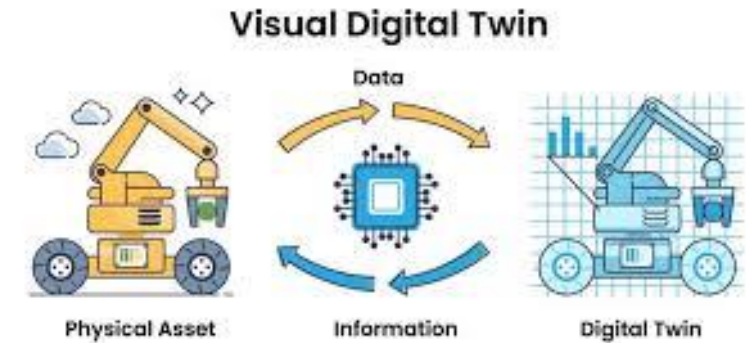


## Integrated Project Cyber security of energy systems for the digital-energy transition

*Design of cybersecurity twins based on ICT-power co-simulation*



- Digital twins are virtual replicas of physical systems—assets, processes, or entire infrastructures—that stay synchronized with the real world through data. They let you observe, simulate, predict, and optimize how something behaves before acting on the physical system.
- A digital twin combines:
  - A physical object or system
  - A digital model
  - Live data connection
  - Analytics & simulation





- Design a cybersecurity twin for energy systems
  - Integrate ICT and power system
  - Assess the impact of anomalies and cyberattacks
  - Support secure design and cybersecurity training
- Evaluation
  - Resilience
  - Impacts of adverse events
  - PKI on scale up scenarios

## Objectives:

- Digital replica of electrical and ICT systems
- Co-simulation of ICT events and power dynamics
- Analysis of normal and attack scenarios
- Connection with RSE test facilities





Criterion	OMNeT++	NS3	Containernet-WiFi
Scalability	✓	✓	÷
Protocol and Network Fidelity	÷	✓	✓
Extensibility and Modularity	✓	✓	✓
Ease of Use	÷	÷	✓
Reproducibility and Experiment Control	✓	✓	÷
Observability and Results Analysis	✓	✓	✓
Wireless and 5G Network Modeling	✓	✓	÷
Execution of Real Applications / Industrial Protocols	÷	÷	✓
Modeling of Resource-Constrained Hosts	x	x	✓
Long-Duration Orchestration	÷	÷	✓

✓ = full support  
 ÷ = partial / indirect support  
 x = not supported / impractical

### OMNeT++

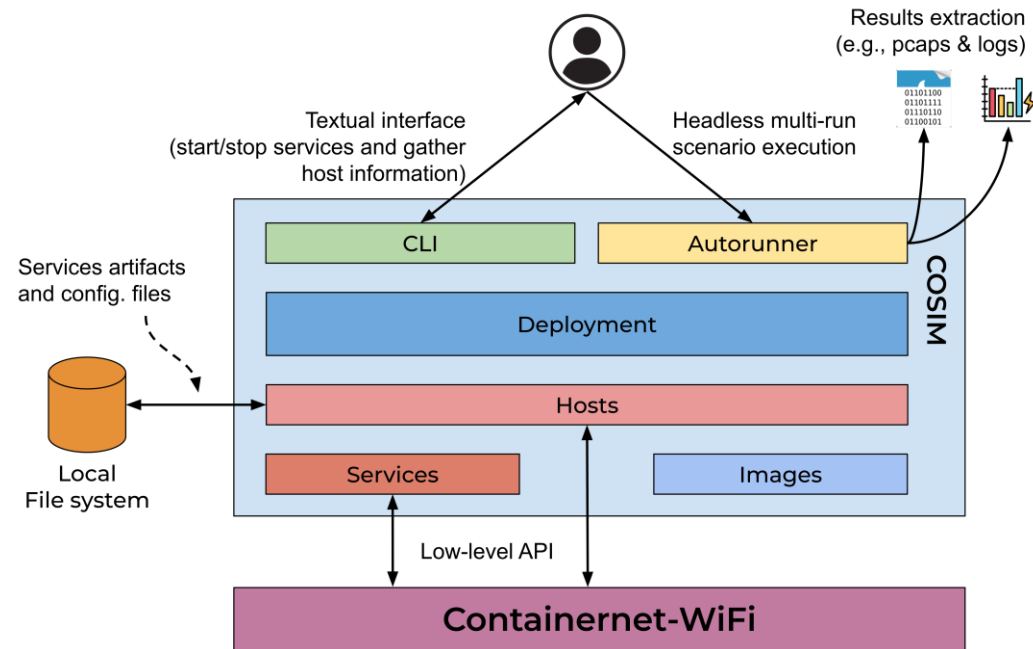
- ✓ High scalability
- ✓ Strong reproducibility and result observability
- Limited protocol fidelity for industrial applications
- ✗ No support for real protocol execution or resource-constrained hosts

