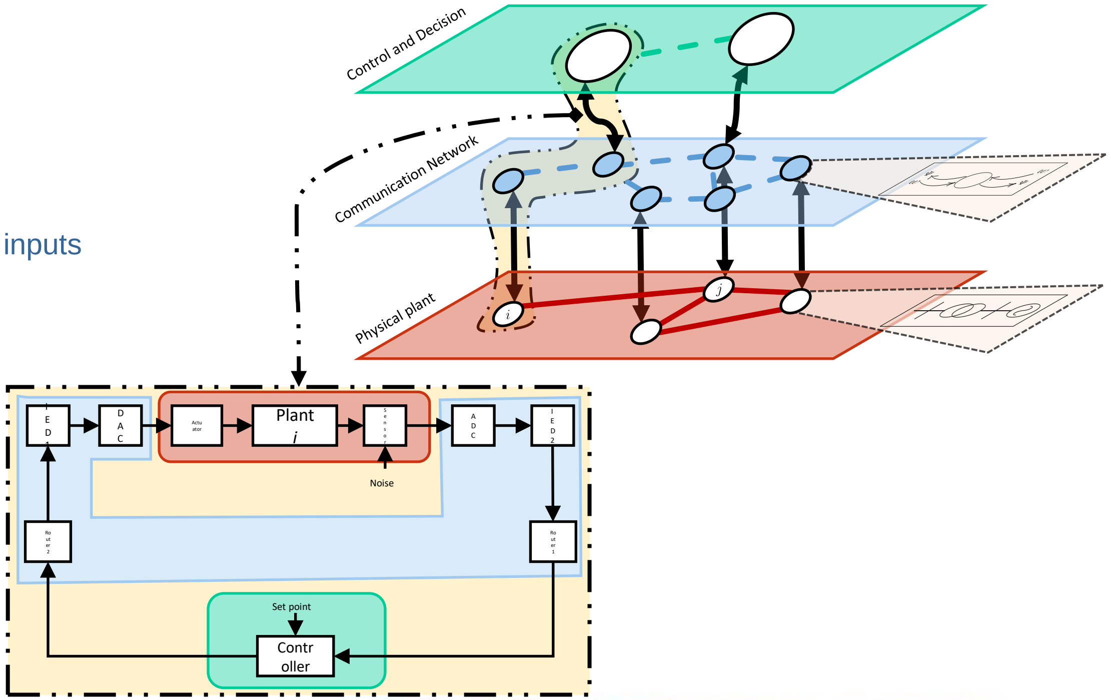
External inputs

$$\dot{z}(t) = F(z(t), w(t))$$

$$z^{+}(t) = G(z(t), w(t))$$

$$\Psi(t) = \phi(z(t))$$

output

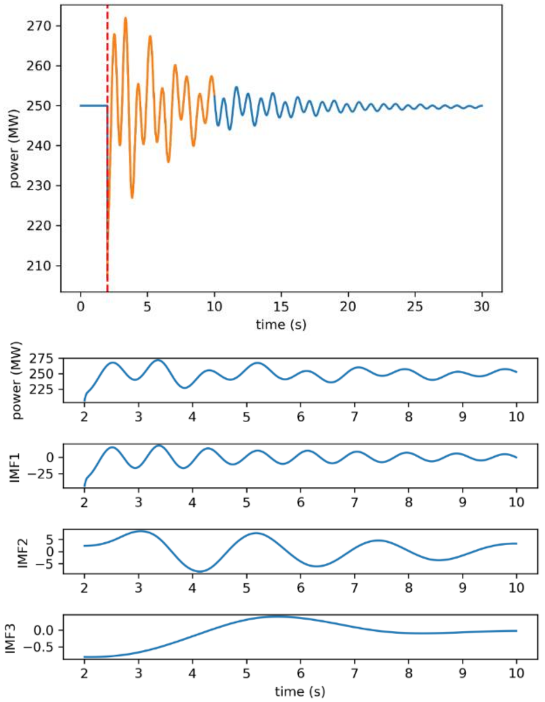


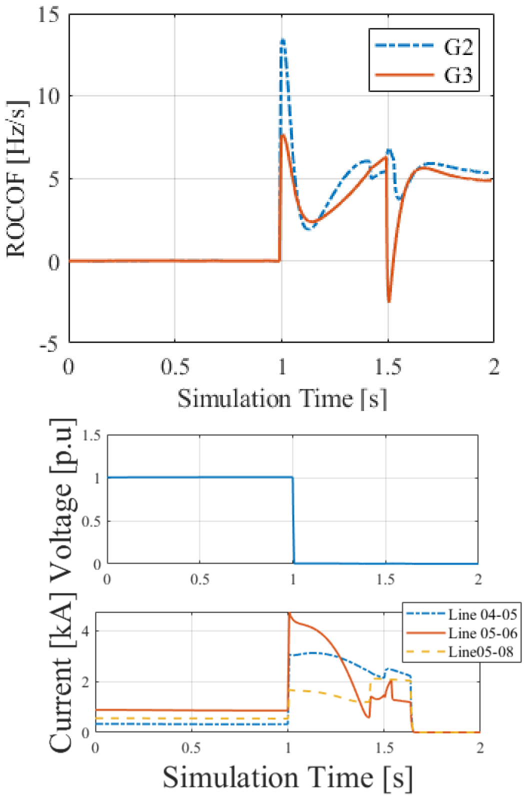
Cyber Attacks on Power Systems: Analysis of Cascading Failures

Scientific Contributions

- Compute Point of No Return (PNR) for cyber induced cascading failures
- Time-frequency analysis of system response

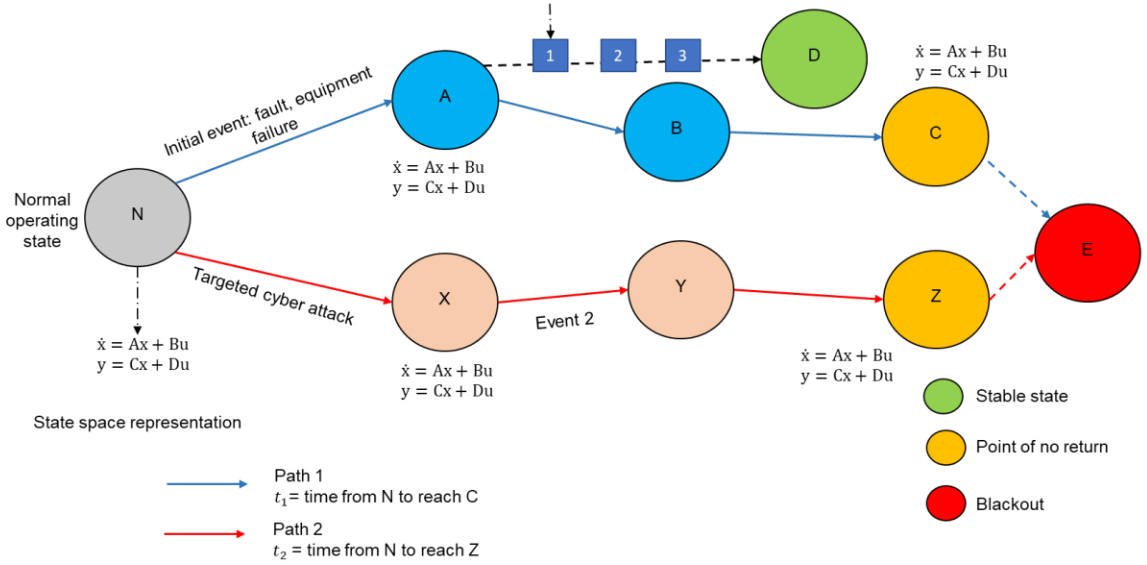
Results





Proposed Method

- Instantaneous damping $\alpha(t) = -\frac{2\dot{A}(t)}{A(t)}$
- Form covariance matrix R of $\alpha(t)$ and analyse decomposition



Conclusions

- Cyber attacks can cause and accelerate cascading failures

Intrusion Detection System for Control Room of the Future

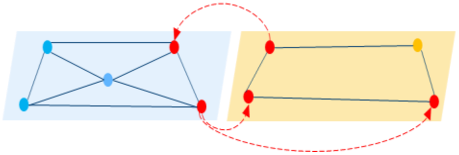
Scientific Contributions

- Spatial-temporal correlation and anomaly detection of cyber-physical power system

