SECURING THE FUTURE

HIL Cyber-Physical Testing Platform to Address the Challenges of Grid Digitalization

Louis Raymond
Market Development Manager - OPAL-RT

OPAL-RT TECHNOLOGIES

INCREASING DYNAMIC RESPONSE AND COMPLEXITY

Time Scale

Relative Complexity

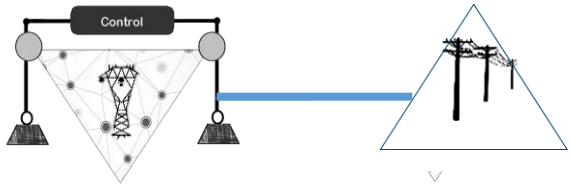
Pre-1970s

1 s

- **High Inertia – slow reaction**
- **Passive Distribution**
- Unidirectional distribution
- Schedulable generation
- Local, slow protection

10 ms

Through 21st Century

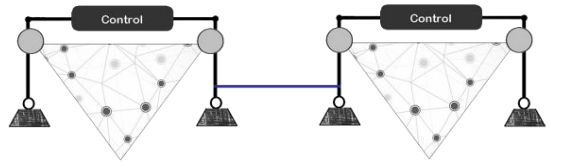


- High Inertia – slow reaction
- Passive Distribution
- Unidirectional distribution
- Schedulable generation
- **Faster control and protection**
  Machine V Regulators
  HVDC, FACTS, SVC
  Control & protection

- **Wide-Area Control & Protection**
- Operates near stability limits
- **Communication Systems**

50 us

Today and the Future



Transmission Distribution

- **Low inertia – fast reaction**
- **Active Distribution**
  - **Intermittent generation sources**
  - **Storage**

- More Wide Area Control & Comms
- **High dependance on communication systems**.

- **High penetration of inverter-Based Technologies (IBR, HVDC, FACTS)**
  - **Dynamics dependant on controls and protections**
  - **Control interactions**
  - **Low short-circuit**

5 us

OPAL-RT TECHNOLOGIES

Inter OPERA
Enabling multi-vendor HVDC grids

Enabling interoperability of multi-vendor high-voltage direct current (HVDC) grids

InterOPERA, funded by Horizon Europe, brings 21 European partners together from across the wind generation and transmission value chain to unlock the potential of multi-vendor HVDC systems and to foster transition of the European energy sector.

Disclaimer

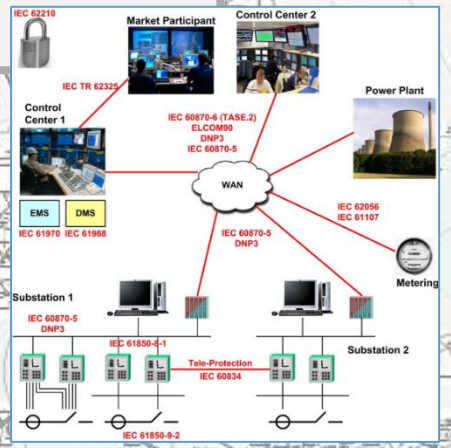
Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

PROJECT DETAILS
Duration: 1 January 2023 – 30 April 2027
Grant agreement: 101095874

INTEROPERABILITY

Numerous IEDs on the field
Many comm. Protocols
Multiple vendors

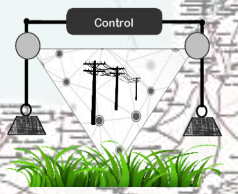


SIEMENS

RENEWABLES

Decentralized production
Intermittent (solar, wind)
Multidirectional power flows
Microgrids

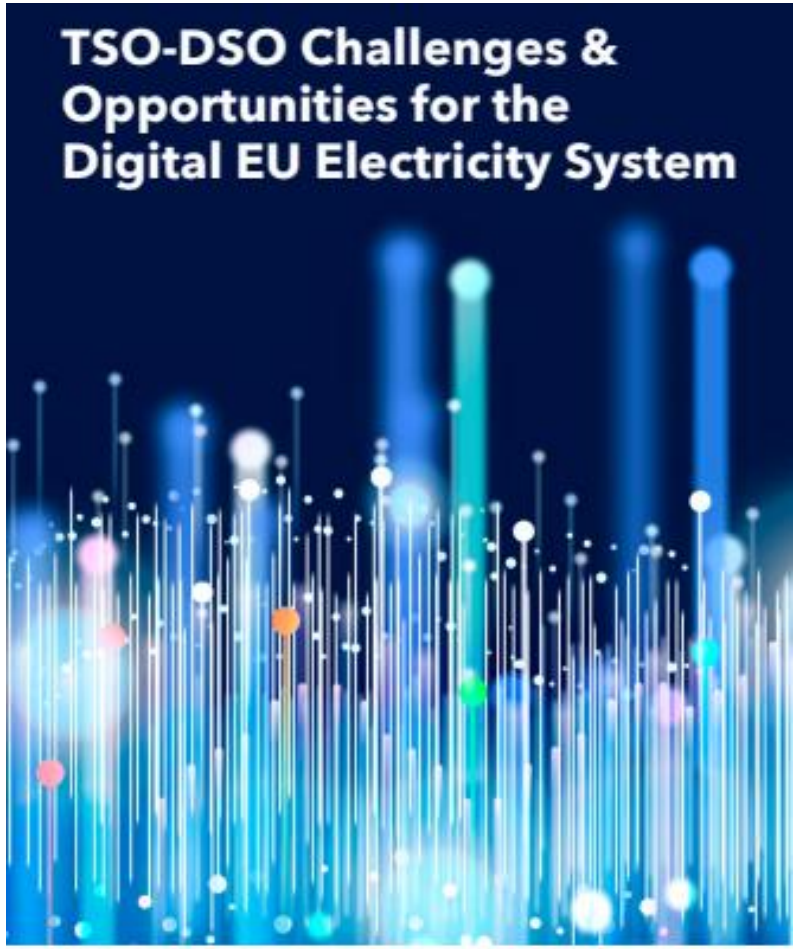
ABB



GRID OPERATION

Huge amount of controllable components
Naturally unstable
Need for synchronization
High QoS expected

https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Publications/RDC%20publications/DESAP_joint_report_on_common_TSO-DSO_challenges___opportunities_v1.1.pdf?utm_source=ENTSO-E+News+alerts&utm_campaign=42a66a6ed2-EMAIL_CAMPAIGN_2024_04_05_01_10_COPY_01&utm_medium=email&utm_term=0_-2411c18a3d-97062916



DSO ENTITY
DSOs FOR EUROPE

entsoe

Executive summary

The report underscores the critical need for digitalisation to enhance grid operation, planning, and customer integration, which is essential for achieving global and European carbon emission reduction targets. The recommended solution is the development of digital twins (DTs), as virtual replicas of physical systems, tightly connected via indispensable communication interfaces. These cutting-edge technologies enable improved monitoring, prediction, and decision-making across the lifecycle of grid assets, from development and planning to operational monitoring and scenario simulation.

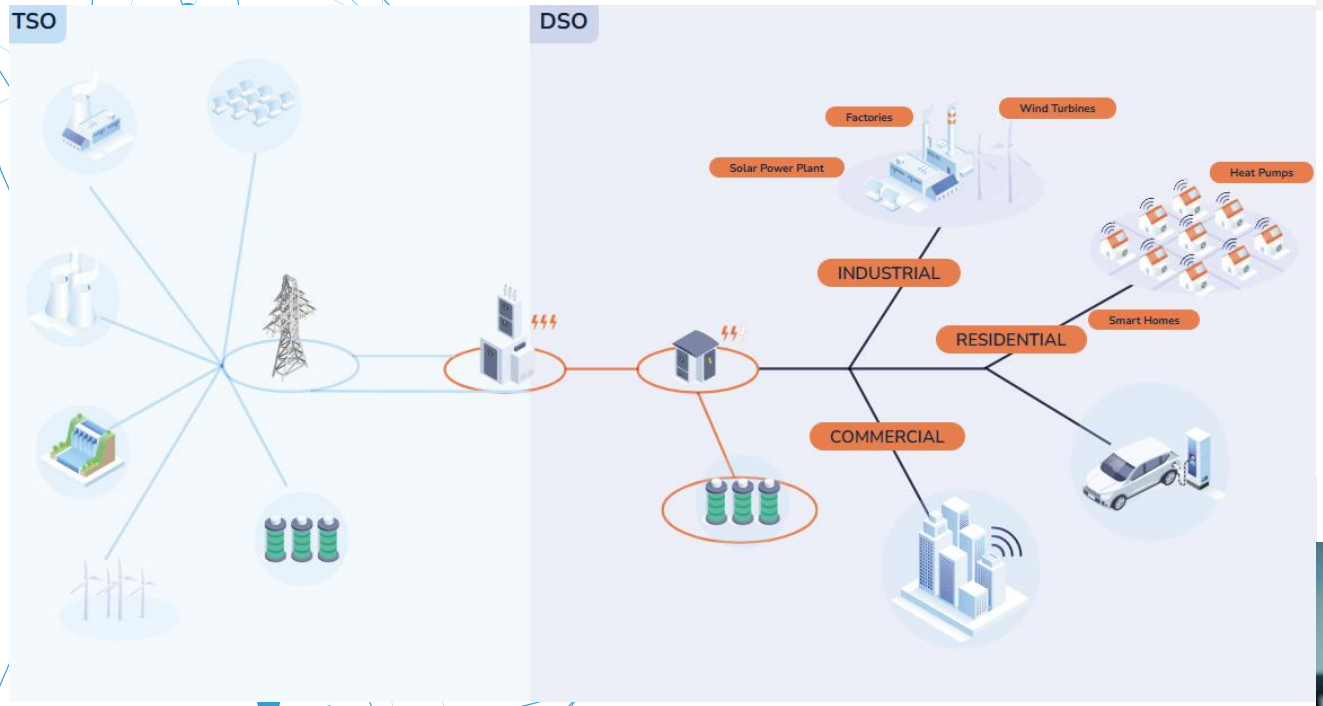
The power system faces several challenges today, including a rapid increase of distributed energy resources that must be integrated into the system, which requires coordinated planning and operational strategies. In addition, rapidly increasing demand in many countries necessitates timely and accurate investment decisions to ensure grid capacity. With increasing weather anomalies and weather-dependent production, advanced forecasting is fundamental for secure and optimal grid operation. Finally, the evolving geopolitical situation requires a robust, data-driven, and resilient cyber defence that safeguards the power system at all times, including when external entities try to sabotage its operation.

Implementing DTs will contribute to solving major challenges and exploiting opportunities. They will provide relevant insights for informed decision-making for grid planning and system operation, leading to improved security of supply and grid utilisation, as well as enabling customer integration to increase flexibility. This digitalisation effort supports creating a sustainable, secure, and competitive energy market.

The joint task force emphasises the importance of addressing key challenges to digitalisation for the future of the EU electricity system. Fundamental barriers are connected to data quality, standardisation, and access.