### NS-3

- ✓ High protocol and network fidelity
- ✓ Scalable and reproducible simulations
- Steep learning curve
- ✗ Limited support for real industrial protocol execution

### Containernet-WiFi

- ✓ Execution of real applications and industrial protocols
- ✓ Emulation of resource-constrained devices
- ✓ Long-duration experiment orchestration
- Limited scalability compared to discrete-event simulators



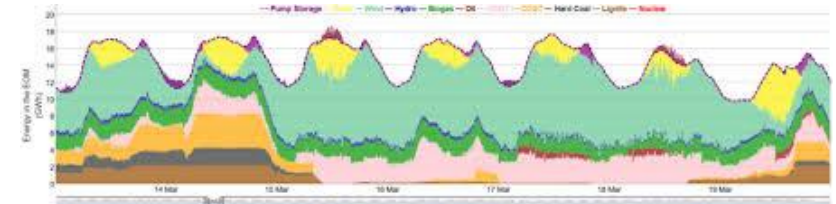
COSIM implements multiple abstraction layers on top of Containernet-WiFi

- Extension of Containernet-WiFi
- Automatic orchestration of scenarios
- Multi-run support and parametric analysis
- Emulation of resource-constrained devices

- Power System Simulator:
  - Steady state simulation
  - Dynamic simulation

## Analysis of network operation and control strategies

- Focus on flexibility
- Involvement of DSOs, Aggregators, and Distributed Energy Resources
- Short-term market sessions
- Critical information exchanges
- Phases vulnerable to cyberattacks



Within short-term local market operations, several information flows represent potential cyber-vulnerability points. The following four critical communication types are identified:

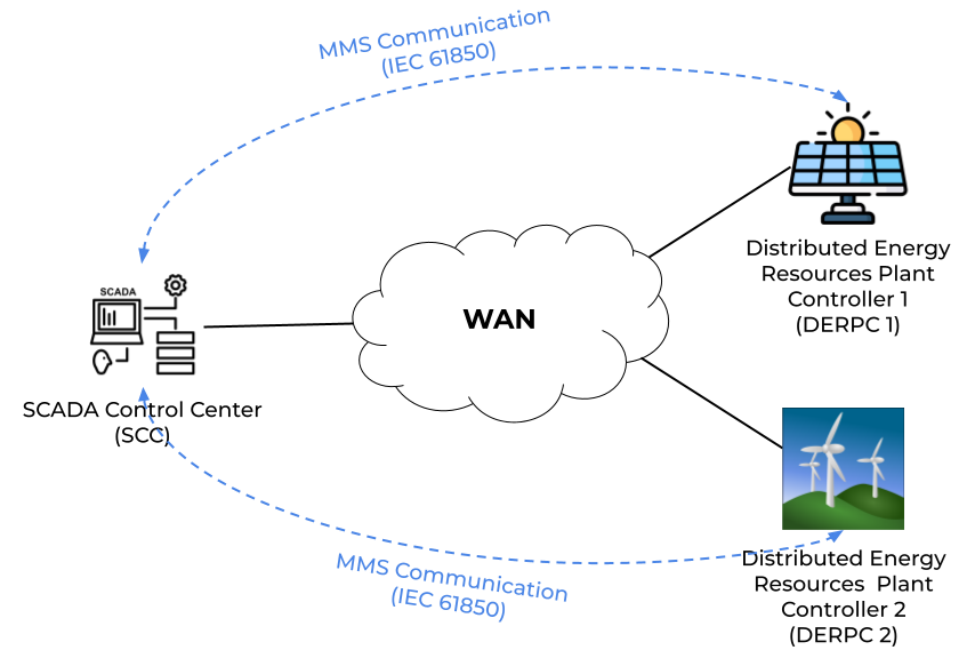
- Bid submission
  - Aggregators → DSO
  - Transmission of bids for participation in the local market
- Activation notifications
  - DSO → market participants
- **Communication of market clearing results and activation outcomes**
  - **Resource–aggregator data exchange**
    - **Resources ↔ Aggregator**
  - **Information exchange to determine the operational status of distributed resources**
- **Setpoint dispatch**
  - **Aggregator → resources**
  - **Transmission of setpoints for the execution of flexibility requests**



