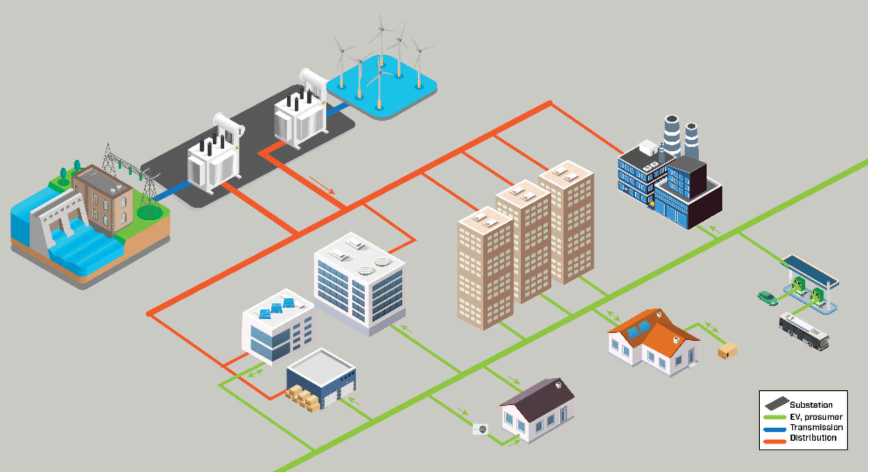
Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems

Tesfaye Amare Zerihun (SINTEF Energi AS)
Santiago Sanchez Acevedo (SINTEF Energi AS)

SINTEF

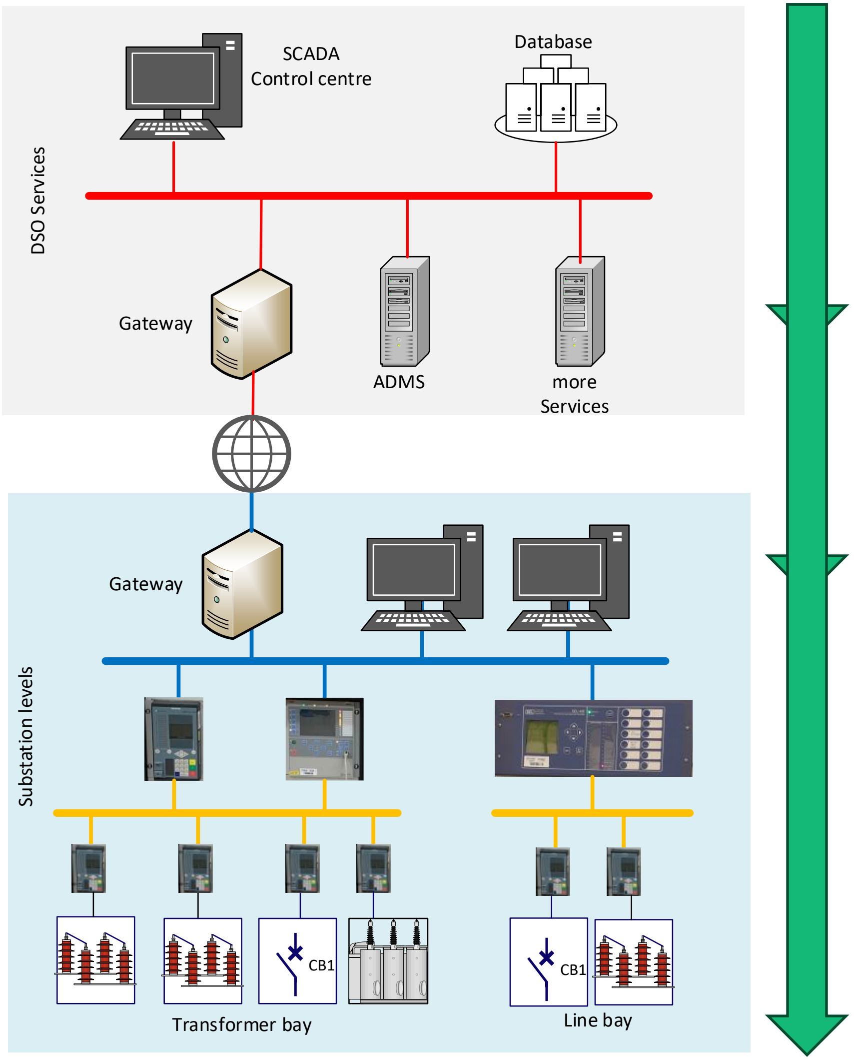
Motivation

- Nowadays, Electric Power Systems (EPES) are increasing the using of information and communication technology (ICT)
- It is increased the amount of data transmitted in the substations and to the Operator's Control centre.
- With the addition of the ICT the EPES increase its vulnerability.
  - Risk of **blackout** due to a **cyber-attack**