OPAL-RT TECHNOLOGIES

CYBERSECURITY IN THE EUROPEAN POWER SYSTEM SECTOR



NEWS

First Network Code on Cybersecurity for the electricity sector has been published

24 May 2024

DSO Entity and ENTSO-E Joint Statement on Cyber Security Network Code

Today, the European Union published the first-ever EU Network Code on Cybersecurity for the electricity sector. The publication is an important step to improve the cyber resilience of critical EU energy infrastructure and services.

The new Network Code on Cybersecurity has been developed in response to the growing digitalisation and interconnection of national power systems. It provides a common standard to ensure the security and reliability of the interconnected system.

Emergency Response Coordination Centre (ERCC)

OPAL-RT TECHNOLOGIES
17,642 followers
5d • Edited •

⚡ A fantastic close to XX ERIAC 2025 in Ciudad del Este, Paraguay — and we're returning home with an award!

🏆 We're thrilled to share that Thais Marzalek Blasi's paper, "Cyber-Physical Co-Simulation Platform for Cybersecurity Studies in Electric Power Systems," received 2nd place for Best Paper presented at Study Committee D2 (CIGRE) during the event!

This honorable recognition is strong validation of our work advancing real-time cybersecurity research through co-simulation — powered by our Cyber-Physical solution with EXata.

📄 Check out the paper here (Access requires XXERIAC 2025 credentials):
https://lnkd.in/d5_NJYw5
Curious to learn more? Feel free to reach out—we'd love to share insights!

Thank you to everyone who attended Thais's session and visited our booth to engage with her and Rita Kwiek on the future of cyber resilience in electric power systems.

CYBER THREATS ON POWER GRID

Modern power grids are Cyber-Physical Systems (CPS) composed of electrical and information infrastructure

- Wide deployment of new technologies
- Substation, transmission and distribution automation
- More Distributed Energy Resources (DER)
- Advanced two-way communication networks
- Development of synchrophasor systems

Cyber-Physical System (CPS)

Conventional power grid

Communication network infrastructure

New technologies, new challenges on cyber security: Accidental[1)] and Malicious

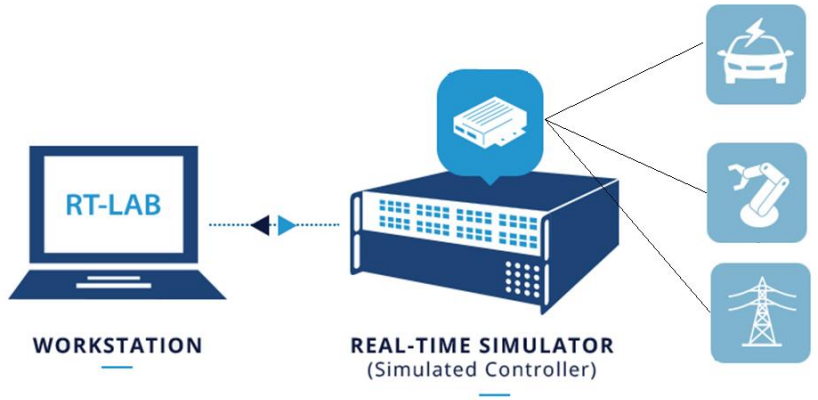
1) See NIST Program "Cybersecurity for Smart Grid Systems"