**DSO Scada Control Center (SCC)** is responsible for monitoring (by receiving periodic reports and sending explicit read requests) and controlling (issuing updated setpoints or state-modification commands) multiple **Distributed Energy Resources Plant Controllers (DERPCs)**.

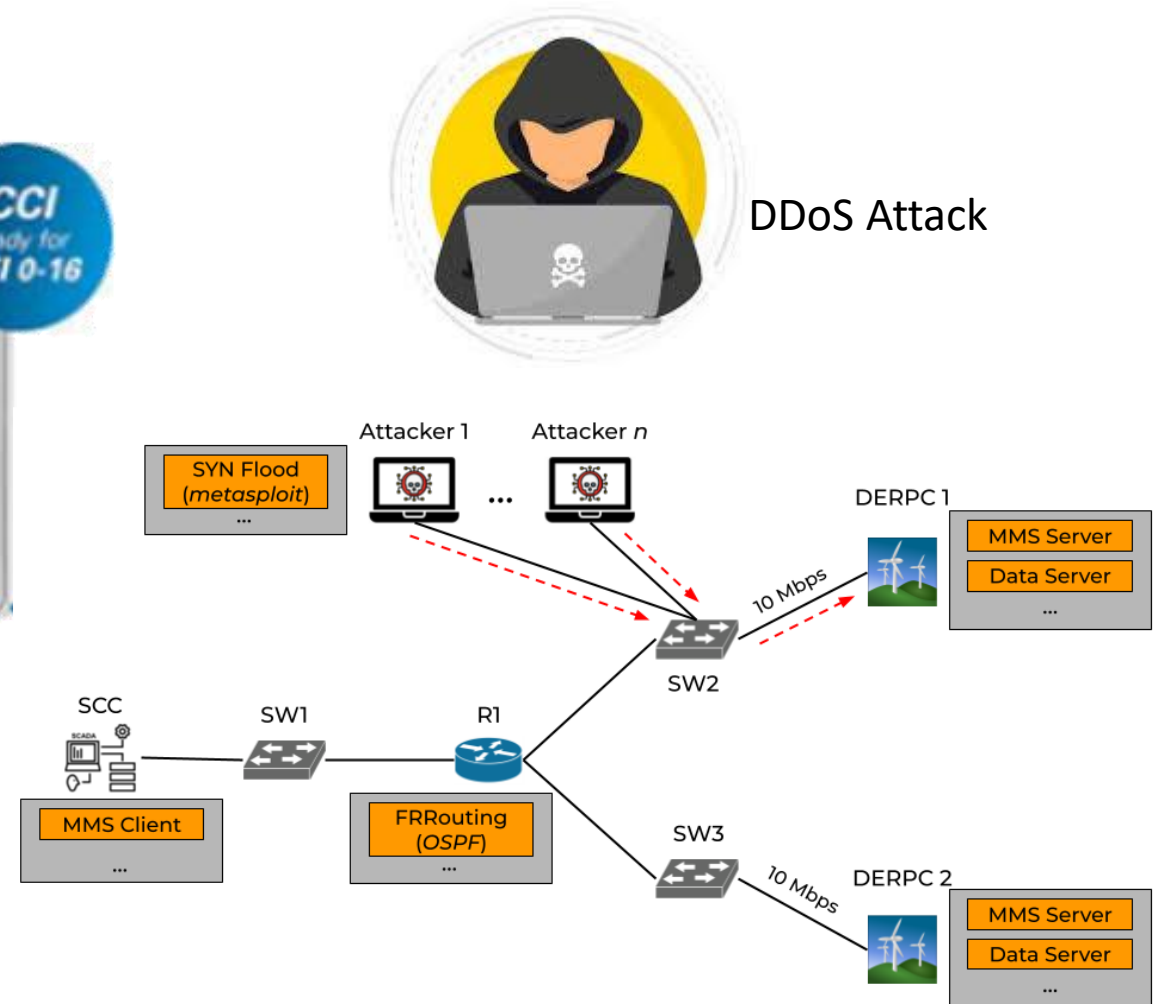
Communication on a Wide Area Network (WAN)