Distribution systems SCADA and Digital Substation

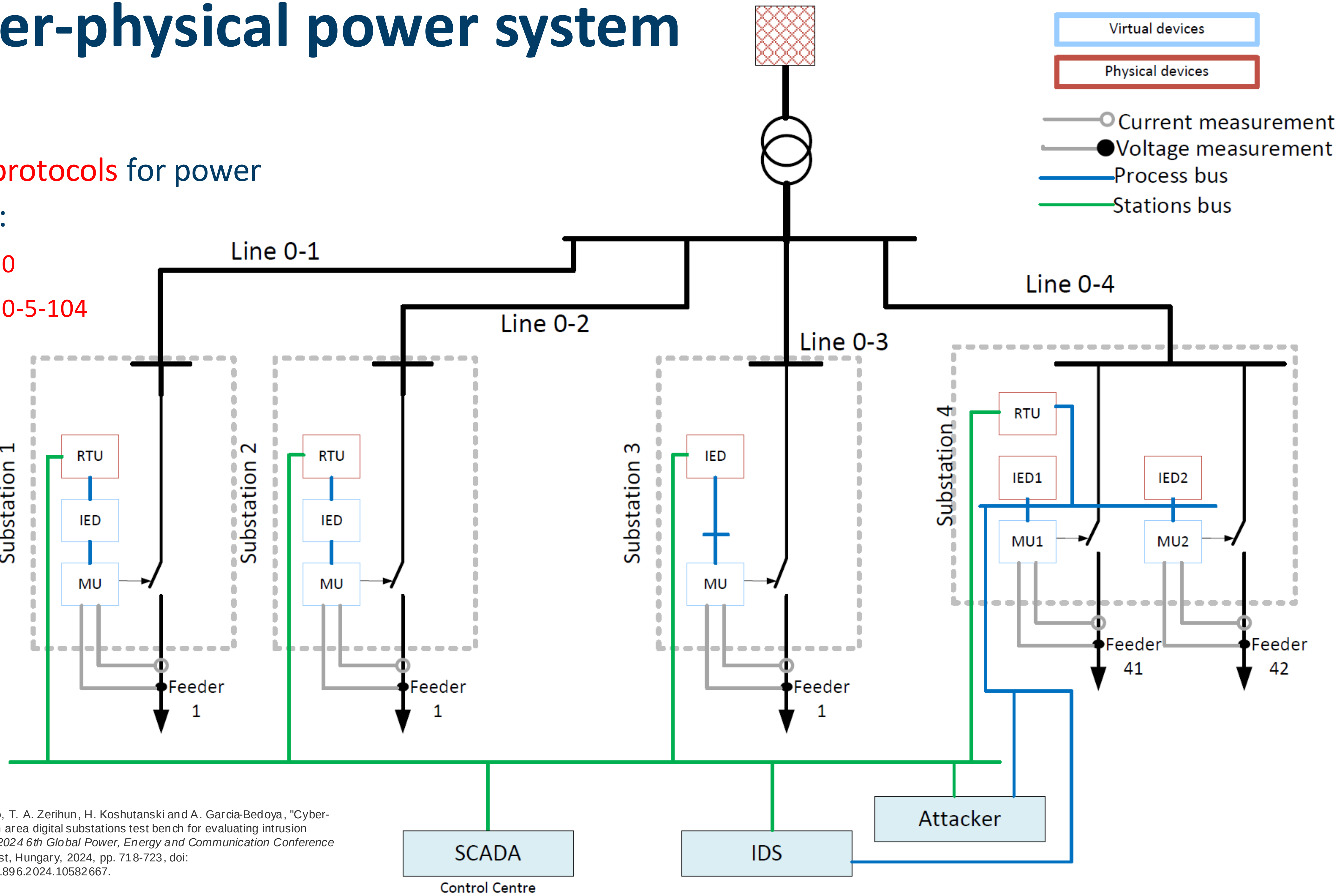
- At Operator's Control Centre
  - The area of the power system can be monitored and controlled by the SCADA.
  - Communication Substation to control centre with RTU or IED
  - Protocol example: IEC 60870-4-105
- Local communications in the substation
  - Standard IEC 61850