Source: EPRI 2007

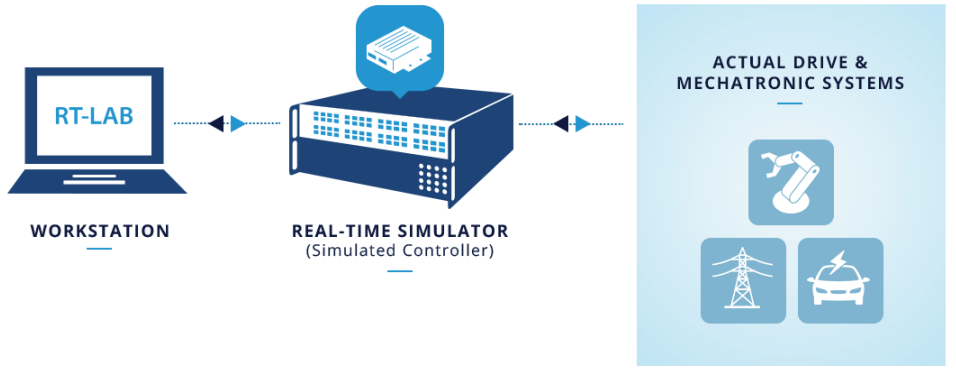
OPAL-RT TECHNOLOGIES

TESTING APPROACHES

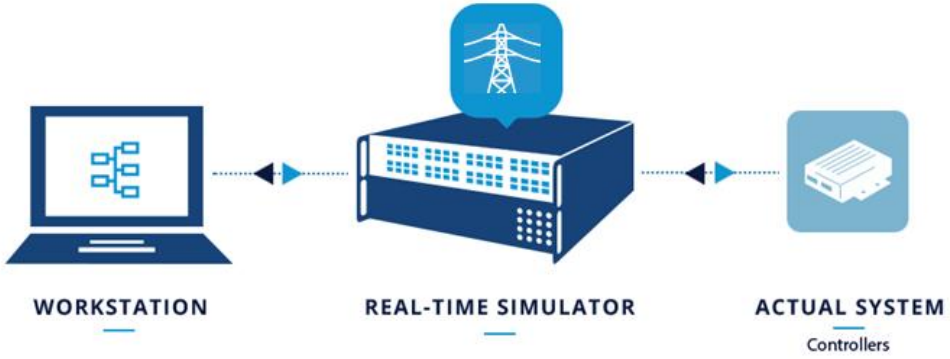
MODEL/SOFTWARE-IN-THE-LOOP



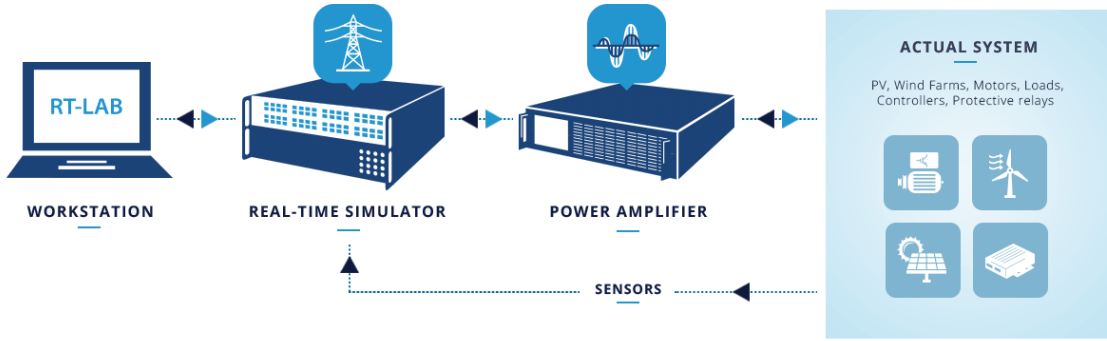
RAPID CONTROL PROTOTYPING



HARDWARE-IN-THE-LOOP



POWER HIL



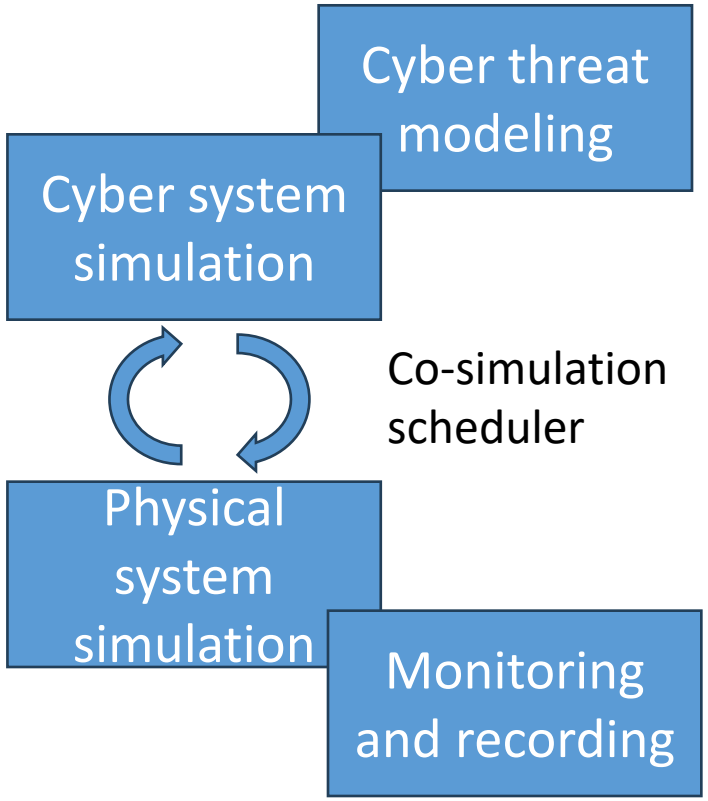
OPAL-RT TECHNOLOGIES

REAL-TIME
Co-Simulation

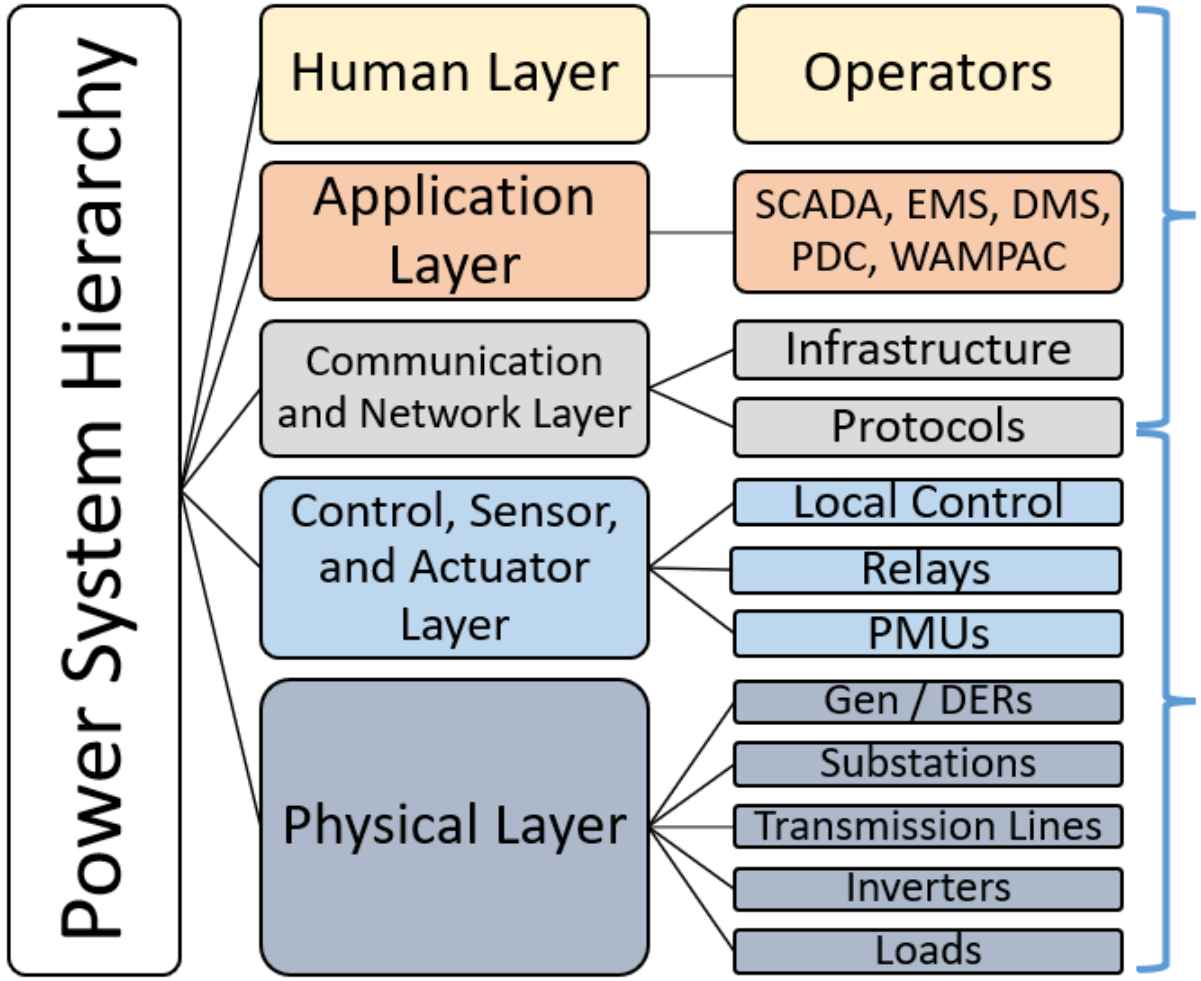
OPAL-RT TECHNOLOGIES

CYBER PHYSICAL SYSTEM CO-SIMULATION

- Transition of traditional grids to smart grids brings challenges
- Near impossible to perform cybersecurity research in real environment
- CPS testbed: integration of physical and cyber systems within a simulation environment
- Different simulation testbeds: offline, real time
  - Synchronization is the main challenge in offline co-simulation testbed
  - Real time testbed does not have same synchronization problem
  - Ability to interface hardware devices such as controllers, SCADA systems in real time testbed



CYBER-PHYSICAL SYSTEM CO-SIMULATION



Communication simulation

Power grid simulation

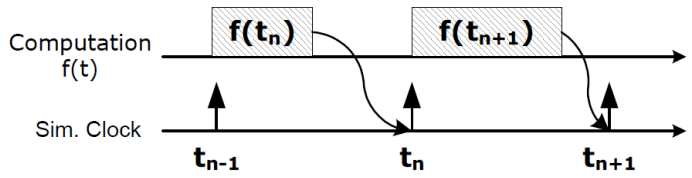
KEYSIGHT TECHNOLOGIES

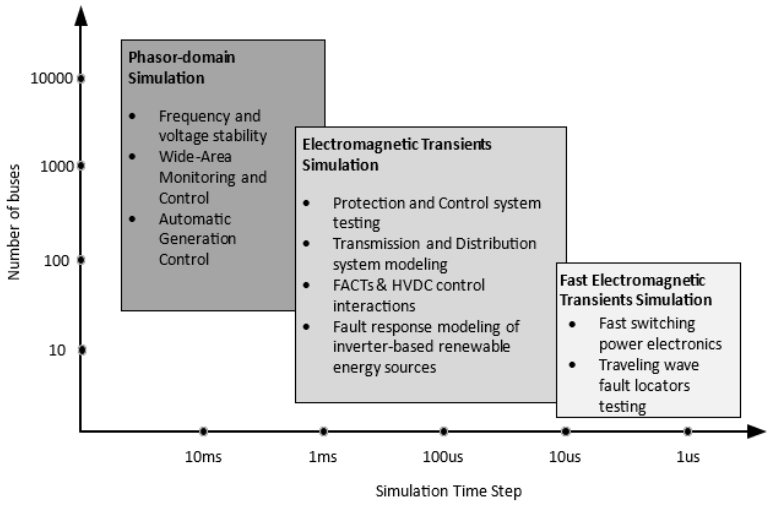
OPAL-RT TECHNOLOGIES

OPAL-RT TECHNOLOGIES

REAL-TIME SIMULATION OF POWER GRID

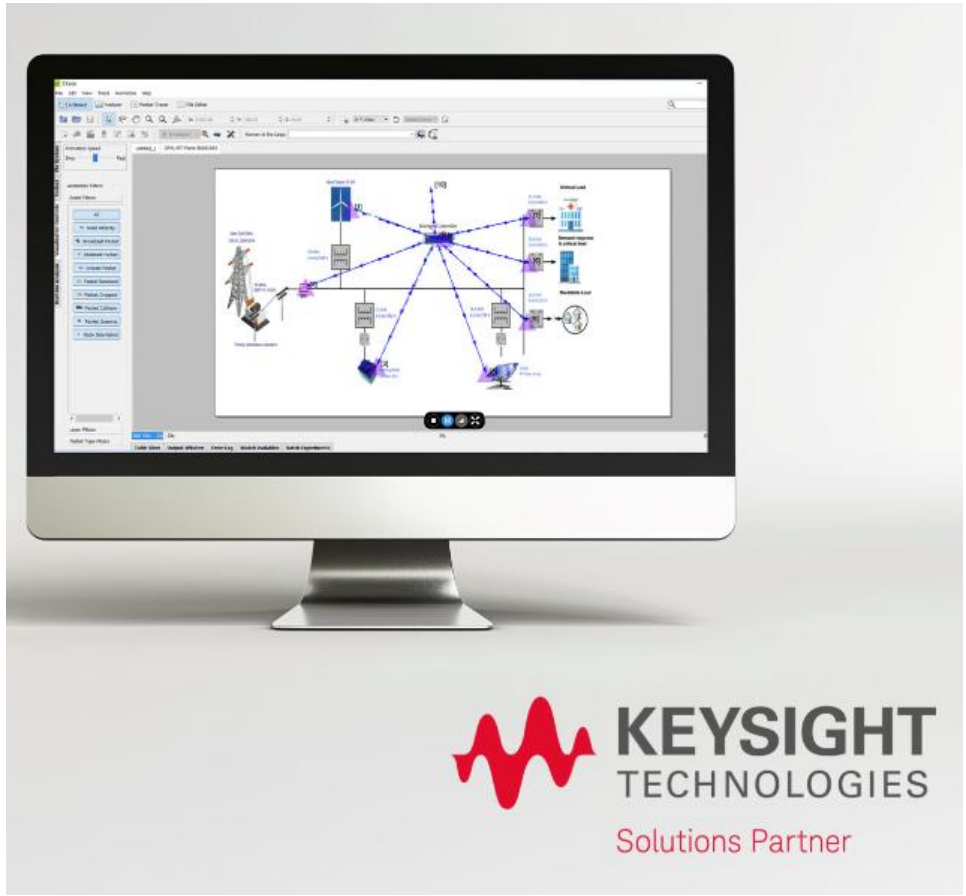
- Real time simulation (RTS) definition
- RTS simulates a wide range of frequencies for different applications
  - Phasor domain
  - Electromagnetic transients
  - Fast electromagnetic transients
- Support of Analog, Digital I/Os and Communication Protocols such as
  - C37.118,
  - Modbus,
  - IEC 61850,
  - etc





REAL-TIME SIMULATION OF COMMUNICATION NETWORK

- Any CPS testbed must be able to model high fidelity communication network
- Network types such as satellite, wired, wireless, 5G can be designed
- Components such as switches, nodes, routers, satellite, connected to one another via communication links
- Cyber attacks such as packet modification, packet delay, hacking, social engineering (phishing email), DOS initiated, vulnerability exploitation, worm and virus propagation on nodes



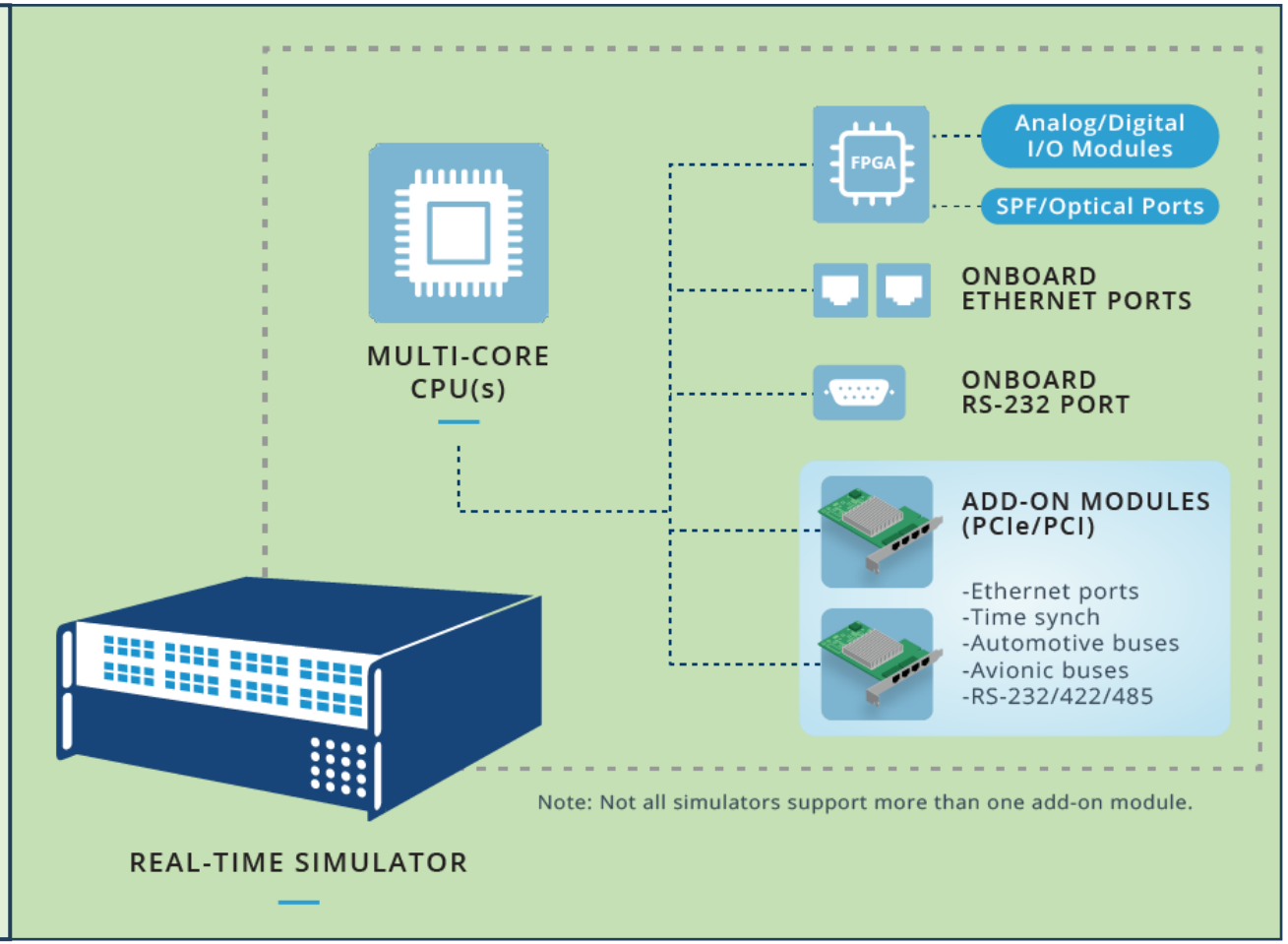
Cyber-Physical System (CPS)
Co-Simulation Testbed

OPAL-RT TECHNOLOGIES

INTEGRATED CYBER-PHYSICAL SIMULATION

Seamlessly combine advanced power grid simulation with cutting-edge communication network modeling in a single platform.