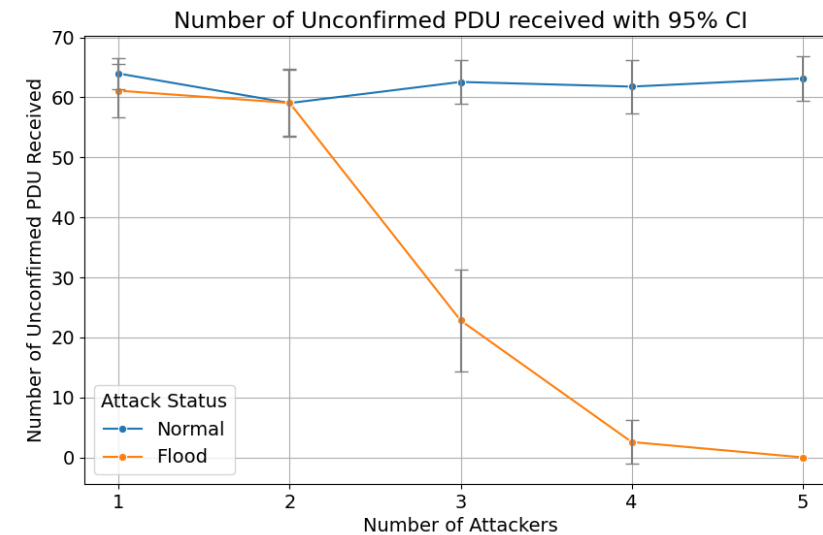
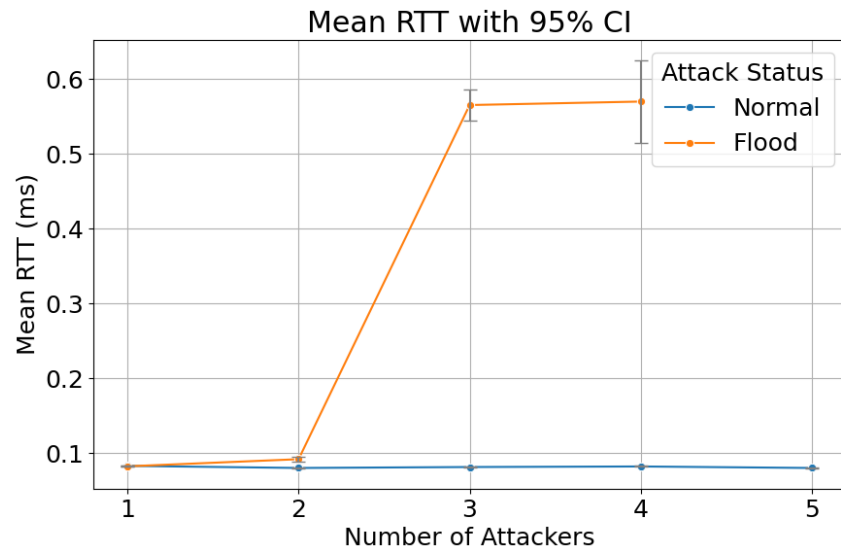