Cyber-physical power system

SIN

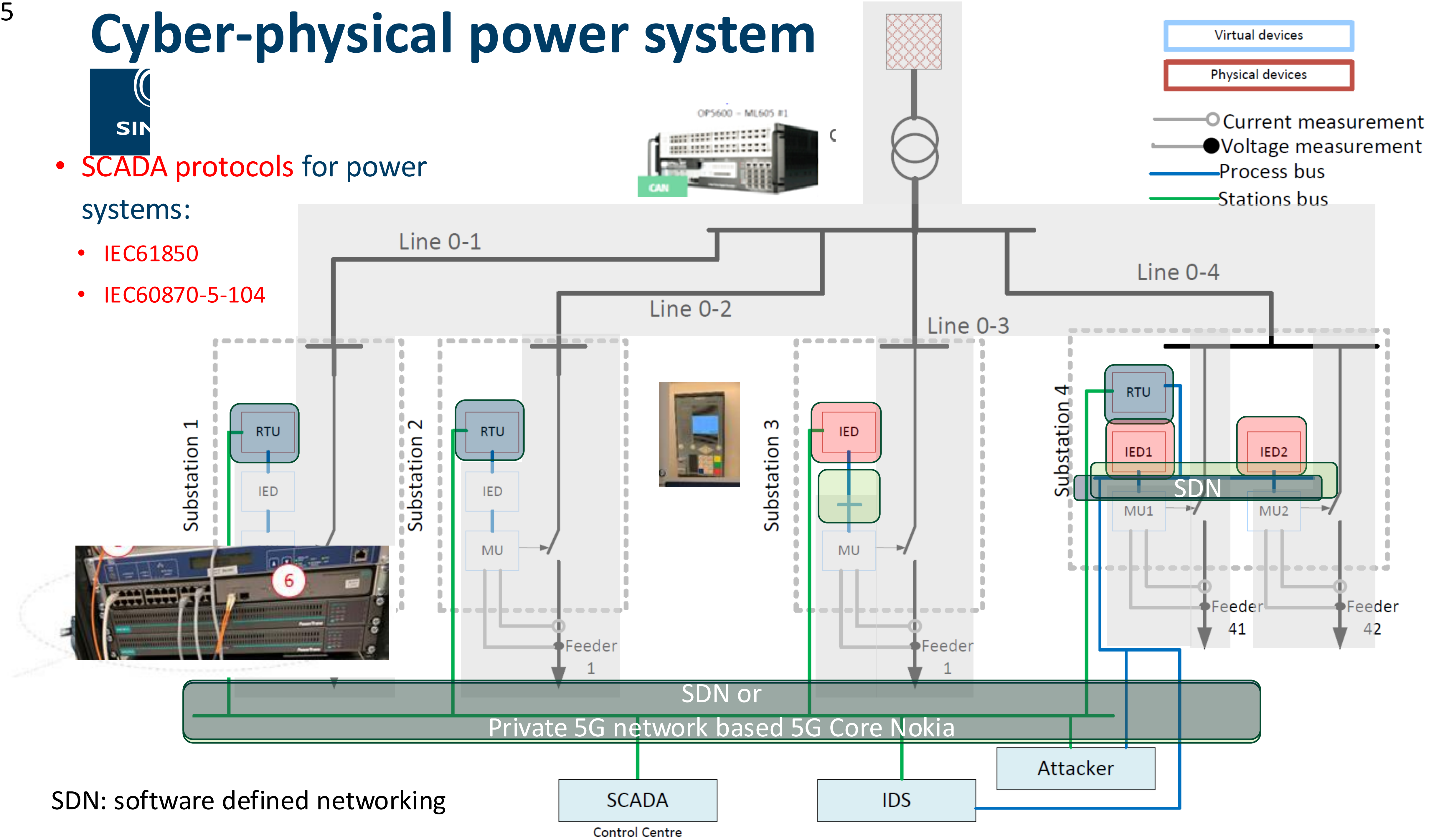
- SCADA protocols for power systems:
  - IEC61850
  - IEC60870-5-104



S. Sanchez-Acevedo, T. A. Zerihun, H. Koshutanski and A. Garcia-Bedoya, "Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems," *2024 6th Global Power, Energy and Communication Conference (GPECOM)*, Budapest, Hungary, 2024, pp. 718-723, doi: 10.1109/GPECOM61896.2024.10582667.