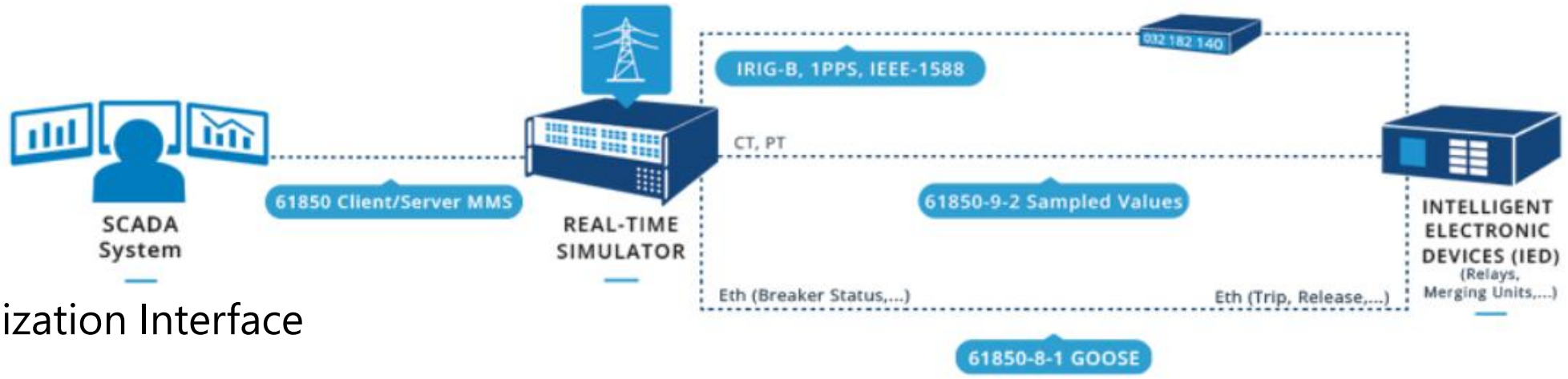
With built-in support for a wide range of communication protocols - including IEC 61850, DNP3, Modbus, and more - we enable realistic testing of system interactions, optimizing workflows and minimizing latency.



COMMUNICATION PROTOCOLS

Supported Communication Protocols with EXata CPS(Ethernet-Based)

- IEC61850 GOOSE, SV & MMS
- C37.118
- DNP3
- IEC 60870-5-104
- TCP/IP, UDP/IP
- Modbus TCP

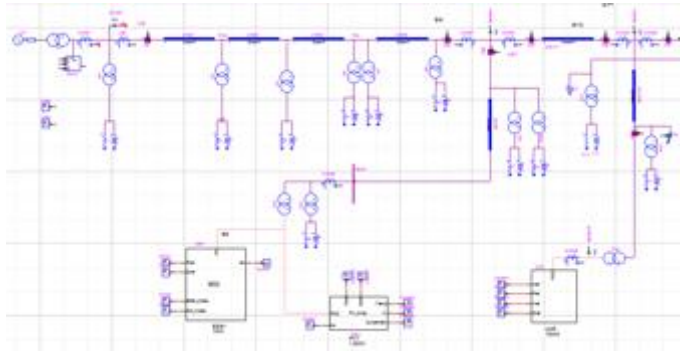


- Time Synchronization Interface

OPAL-RT TECHNOLOGIES

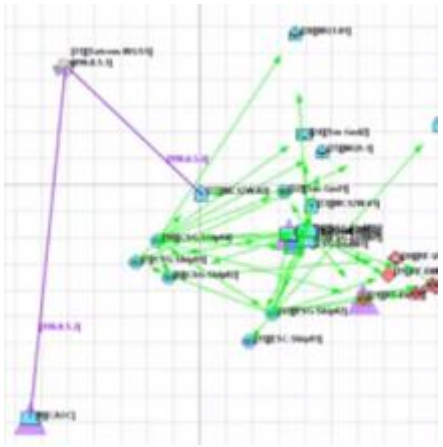
CYBER-PHYSICAL POWER SYSTEMS (CPPS) TESTBED

Virtual Power Grid



\+

Virtual Communication Network



Physical Devices & Systems
(SCADA, Relays, PMUs, IEDs, Controllers, etc)

Digital I/Os

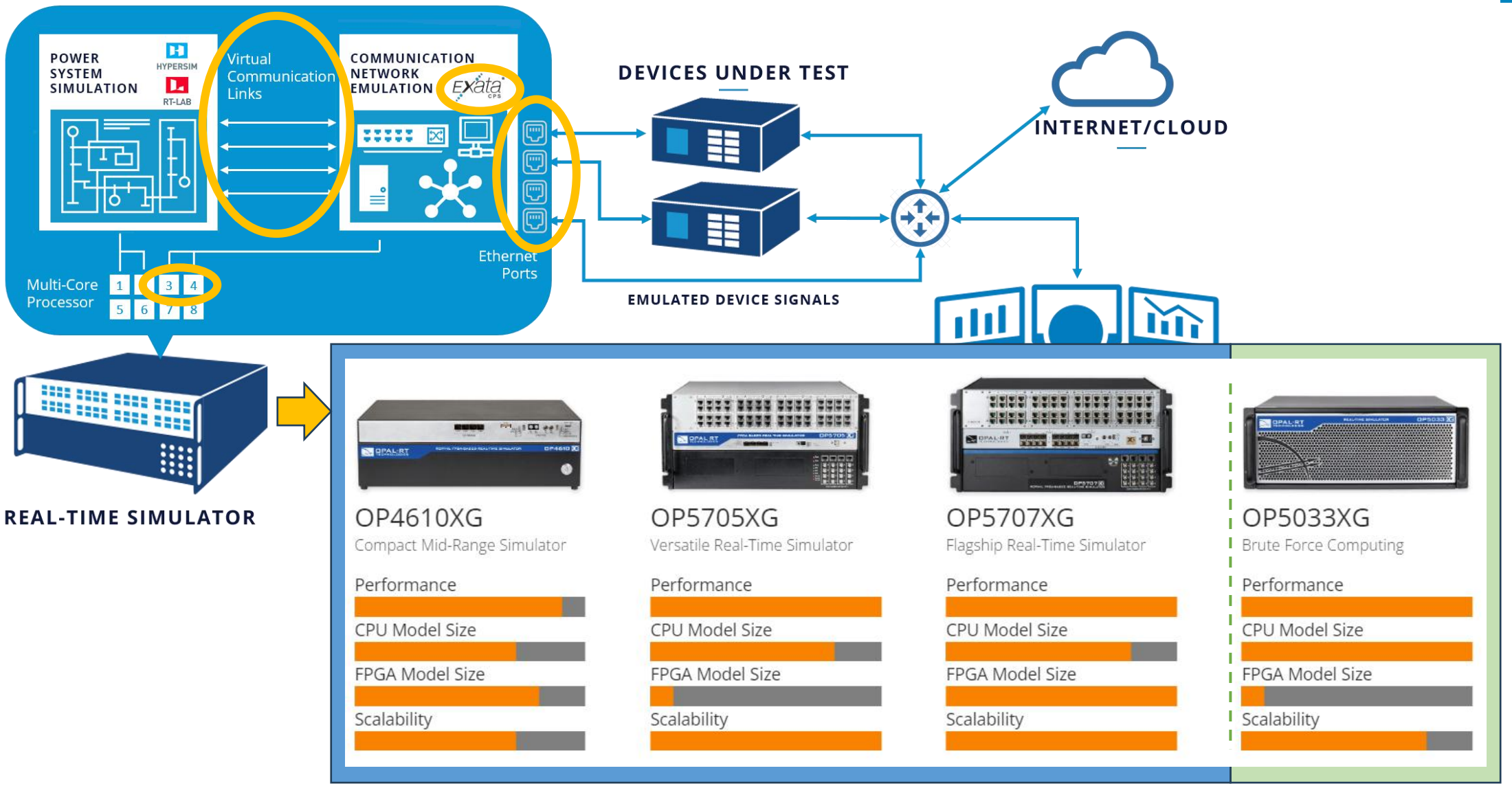
Analog I/Os

Time Synchronization (IRIG-B, 1PPS, IEEE 1588 PTP)

Communication Protocols (DNP3, IEC 61850, Modbus, C37.118, OPC-UA, IEC-104, etc.)