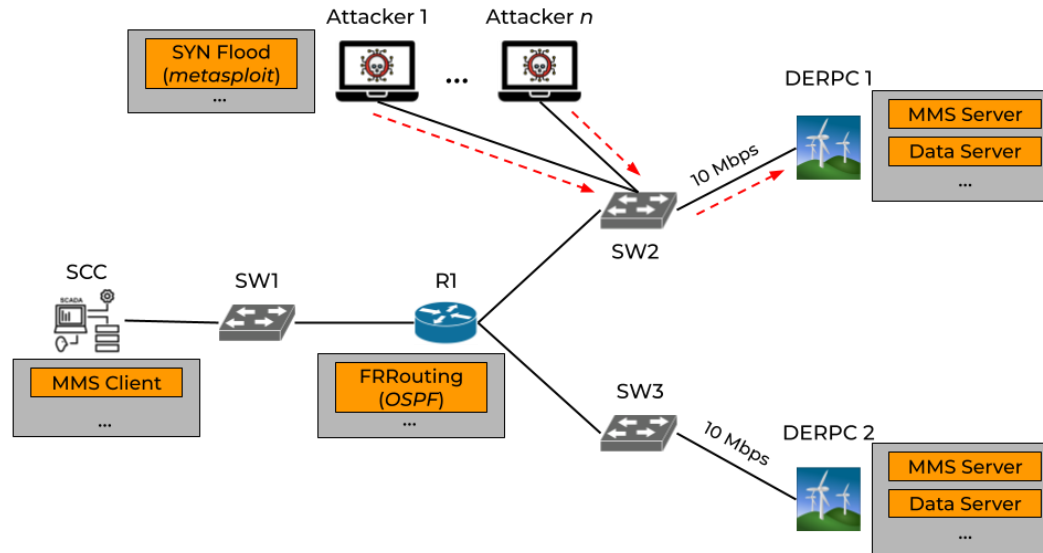
- Attack surface has largely expanded