Proposed Methods

- Deep learning model based on GNN, CNN and LSTM

$$A_{c+p}\ [A_c \cup A_p]$$

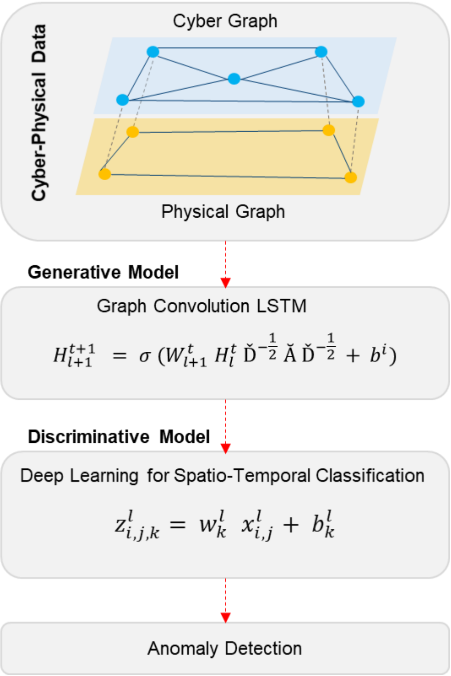


$$\mathcal{G}_c = \{ \mathcal{V}_c , \mathcal{E}_c \}$$

$$\mathcal{G}_p = \{ \mathcal{V}_p , \mathcal{E}_p \}$$

$$\Gamma : \mathcal{V}_c \leftrightarrow \mathcal{V}_p$$

$$\Gamma = \{ \mathcal{V}_c^{1,1} \leftrightarrow \mathcal{V}_p^{1,1} \mid \ldots \mid \mathcal{V}_c^{i,j} \leftrightarrow \mathcal{V}_p^{u,v} \}$$



Generative Model

Graph Convolution LSTM

$$H_{l+1}^{t+1} = \sigma\,(W_{l+1}^{t}\, H_l^t\, \check{\mathrm{D}}^{-\frac{1}{2}}\, \check{\mathrm{A}}\, \check{\mathrm{D}}^{-\frac{1}{2}} + b^i)$$

Discriminative Model

Deep Learning for Spatio-Temporal Classification

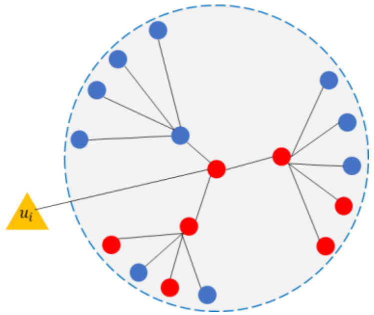
$$z_{i,j,k}^{l} = w_k^l\ x_{i,j}^l + b_k^l$$

Anomaly Detection

Results

$$A_{c+p} = \begin{bmatrix} c_{11} & \cdots & c_{1j} & x_{1,j+1} & \cdots & x_{1,j+v} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ c_{i1} & \cdots & c_{ij} & x_{i,j+1} & \cdots & x_{i,j+v} \\ x_{i+1,1} & \cdots & x_{i+1,j} & p_{i+1,j+1} & \cdots & p_{i+1,j+v} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ x_{i+u,1} & \cdots & x_{i+u,j} & p_{i+u,j+1} & \cdots & p_{i+u,j+v} \end{bmatrix}$$

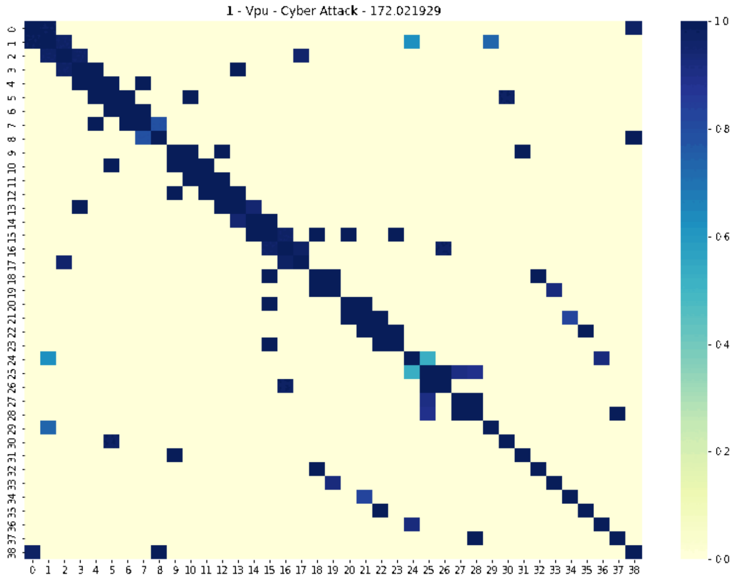
correlation



● Normal node ● Anomalous node

Attack graph, $\Lambda = \{ \mathrm{a_i}, \bar{\mathrm{a}}_i , \in V\}, \{u_i \notin V \}$