Cyber-physical power system

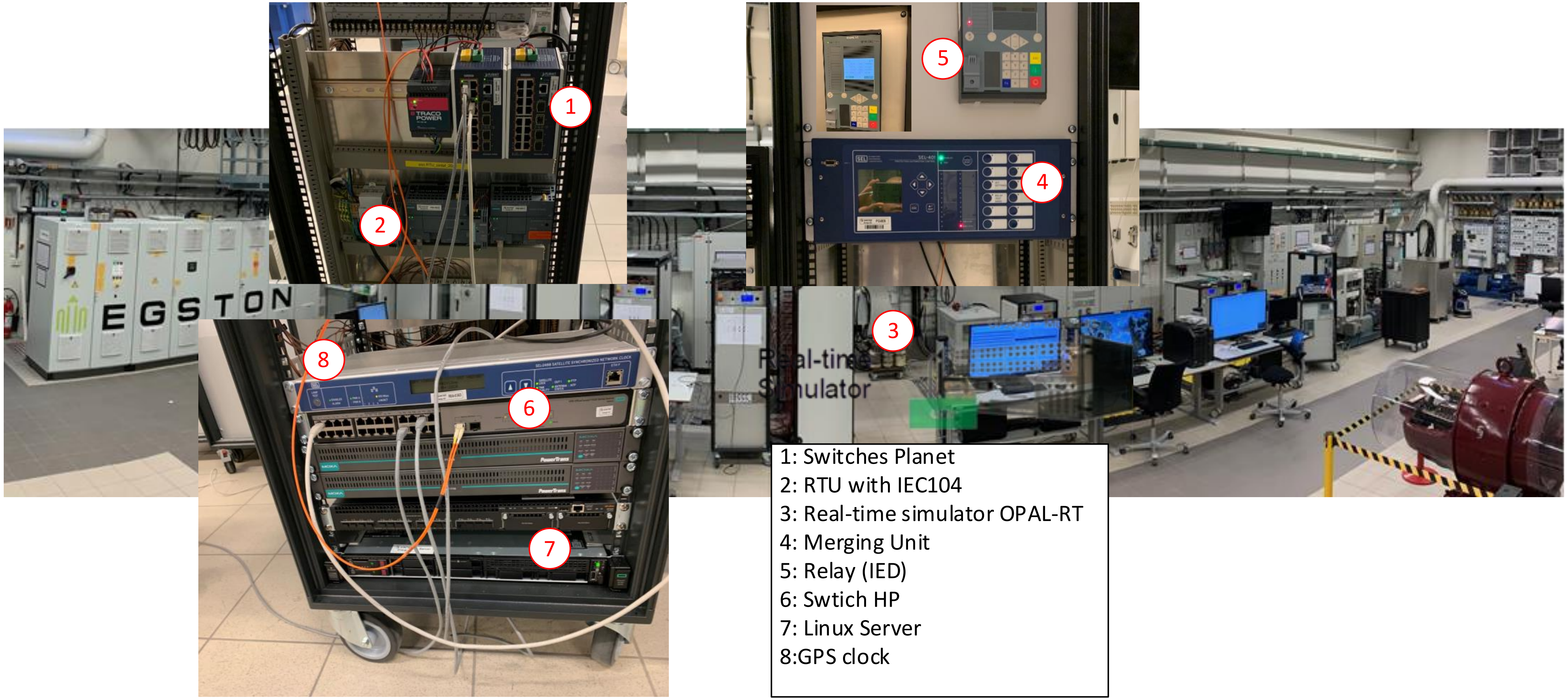
- SCADA protocols for power systems:
  - IEC61850
  - IEC60870-5-104