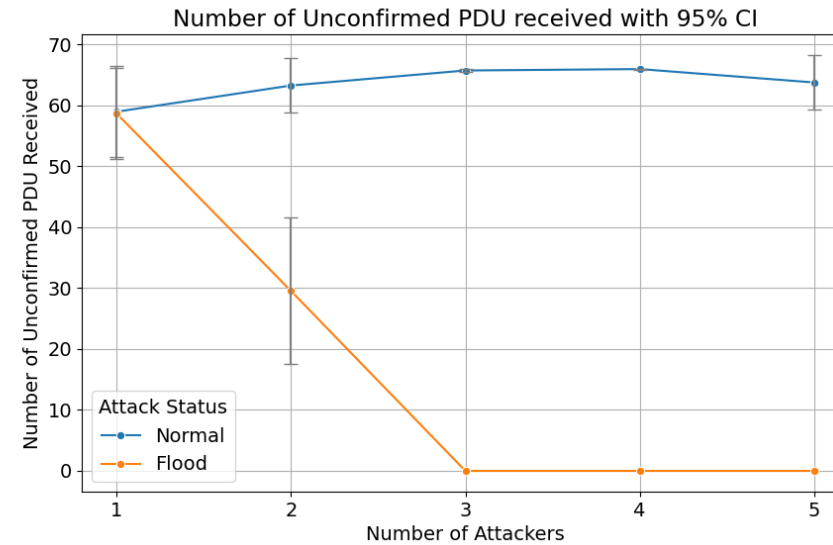
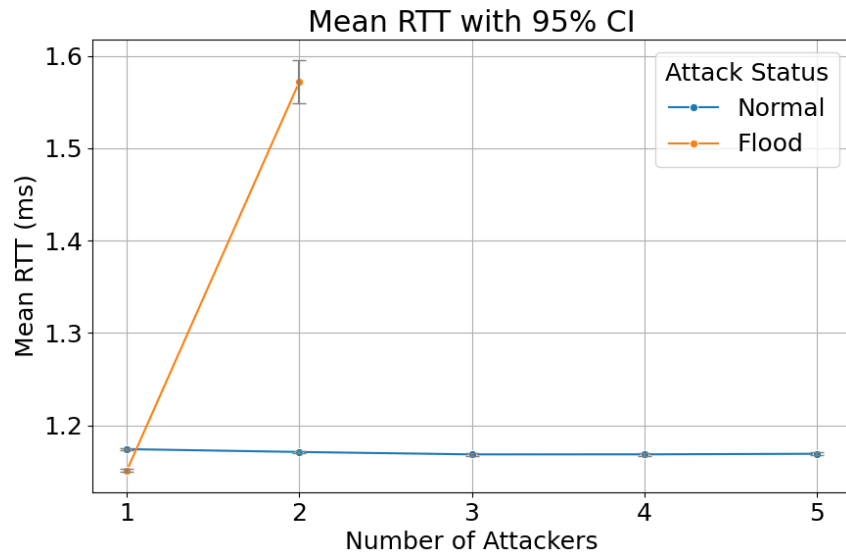
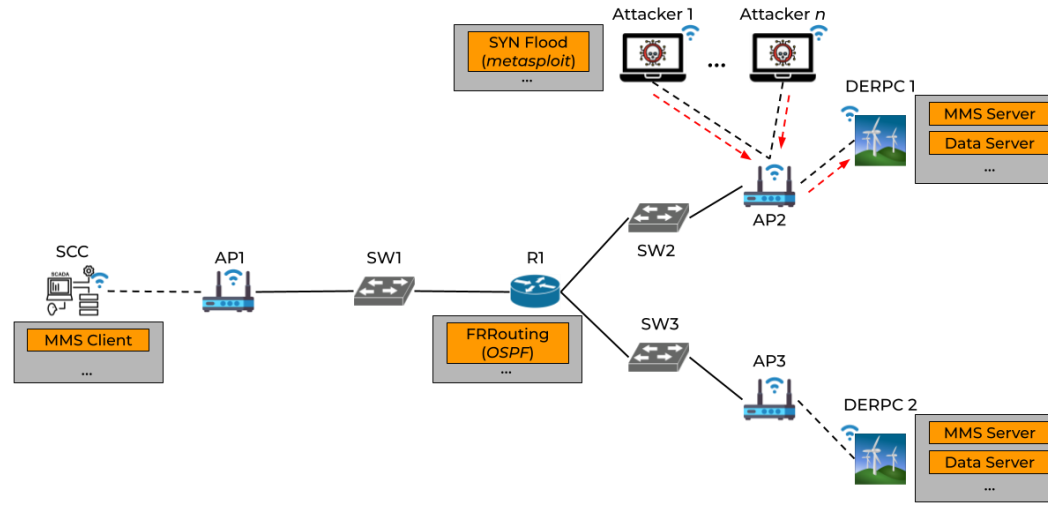