OPAL-RT TECHNOLOGIES

SOLUTION FOR CYBERSECURITY APPLICATIONS

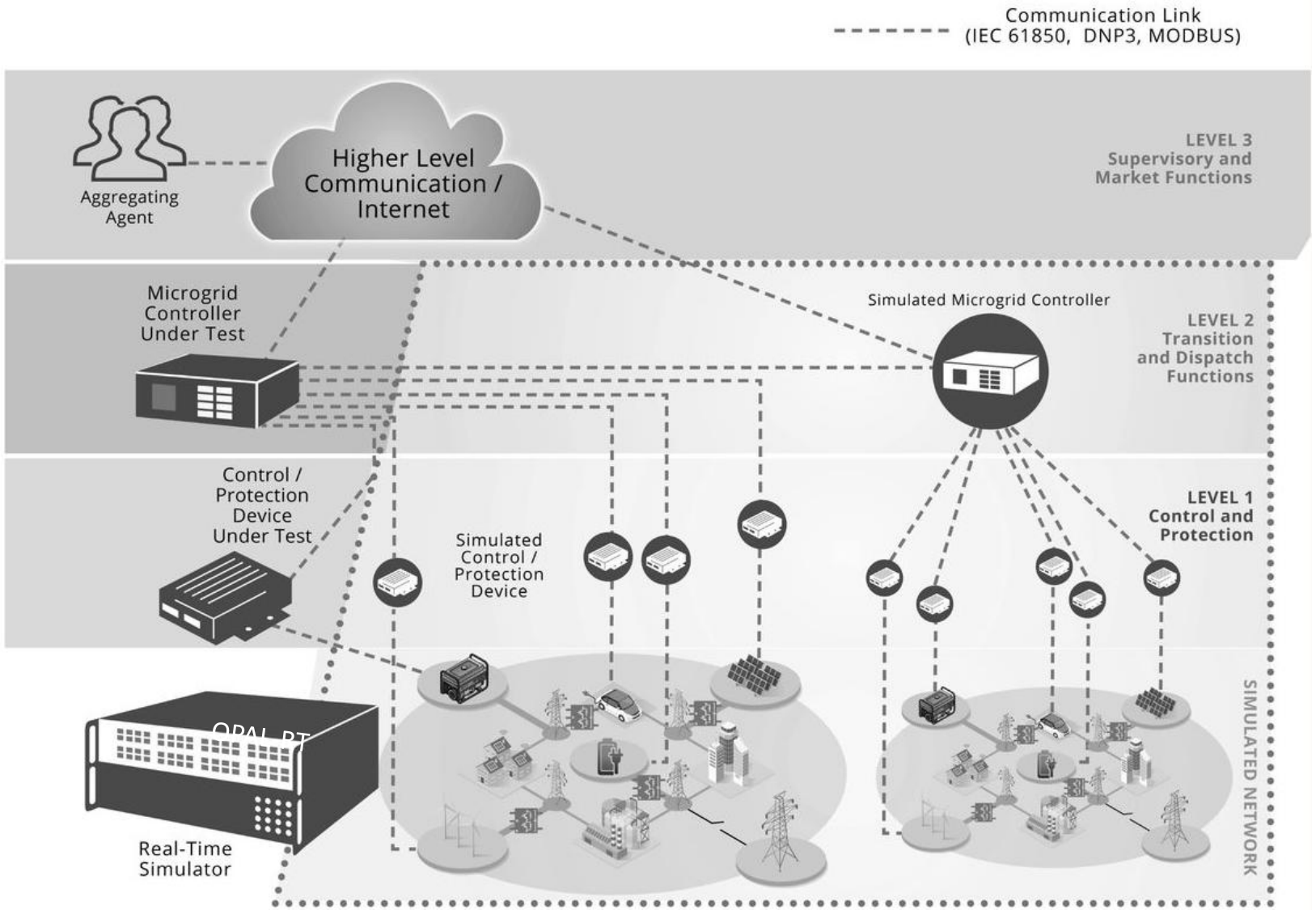


EXata CPS

OPAL-RT TECHNOLOGIES

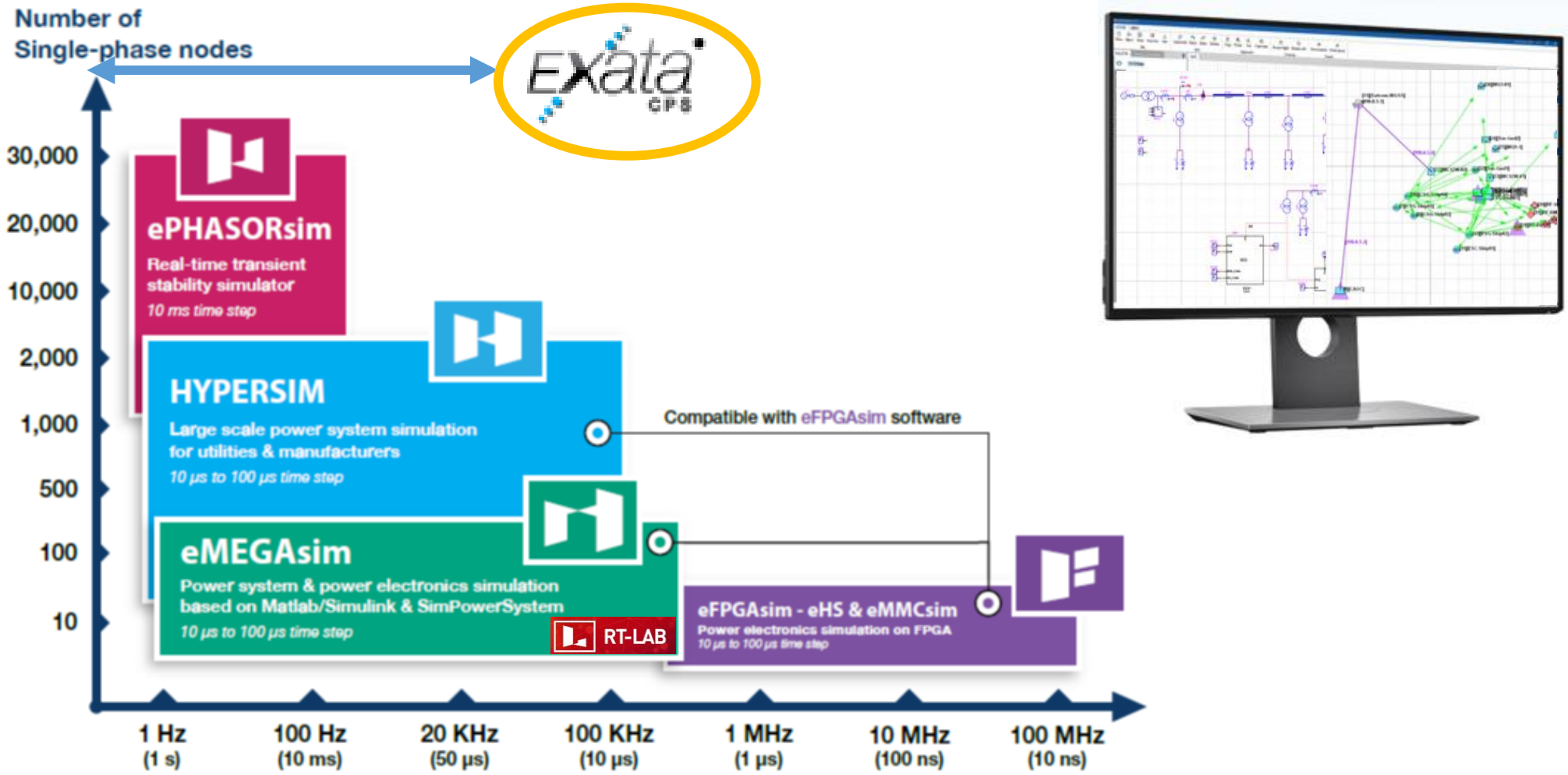
INTEGRATION OF GRID AND COMMUNICATION SYSTEMS

Communication System Emulators **(EXata CPS)** can be inserted at all levels to analyze performance and sensitivity to cyberattacks and to analyze counter-measures



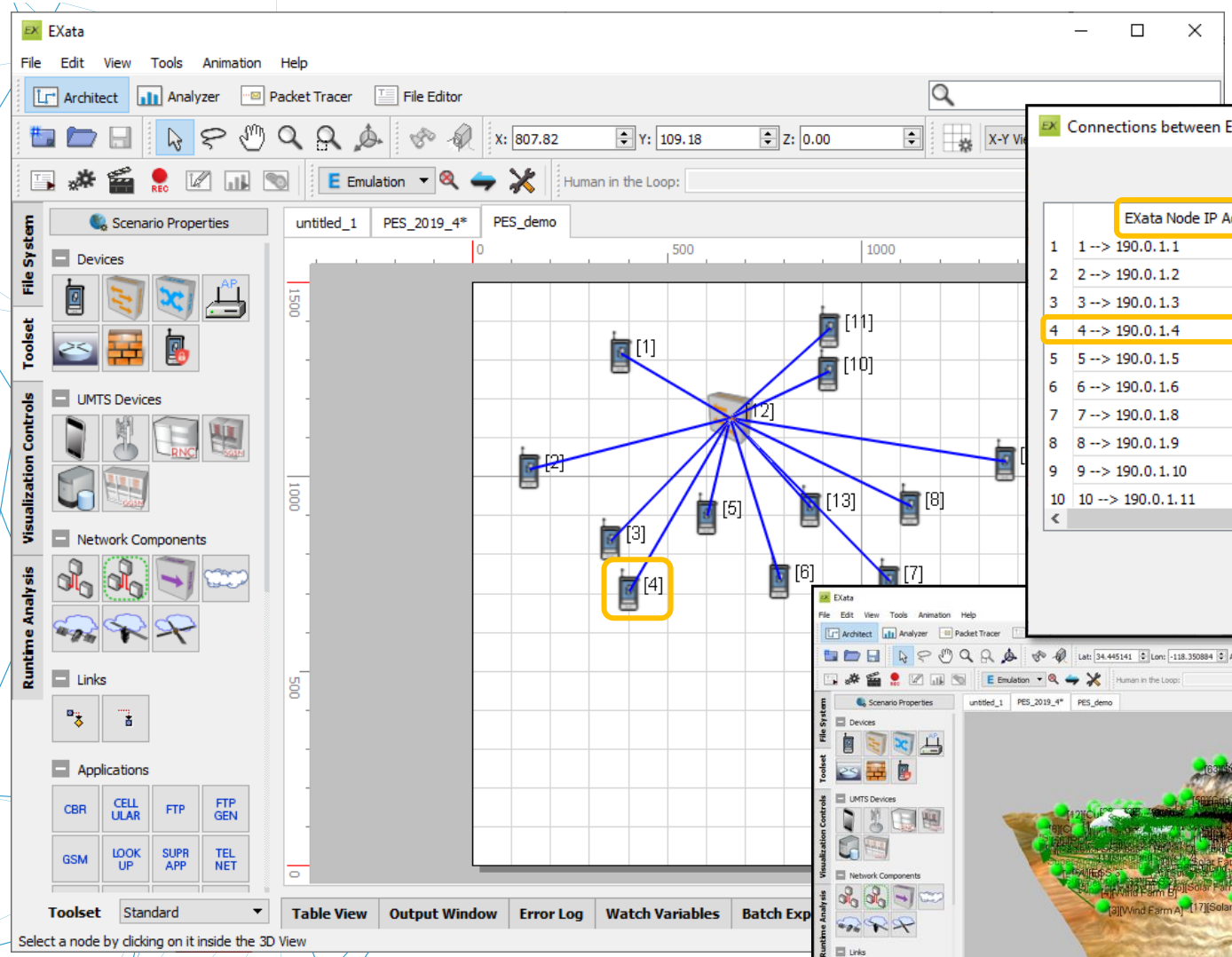
OPAL-RT TECHNOLOGIES

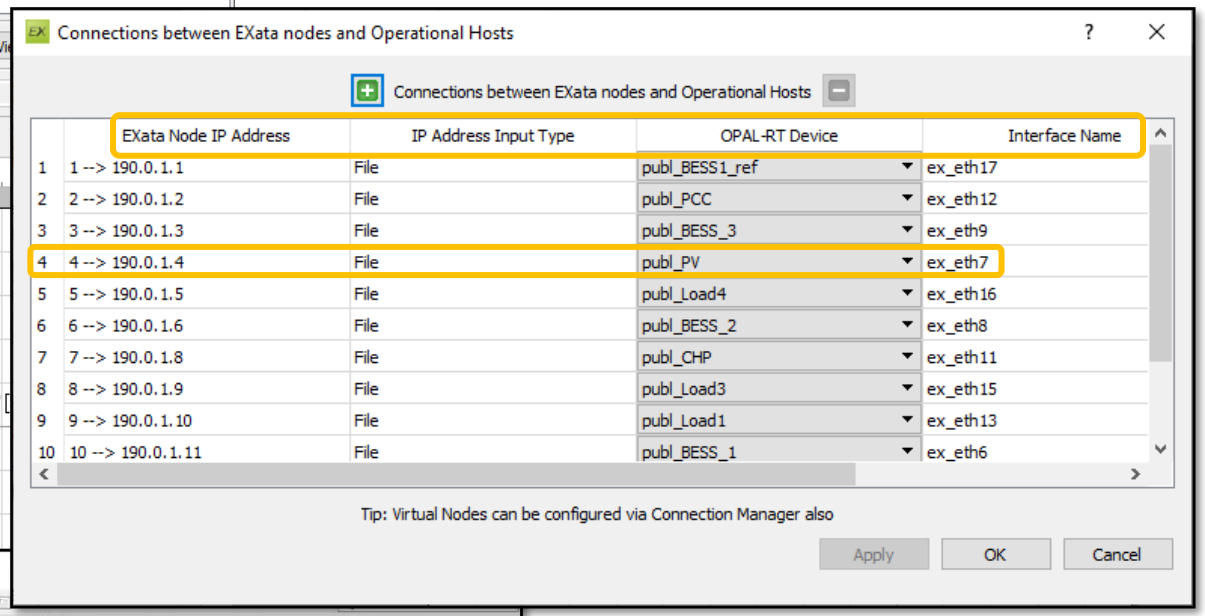
CYBER-PHYSICAL SYSTEM SIMULATION OVERVIEW