SDN: software defined networking

Cyber-physical power system

- Laboratory setup



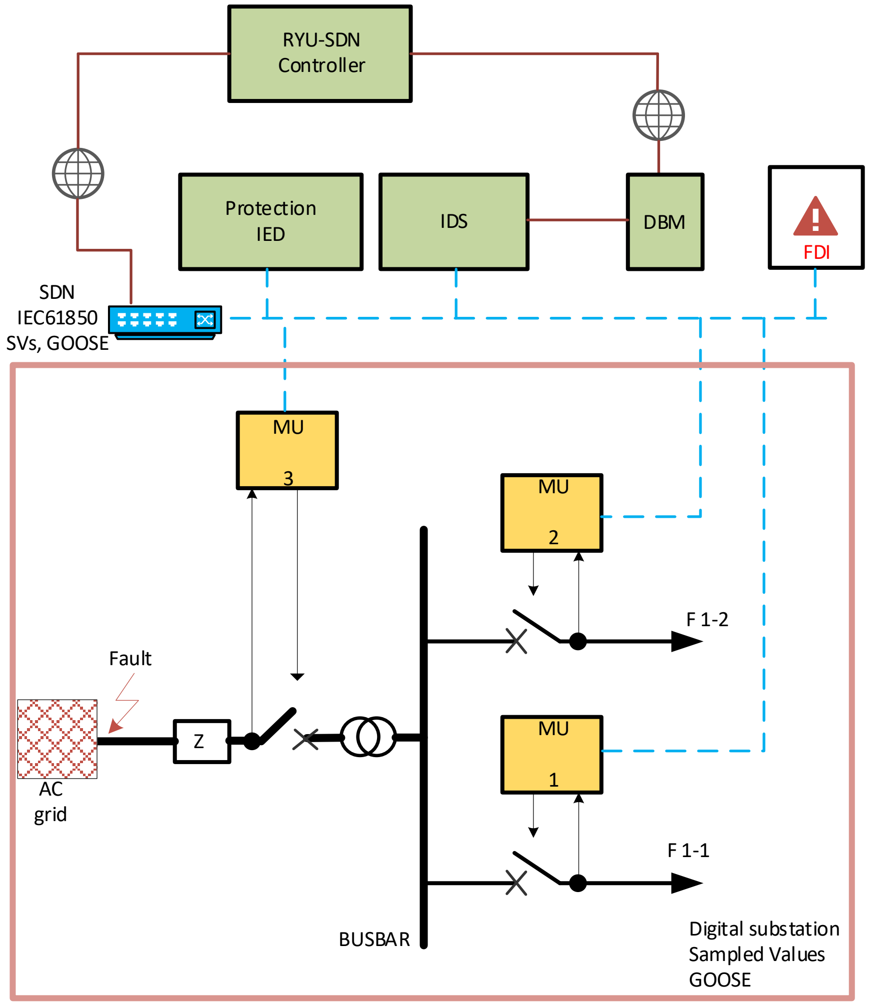
1: Switches Planet
2: RTU with IEC104
3: Real-time simulator OPAL-RT
4: Merging Unit
5: Relay (IED)
6: Swtich HP
7: Linux Server
8:GPS clock

Cyber Attacks

- Attacks on IEC-104
  - **FDI Monitoring Direction**: Injection of spoofed IEC-104 packets within a valid TCP session from RTU to SCADA, tricking SCADA into accepting false data as if from the RTU.
  - **FDI Control Direction**: Injection of spoofed IEC-104 packets within a valid TCP session from SCADA to RTU, allowing manipulation of the breaker state at the RTU.
- Attacks on IEC-61850 GOOSE
  - **Packet Replay**: Replay of previous valid GOOSE packets to manipulate the breaker state.
  - **FDI Version 1**: Injection of GOOSE packets with manipulated sequence numbers and timestamps, simulating a real GOOSE message sequence.
  - **FDI Version 2**: Injection of false GOOSE packets just before the original ones, maintaining the attack by syncing with the packet announcement rhythm.
- Attacks on IEC-61850 SV
  - **Packet Replay**: Replay of SV frames with previous communication values at a specific rate.
  - **FDI**: Injection of SV frames with false values and spoofed sample count values, destabilizing the IED's readings.
- Attacks on PTP (IEEE 1585)
  - **Desynchronization of RTUs/IEDs**: Disruption of GOOSE and SV communications by introducing a bogus master clock, causing RTUs/IEDs to sync with a low precision clock source.

Case 1: digital substation with SDN

- DigSt, Protection IED and MUs for the experimental validation.
- **IDPS**: instruction detection and protection system
- Integration of IDPS in the DigSt.
- The IDPS is in this case centralized and with an **SDN** controller take actions to remove the attacks when they have been detected.