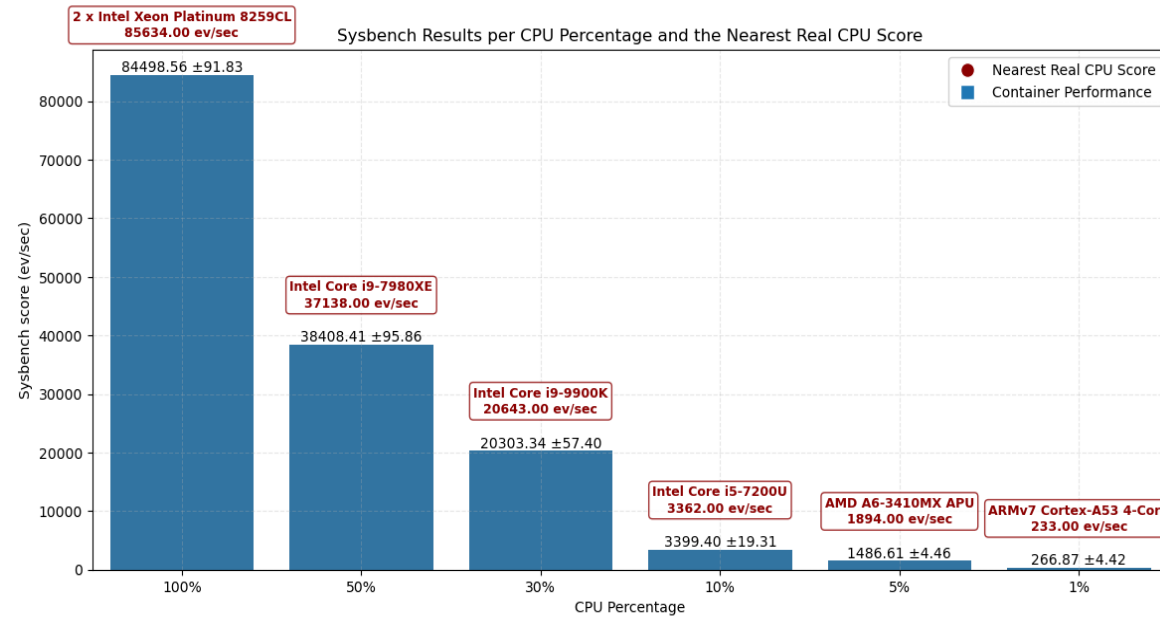


- IEC 61850 / MMS (Manufacturing Message Specification)
- DSO Controller – DER Plant Controller (CCI) communications





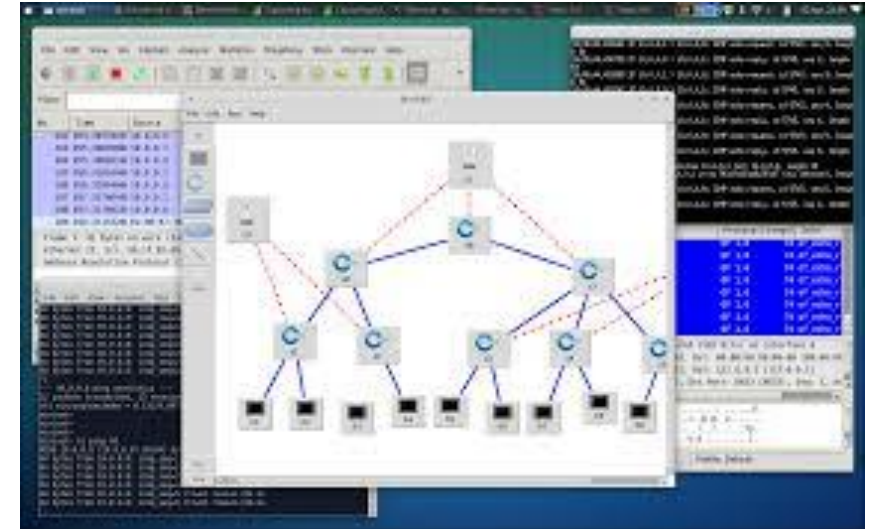


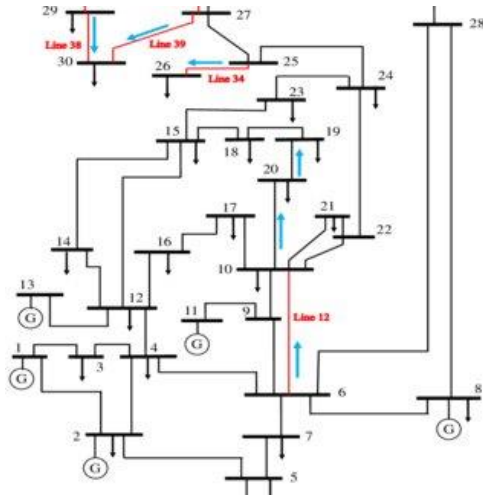


COSIM's ability of emulating different hardware conditions.

