OPAL-RT and SCALABLE Network Technologies present a state-of-the-art co-simulation testbed for power system and cybersecurity professionals performing in-depth studies into the impact of communication systems latency and failures and cyberattacks on the grid.

The testbed combines two well-recognized COTS software tools fully integrated for real-time Cyber Physical Simulation (CPS):

- HYPERSIM® for Power System simulation
- EXata CPS for communication network and cyberattack simulation

Both software run on the same OPAL-RT real-time simulator and connect to each other virtually permitting the user to emulate communication connections from virtual devices within HYPERSIM and to route them via EXata CPS to external devices.

A major benefit of this testbed is the reduction of the overall communication latency when supporting time-critical applications involving protocols such as IEC 61850 GOOSE and IEEE C37.118.
OPAL-RT is the world leader in the development of PC/FPGA Based Real-Time Digital Simulator, Hardware-In-the-Loop (HIL) testing equipment and Rapid Control Prototyping (RCP) systems to design, test and optimize control and protection systems used in power grids, power electronics, motor drives, automotive industry, trains, aircraft and various industries, as well as R&D centers and universities.

### Features

#### Standard Packages & Features

- **Developer**
  - Design mode
  - Visualize mode
  - Analyser for statistical analysis

- **Cyber (see Cyberattack/defense list)**

- **Wireless**
  - Packet sniffer interface

- **Multimedia and Enterprise**
  - Scenario Player

#### Optional Libraries

- **Advanced wireless**
- **Cellular**
- **Federation interfaces**
- **LTE**
- **Sensor networks**
- **UMTS networks**
- **Urban propagation**

### Available Cyberattack Types

- **Denial of Service (DoS)**
- **Man-in-the-middle**
- **Packet modification**
- **Passive attacks**
  - Eavesdropping
  - Port scanning
  - SIGINT
- **Jamming**
- **Vulnerability exploitation**
  - Attacks to corrupt files and databases
  - Hacking attacks
- **Virus and Worm propagation**
- **Rootkit and botnet**
- **Backdoors/holes in the network perimeter**
- **Communications hijacking**
- **Coordinated and adaptive**

### Available Cyberdefense Models

- **Firewalls**
- **Intrusion Detection System (IDS)**
- **Anti-Virus System (AVS)**
- **Security Logs and Audit Trails**

### DOS Attack Configuration

#### Required Simulator Hardware

- **OPAL-RT Real-Time Simulators with:**
  - 8 or more processing cores
  - OPAL-RT-optimized Linux Operating System

#### Required Software

- **HYPERSIM 2019.2 or later**
- **EXata CPS v1.0 or later**

One or more communication protocols including:

- IEC 61850-8-1 GOOSE
- IEC 60870-5-104
- OPC-UA
- DNP3
- IEEE C37.118
- Modbus TCP