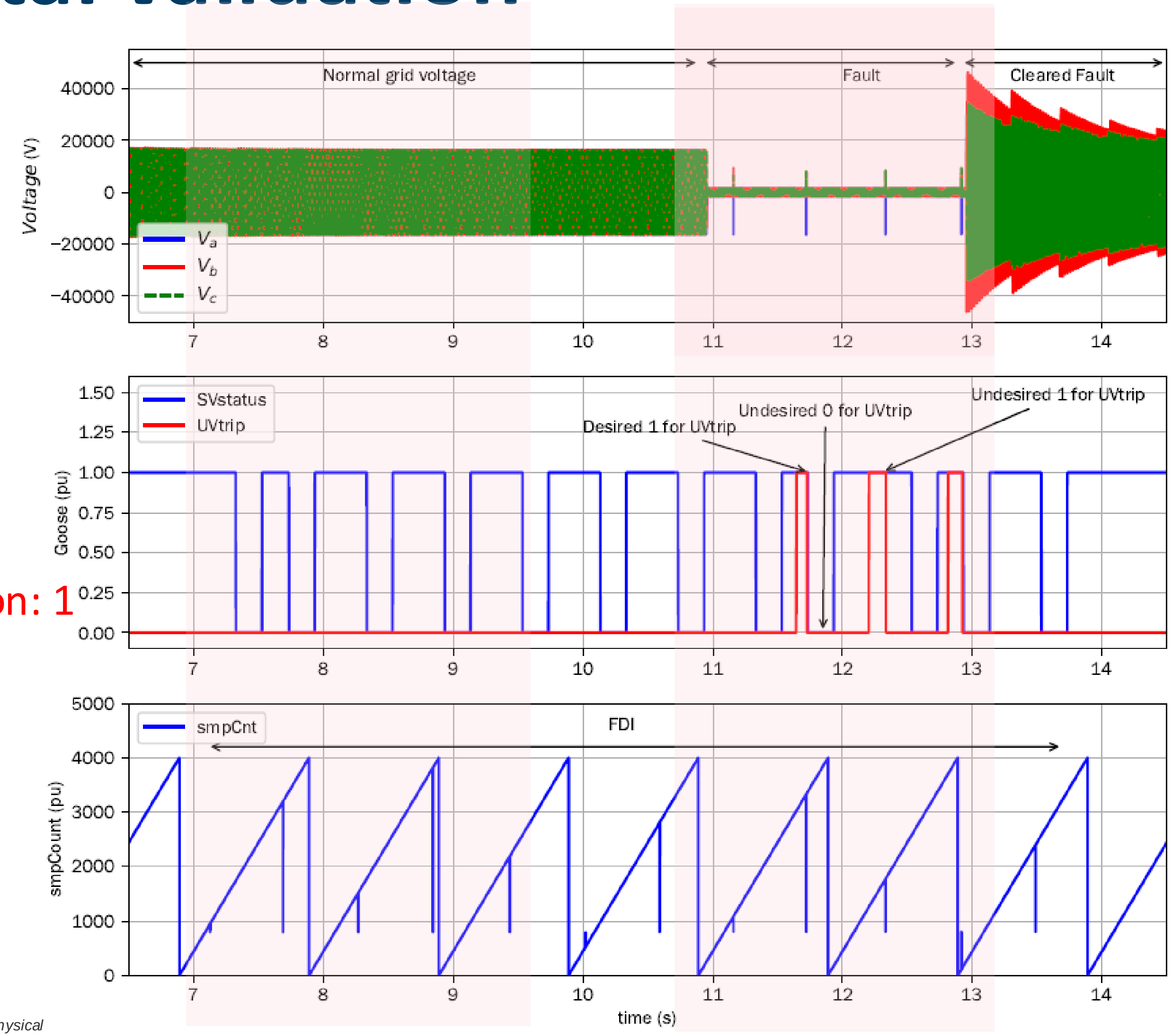
Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

Case 1: Experimental validation

- Effects of FDI-replay attack over Sampled Values for under voltage protection.
- Scenario IEC 61850 Sampled Values
  - Malfunctioning switch or attack.
- Project with DSOs in Norway