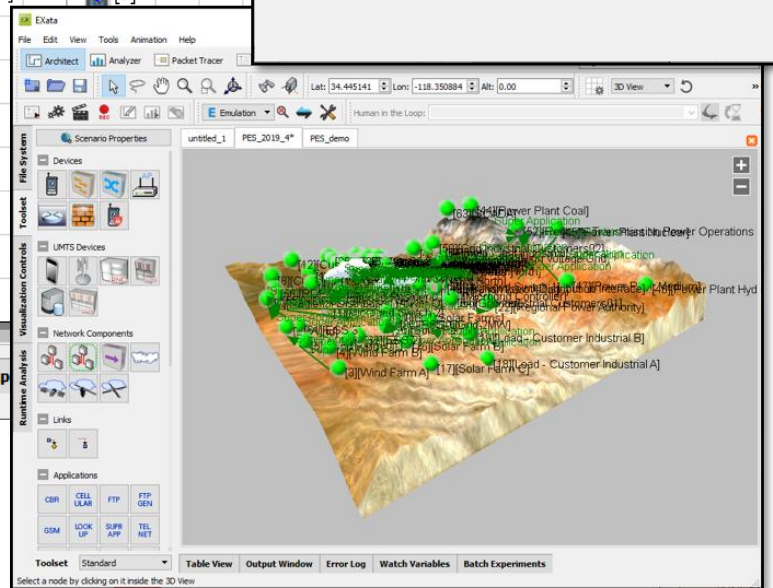


OPAL-RT TECHNOLOGIES

- MODELING, MAPPING, VIRTUAL COMMUNICATION LINK





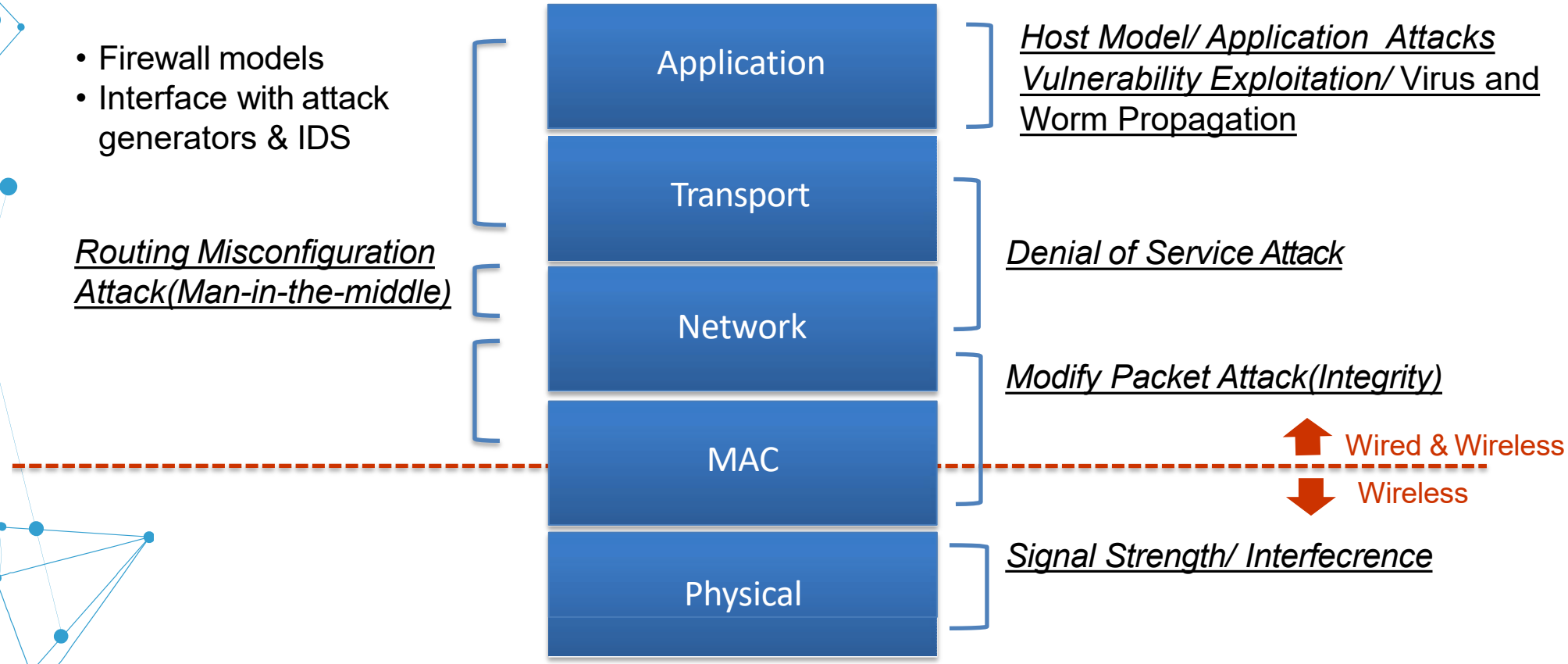


FRAMEWORK & LAYERS

Defensive Model

- Firewall models
- Interface with attack generators & IDS

Routing Misconfiguration Attack(Man-in-the-middle)