Correlation matrix transition during cyber attack in IEEE 39 Bus



Conclusions

- Cyber and physical anomalies are critical to detect a cyber attack on power grids

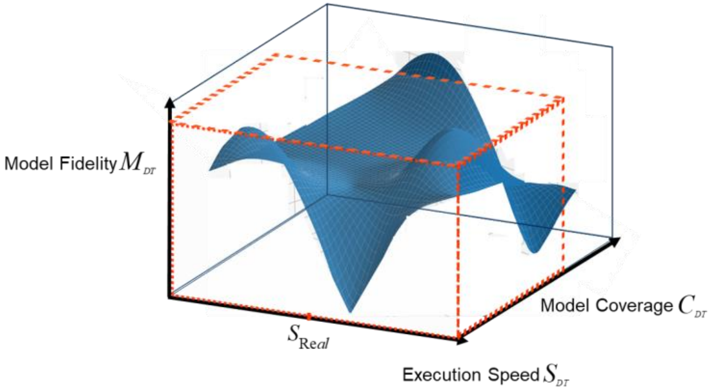
Detection of Cyber Attacks in Cyber-Physical Energy Systems

Scientific Contributions

- Develop digital twin of CPS
- Intrusion detection method based on artificial intelligence

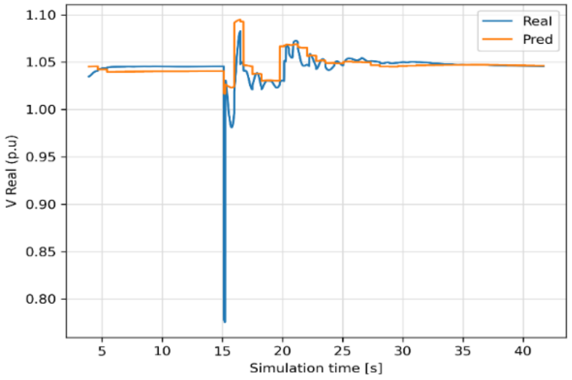
Proposed Method

- Quantify features needed for a sufficient digital twin model
- Unsupervised learning to detect cyber attacks on power systems