SV working Correctly: 1

UV protection: 1

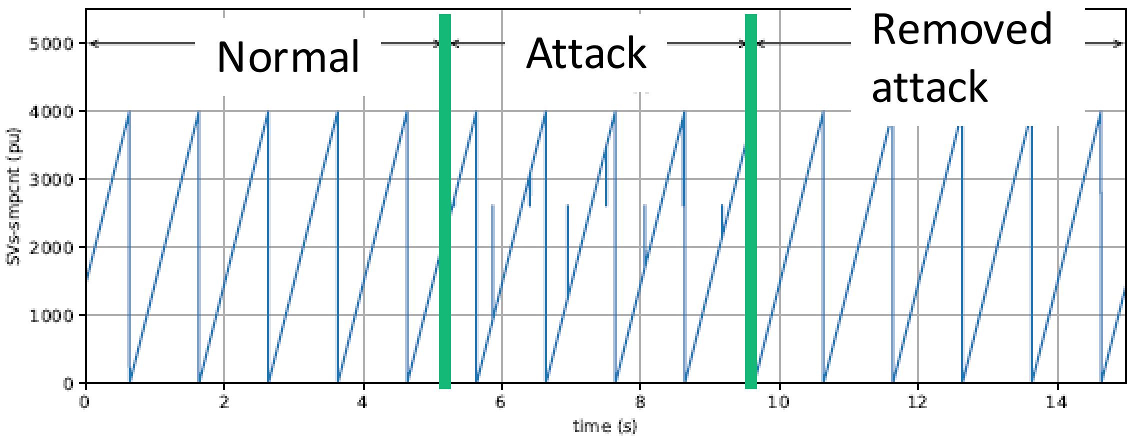


Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

Experimental validation

- Scenario Sampled Values attack.

- Performance of IDPS
- Normal traffic: up to 5 s
- FDI Attack: from 5s
- IDPS action (clean): from ≈9.5 s



FLOWS OF THE SDN SWITCH DURING NORMAL TRAFFIC AND FOR CLEANING THE ATTACK OF SVS.

Time range	Priority	Match	Output
Normal traffic	10	dl_type = 0x88ba	FLOOD
Normal Traffic	10	dl_type = 0x88b8	drop
Cleaned attack	11	$in\_port = 8$ $dl\_dst = MAC_{SV}$ $dl\_type =$ 0x88ba	drop

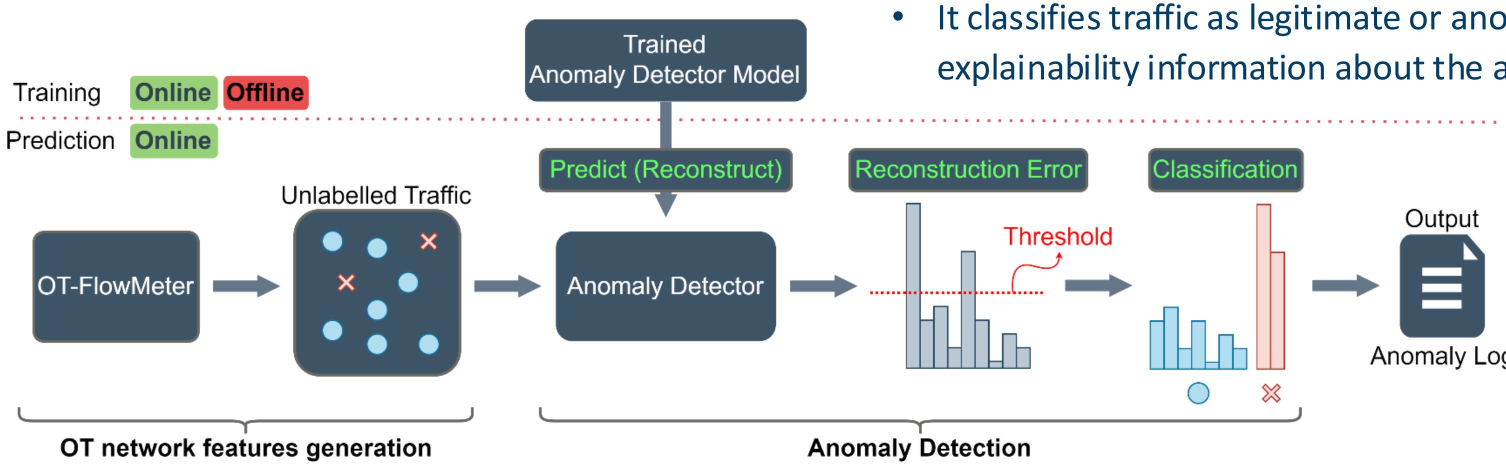
Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

Case 2: Cybersecurity Anomaly Detection for Digital Power Systems

Hristo Koshutanski (Eviden BDS R&D) Alejandro Garcia-Bedoya (Eviden BDS R&D)

- **AI-Based Anomaly Detection IDS**:
  - Developed by ATOS/Eviden BDS R&D Spain under the SDN microSENSE and ELECTRON project (Horizon 2020).
- **Baseline Establishment**: Learns normal patterns of SCADA communication of legitimate behaviour, identifying anomalies as deviations from this baseline.
- **Deep Learning Model**: Utilizes an Autoencoder to model benign traffic patterns features from OT protocols.