Thanks to famous benchmarking utilities (e.g. sysbench) we can assess the truthfulness of such feature.







CS



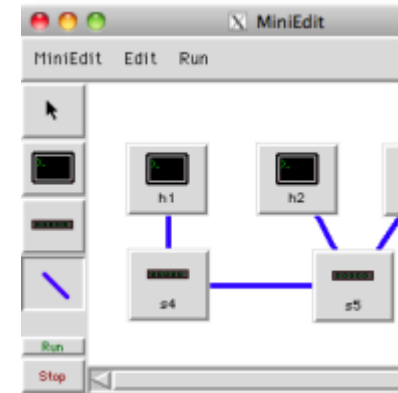
CSMS



CS

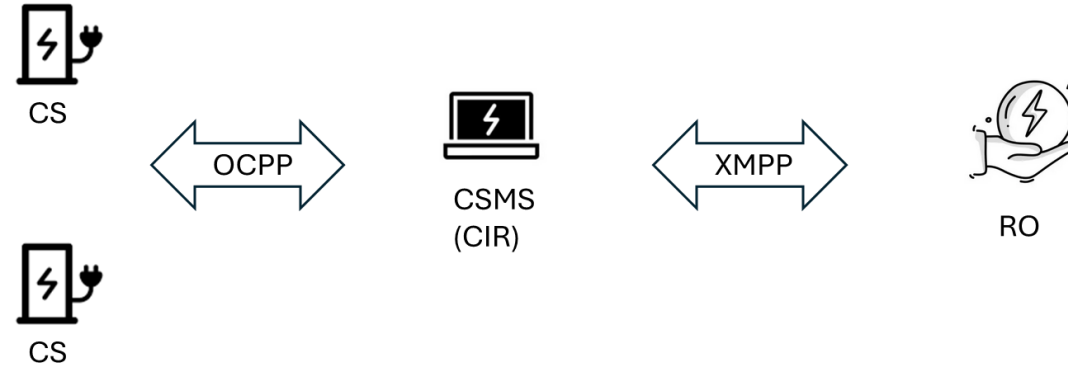


**MATLAB**



**Mininet**

- CS–CSMS simulation
- Assessment of cyber impacts on the grid
- Extension to OCPP 2.0.1 and V2G



- From a flexibility management perspective, EV charging infrastructures are considered key elements of the power system.
  - The architecture will be extended to include **remote operators** capable of controlling grid power absorption and, in the future, power injection through V2G.
  - In this configuration, the CSMS also implements **CIR (Charging Infrastructure Controller)** functionalities in accordance with CEI PAS 57-127.
  - Communication between system components is based on the XMPP protocol.



- Cybersecurity twin as a key enabling tool
  - The digitalization of power systems requires advanced tools for cybersecurity analysis and for assessing the impact of anomalies on energy infrastructures
- Full ICT–Power integration
  - Cybersecurity twin environments, accurately reproducing both electrical components and ICT infrastructures and their interactions, enable a realistic representation of cyber-physical contexts
- Analysis of complex scenarios and Support for resilience and future planning
  - Cybersecurity twins are a key enabler for assessing future energy-transition scenarios, allowing the analysis of tightly coupled ICT–electrical phenomena in a controlled and reproducible environment
- Extension toward large-scale heterogeneous co-simulation

Thank you for the attention

*Roberta Terruggia*  
*[roberta.terruggia@rse-web.it](mailto:roberta.terruggia@rse-web.it)*