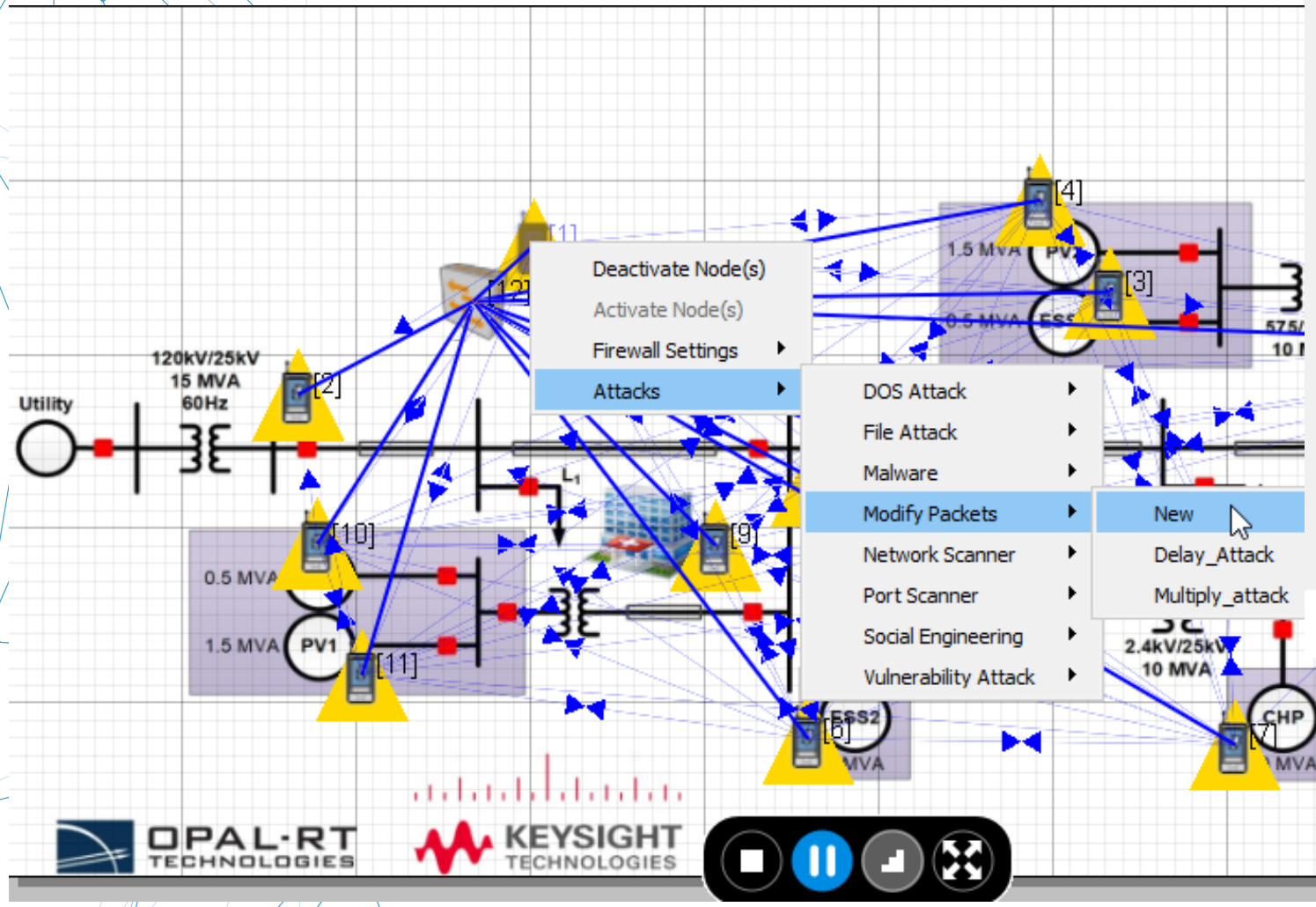
PRE-BUILT CYBERATTACK & DEFENSE LIBRARY

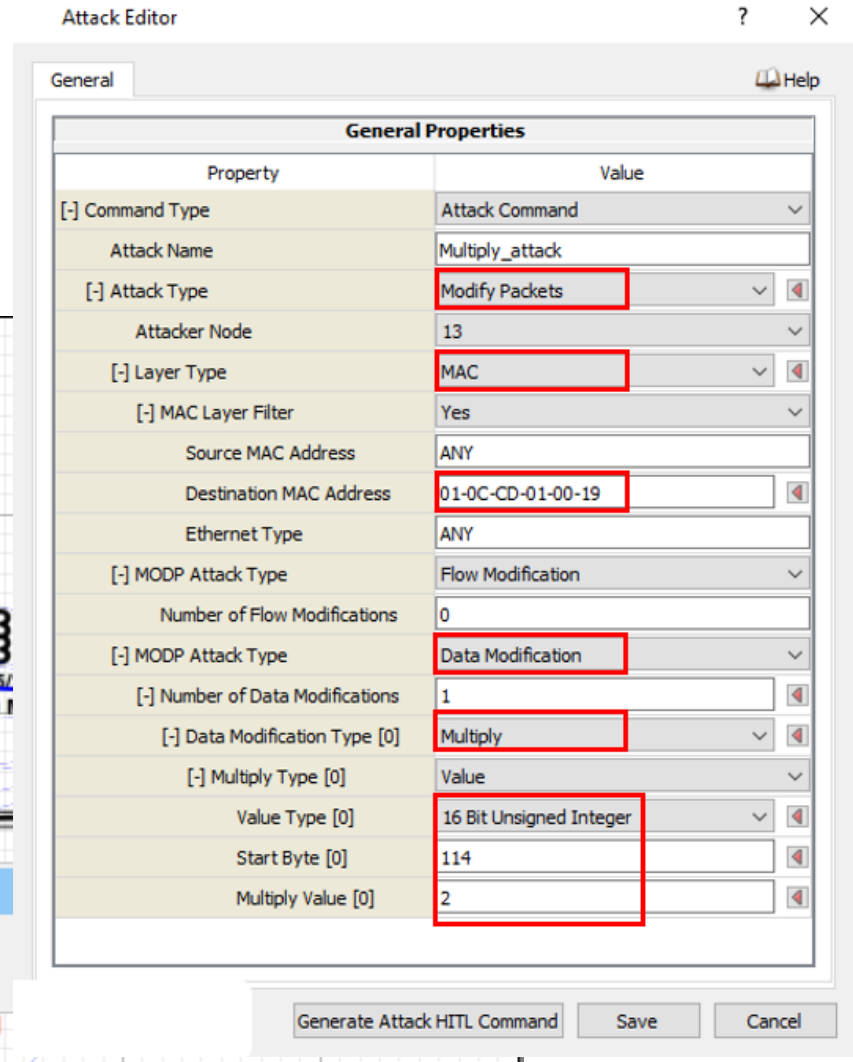
Model Name	Model Type
Adaptive Attacks	Attack Model
Anonymous On-demand Routing (ANODR) Protocol	Routing Protocol
Botnet Worm and Virus Attacks	Attack Model
CPU and Memory Resource Model	OS Resource Model
Credential Model: IFF Certificate	Network Layer
Data Transfer Attacks	Attack Model
Denial of Service (DOS) Attacks	Attack Model
File Attacks	Attack Model
Firewall Model	Network Layer
Hacking Attacks	Attack Model
Host Model	Application Layer
Information Assurance Hierarchical Encryption Protocol (IAHEP)	Network Layer
Internet Protocol Security (IPSec) Model	Network Layer
Internet Security Association and Key Management Protocol with Internet Key Exchange (ISAKMP-IKE)	Network Layer
Malware Virus Attacks	Attack Model
Malware Worm Attacks	Attack Model
Modify Packets Attacks	Attack Model
Network Scanning Attacks	Attack Model
Phishing Email Attacks	Attack Model
Port Scanning Attacks	Attack Model
Public Key Infrastructure (PKI) Model	Network Layer

- Accelerate your cybersecurity testing with a readily available library of programmable attack and defense models.
- Simulate real threats like man-in-the-middle, denial-of-service, and spoofing, while testing countermeasures such as firewalls and antivirus solutions—saving months of development time.

Model Name	Model Type
Ransomware Attacks	Attack Model
Remote Access Attacks	Attack Model
Rootkit Attacks	Attack Model
Secure Neighbor Model	Network Layer
Vulnerability Attacks	Attack Model
Wired Equivalent Privacy (WEP) and CTR with CBC-MAC (CCMP) Model	MAC Layer
Wormhole Model	MAC Layer

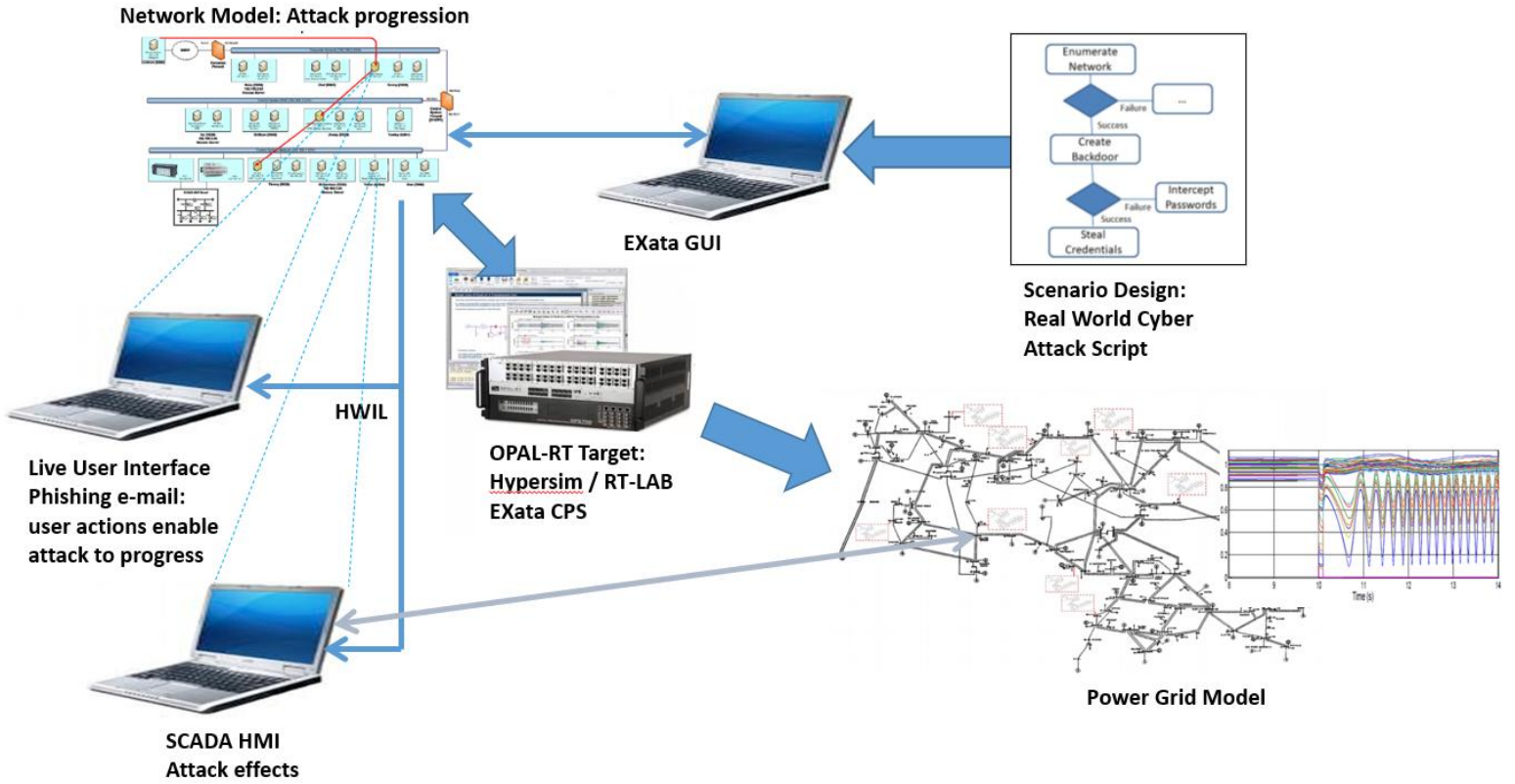
- CYBER ATTACKS



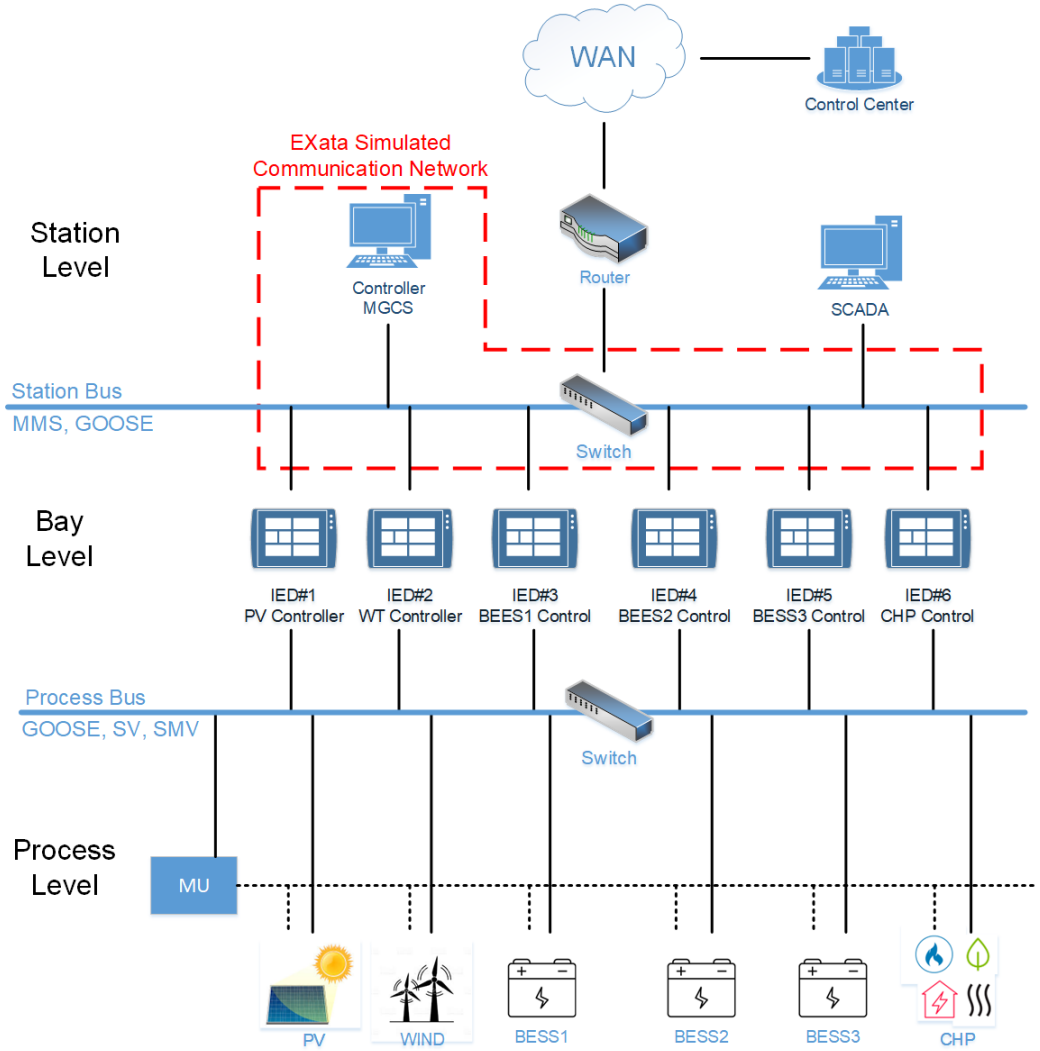


UKRAINE CYBER ATTACK SIMULATION (**SCADA**)