- **Workflow**:
  - training deep learning models with legitimate traffic before switching to monitoring mode.
  - The OT-FlowMeter module extracts network behavioural features
  - to feed the Brain module.
- **Anomaly Classification**:
  - The Brain module, containing deep learning
  - It classifies traffic as legitimate or anomalous and provides explainability information about the anomalies.



OT: Operational Technology

Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

SINTEF

Experimental Results - Metrics

- The IDS tool achieved over 92% accuracy
- with F1-Scores exceeding 94% for legitimate cases and 85% for anomalous cases.
  - F1: Harmonic precision and recall
- Confusion matrices confirm the high performance.
- High detection rates are due to specific features defined for OT protocols.
- The IDS solution extracted over 1800 features for IEC-104 and over 400 features for GOOSE and SV, ensuring consistent detection metrics regardless of EPS network size, IEDs, or topology.

	Predicted Negative	Predicted Positive
Actual Neg.	TN	FP
Actual Pos.	FN	TP

Protocol	Attack Name	Accuracy	F1-Score (Legit)	F1-Score (Anomaly)
IEC-104	FDI (1.a)	0.94	0.95	0.93
IEC-104	FDI (1.b)	0.99	0.99	0.99
IEC-61850 (GOOSE)	Replay (2.a)	0.92	0.94	0.85
IEC-61850 (GOOSE)	FDI (2.b)	1.00	0.99	1.00
IEC-61850 (GOOSE)	FDI (2.c)	1.00	1.00	1.00
IEC-61850 (SV)	Replay (3.a)	1.00	0.98	1.00
IEC-61850 (SV)	FDI (3.b)	0.98	0.94	0.99
PTP	Desync. (4.a)	1.00	0.98	1.00

IEC104 - FDI (1.a)

Actual \ Predicted	Legit	Anomaly
Legit	0.90	0.10
Anomaly	0.00	1.00

IEC104 - FDI (1.b)

Actual \ Predicted	Legit	Anomaly
Legit	0.99	0.01
Anomaly	0.00	1.00

GOOSE - Replay (2.a)

Actual \ Predicted	Legit	Anomaly
Legit	0.89	0.11
Anomaly	0.00	1.00

GOOSE - FDI (2.b)

Actual \ Predicted	Legit	Anomaly
Legit	0.99	0.01
Anomaly	0.00	1.00

GOOSE - FDI (2.c)

Actual \ Predicted	Legit	Anomaly
Legit	1.00	0.00
Anomaly	0.00	1.00

SV - Replay (3.a)

Actual \ Predicted	Legit	Anomaly
Legit	0.97	0.03
Anomaly	0.00	1.00

SV - FDI (3.b)

Actual \ Predicted	Legit	Anomaly
Legit	0.89	0.11
Anomaly	0.00	1.00

PTP - Desync (4.a)

Actual \ Predicted	Legit	Anomaly
Legit	0.96	0.04
Anomaly	0.00	1.00

Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

SINTEF

Conclusions

- The developed test-bench is a realistic digital substation environment corresponding to TRL7.
- The attacks shown a realistic impact on the substation operation.
- Another added values of the TRL7 testbench is the possibility to validate anomaly detection solutions on the modelling capacity of the baseline traffic footprint of this environment.

SINTEF

Conclusions

AI based IDS

Better results than SURICATA and SNORT®

- Unlike traditional IDS systems like Suricata and Snort, which rely on rule-based detection and require prior expert knowledge, the AI-based IDS solution supports OSI layer 2 protocols and provides automated training to learn legitimate behaviour.

SINTEF

Thank you!

- Questions
  - santiago.sanchez@sintef.no

Results and Figures in this presentation have been taken from the following references:

Sanchez Acevedo, Santiago; D'Arco, Salvatore.
A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. I: 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems - ICPS. IEEE (Institute of Electrical and Electronics Engineers) 2022 ISBN 978-1-6654-9770-1.

S. Sanchez-Acevedo, T. A. Zerihun, H. Koshutanski and A. Garcia-Bedoya, "Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems," *2024 6th Global Power, Energy and Communication Conference (GPECOM)*, Budapest, Hungary, 2024, pp. 718-723, doi: 10.1109/GPECOM61896.2024.10582667.