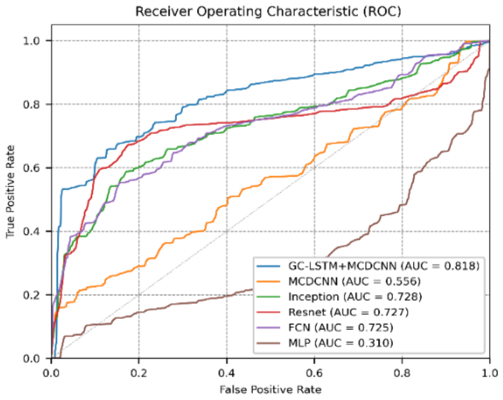


Digital twin features

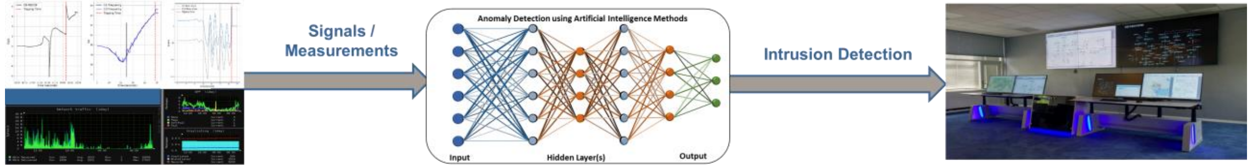
Results



Prediction of power system behaviour

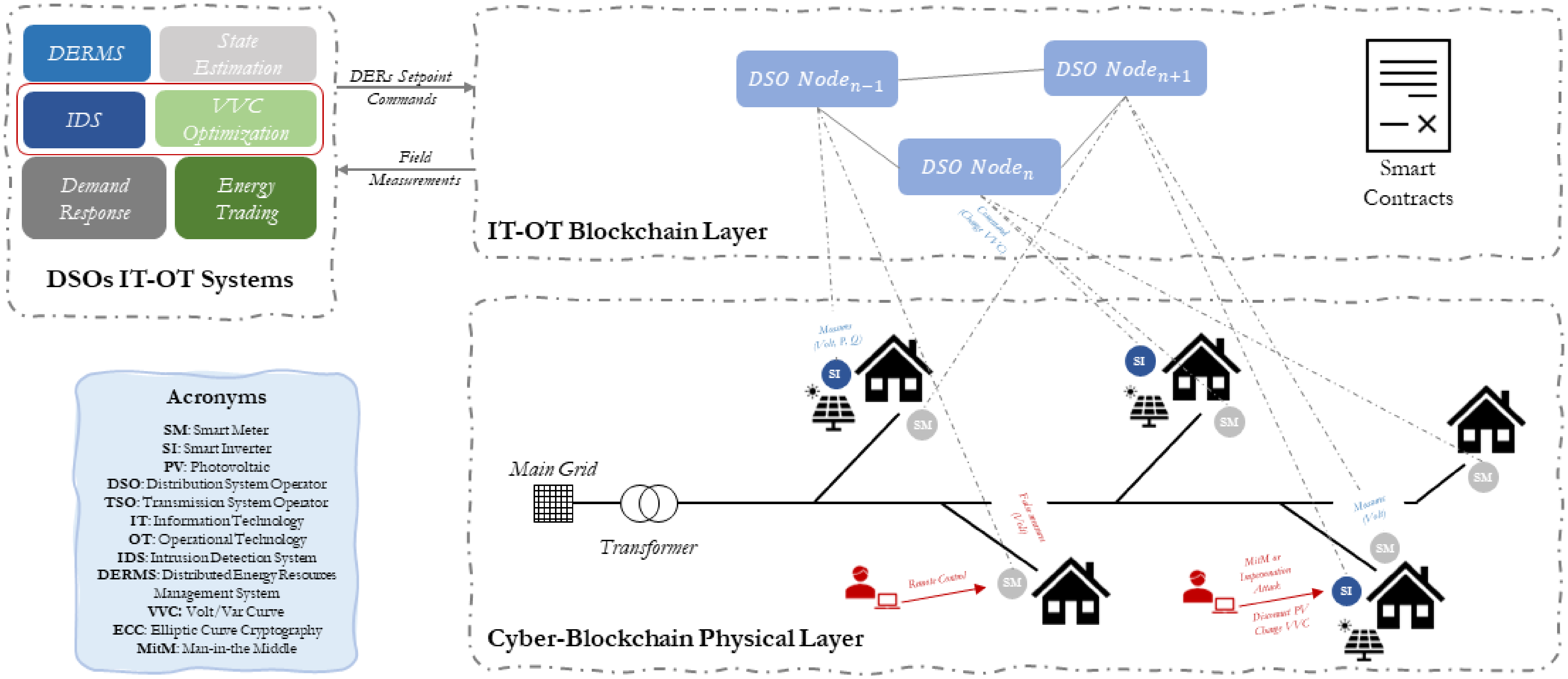


Performance comparison of classifiers



Intrusion detection on Control Room of the Future

Blockchain-based Infrastructure for DERs Security Control and Monitoring



Acronyms

SM: Smart Meter
SI: Smart Inverter
PV: Photovoltaic
DSO: Distribution System Operator
TSO: Transmission System Operator
IT: Information Technology
OT: Operational Technology
IDS: Intrusion Detection System
DERMS: Distributed Energy Resources Management System
VVC: Volt/Var Curve
ECC: Elliptic Curve Cryptography
MitM: Man-in-the-Middle

Thank You

Alex Stefanov

Assistant Professor, Chartered Engineer (CEng MIEI)

Email: A.I.Stefanov@tudelft.nl

Cyber Resilient Power Grids (LinkedIn)

Control Room of the Future (LinkedIn)

Intelligent Electrical Power Grids, EEMCS, **TU Delft**
Mekelweg 4, 2628 CD Delft, The Netherlands