- Scenario based on cyber-attack which caused outage on Ukraine power grid in 2015
- Power grid model in HYPERSIM
- Network model with grid operators, SCADA HMI
- Attacks:
  - Social engineering attack -> phishing email
  - Worm infecting PCs, stealing credentials of SCADA HMI operator workstation
- Attacker uses remote connection to SCADA HMI workstation and causes power outage by opening breakers



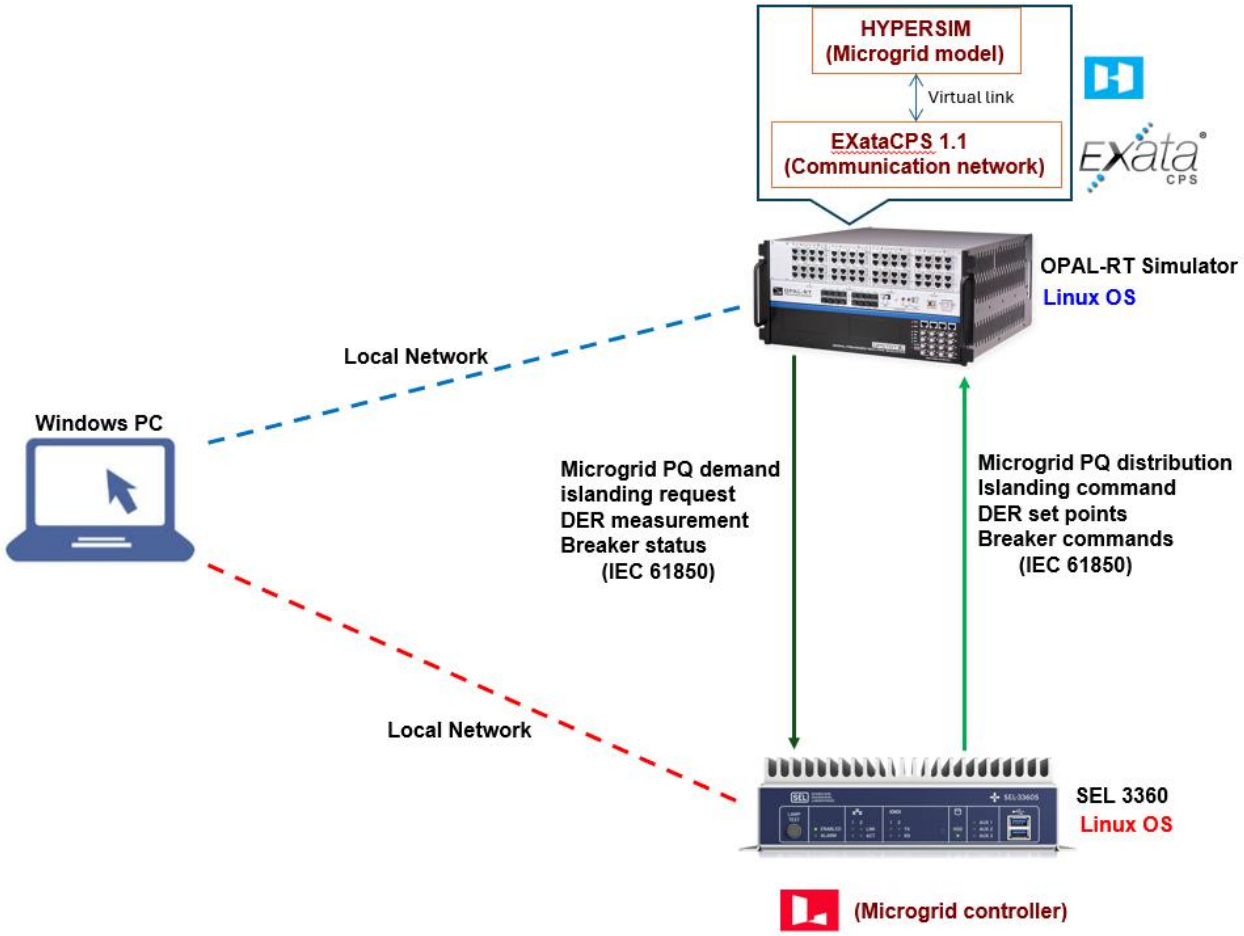
HIL MICROGRID CONTROL (**IEC 61850**)



- Communication topology based on IEC 61850
- GOOSE messages transmitted between Controller and IEDs assigned to DERs
- Simulated network is between IEDs at bay level, Microgrid controller at station level, and a switch

OPAL-RT TECHNOLOGIES

HIL MICROGRID CONTROL (**IEC 61850**)



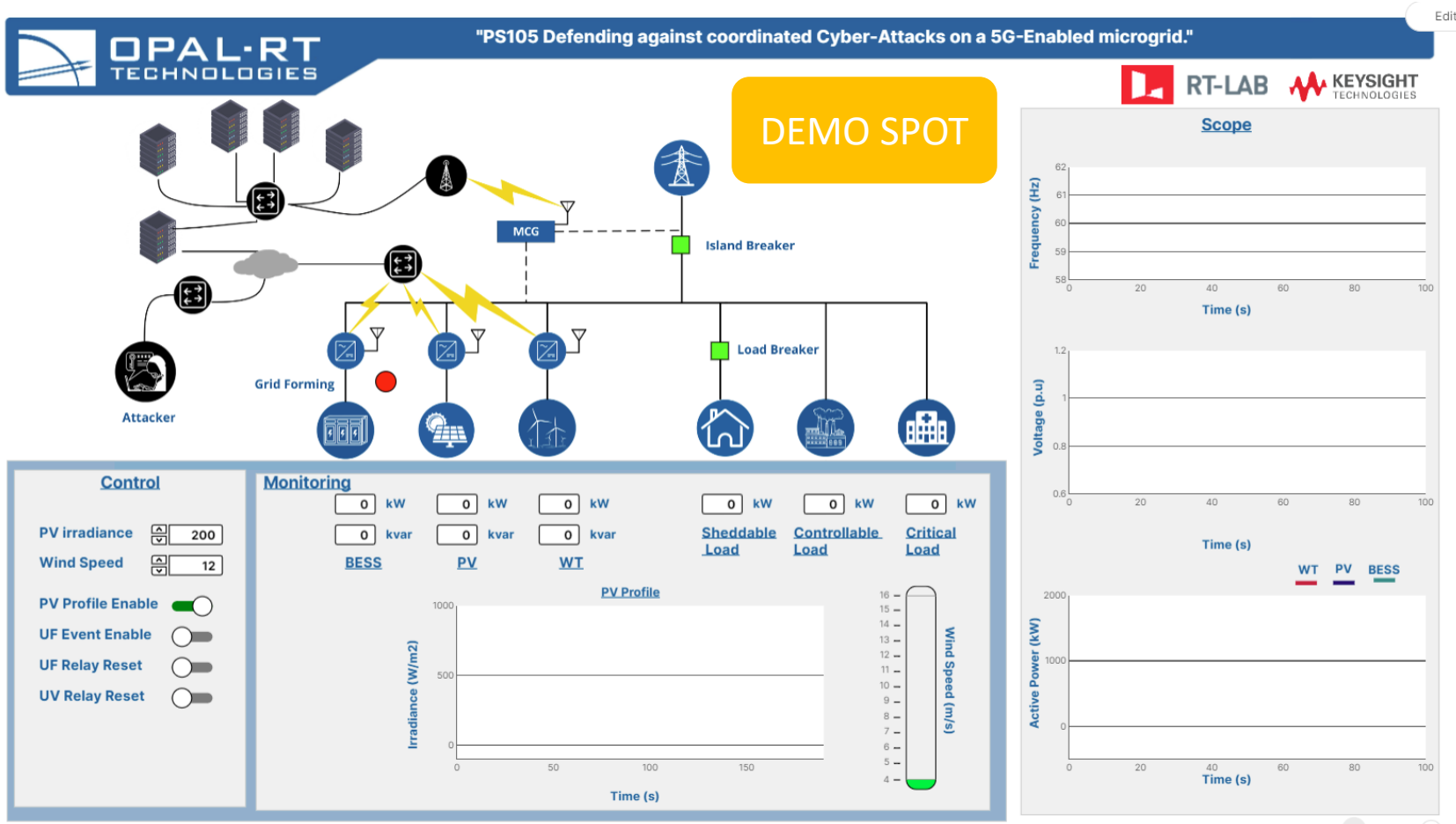
OPAL-RT TECHNOLOGIES

DEFENDING AGAINST COORDINATED CYBER-ATTACKS ON A 5G-ENABLED MICROGRID

Hybrid simulation of a Microgrid system

- EMT (Electromagnetic Transients) simulation
- Cyber-attack modeling

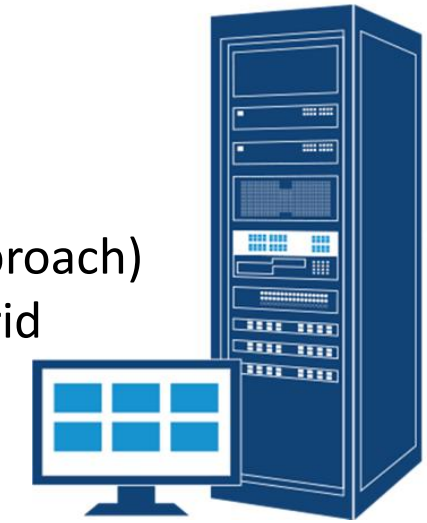
Analyze the effects of various cyber threats on Power Systems, particularly focusing on Microgrids with Distributed Energy Resources (DERs).



LEVERAGING CO-SIMULATION HIL PLATFORMS

Simulate Complex Attack Scenarios

Complex and adaptative cyber-attacks as malware, DDoS, data integrity manipulation, and protocol exploits in controlled environments



Validate & Test

Hybrid testing environment (HIL approach) for IEDs, digital substation, power grid and SCADA control centers

Develop Countermeasures

Enabling responses to emerging threats thanks to the development of robust/cyber-secure control algorithms to ensure the robustness and resilience of the electricity network

Aalborg University Denmark
Arizona State University
Australian National University
Boise State University
Carleton University
FISK University
FIU Florida International University
FSU Florida State University
Kansas State University
Technische Universität Ilmenau
OntarioTech University
Purdue University Northwest
McGill University
Tennessee State University
TUHH Technische Universität Hamburg
University of Sheffield
Texas State University
The University of Texas Permian Basin
University of Central Florida
UF University of Florida
Universidad del Valle
University of Alberta
University of Calgary
The University of New Mexico
University of Illinois Chicago
University of Nevada, Reno
KAUST
UTSA The University of Texas at San Antonio
University of Georgia
UNSW The University of New South Wales
The University of Texas at El Paso
Imperial College London
UM6P University Mohammed VI Polytechnic
Zhejiang University
Vaasan yliopisto University of Vaasa
Brookhaven National Laboratory
New York Power Authority
institutos lactec
HOPS
CEPRI 中国电力科学研究院 China Electric Power Research Institute
DSO National Laboratories
Lawrence Livermore National Laboratory
KIT Karlsruhe Institute of Technology
Sandia National Laboratories
Southern Company
PSYMETIS
OPAL-RT TECHNOLOGIES