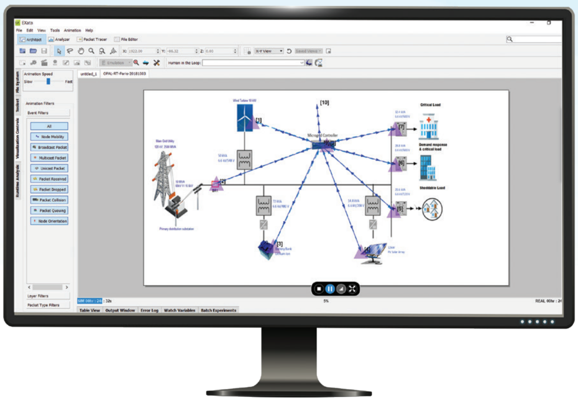
OPAL-RT TECHNOLOGIES

KEYSIGHT TECHNOLOGIES
Solutions Partner

Cyber-Physical Simulation Testbed for Power Systems



OPAL-RT and Keysight 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.

HYPERSIM RT-LAB EXata CPS

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

- **HYPERSIM®** or **RT-LAB** for Power System simulation
- **EXata CPS** for communication network and cyberattack simulation

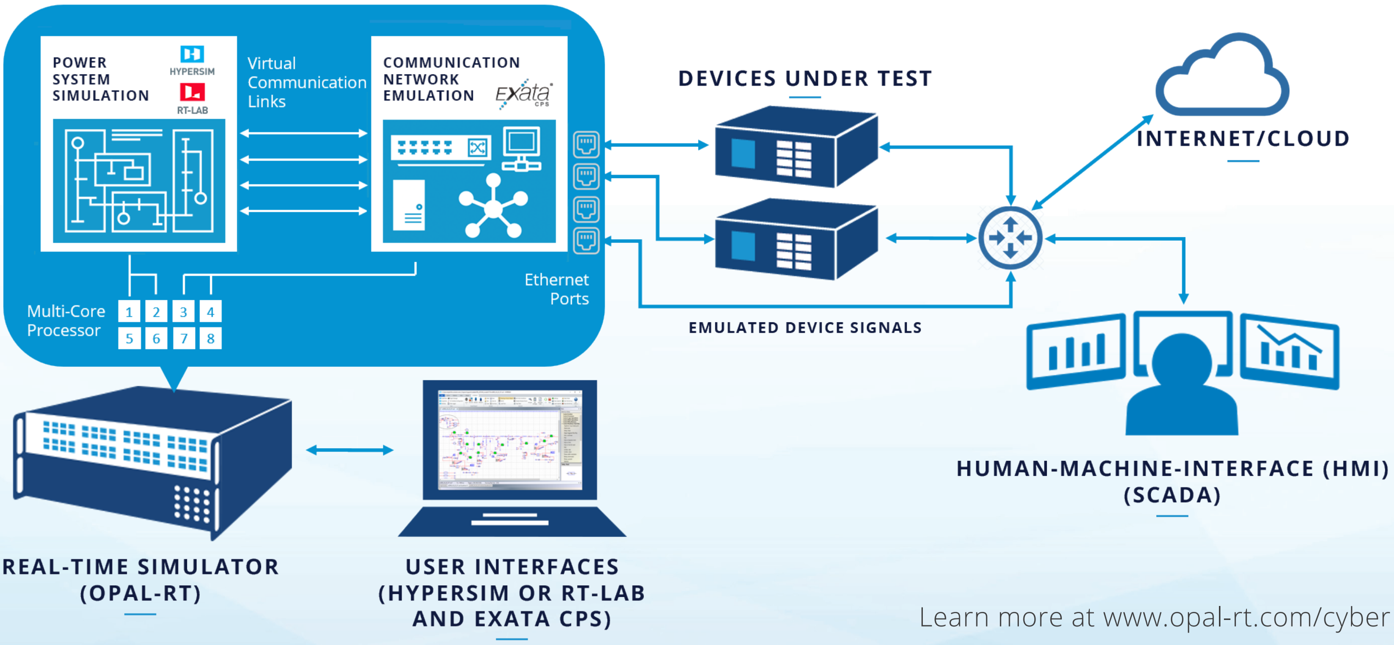
Both software run on the same OPAL-RT real-time simulator and connect to each other virtually permitting the user to emulate communication connections from virtual devices within HYPERSIM and to route them via EXata CPS to external devices.

Two major benefits of this testbed are (1) the reduction of the overall communication latency when supporting time-critical applications involving protocols such as IEC 61850 GOOSE and (2) an enhanced user-experience with automation of several configuration processes.

Plug-and-play Cyber-Physical System (CPS) co-simulation on one platform

USA DoD-proven high-fidelity communication network and cyberattack emulation with low latency

Simple graphical configuration for connections between emulated devices, communication nodes and external devices



POWER SYSTEM SIMULATION

HYPERSIM

RT-LAB

Virtual Communication Links

COMMUNICATION NETWORK EMULATION

EXata CPS

Multi-Core Processor

1 2 3 4
5 6 7 8

Ethernet Ports

DEVICES UNDER TEST

INTERNET/CLOUD

EMULATED DEVICE SIGNALS

HUMAN-MACHINE-INTERFACE (HMI) (SCADA)

REAL-TIME SIMULATOR (OPAL-RT)

USER INTERFACES (HYPERSIM OR RT-LAB AND EXATA CPS)

Learn more at www.opal-rt.com/cyber

EXata CPS 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

5G

Advanced wireless

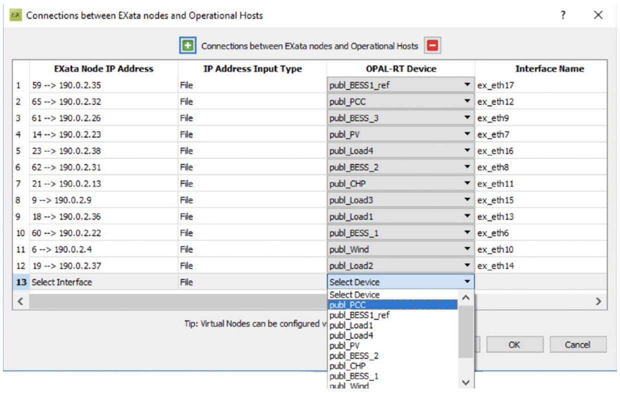
Cellular

Federation interfaces

LTE

Sensor networks

UMTS networks



Connections between EXata nodes and Operational Hosts

Connections between EXata nodes and Operational Hosts

	EXata Node IP Address	IP Address Input Type	OPAL-RT Device	Interface Name
1	59 --> 190.0.2.35	File	publ_BESS1_ref	ex_eth17
2	65 --> 190.0.2.32	File	publ_PCC	ex_eth12
3	61 --> 190.0.2.26	File	publ_BESS_3	ex_eth9
4	14 --> 190.0.2.23	File	publ_PV	ex_eth7
5	23 --> 190.0.2.38	File	publ_Load4	ex_eth16
6	62 --> 190.0.2.31	File	publ_BESS_2	ex_eth8
7	21 --> 190.0.2.13	File	publ_CHP	ex_eth11
8	9 --> 190.0.2.9	File	publ_Load3	ex_eth15
9	18 --> 190.0.2.36	File	publ_Load1	ex_eth13
10	60 --> 190.0.2.22	File	publ_BESS_1	ex_eth6
11	6 --> 190.0.2.4	File	publ_Wind	ex_eth10
12	19 --> 190.0.2.37	File	publ_Load2	ex_eth14
13	Select Interface	File	Select Device	

EXata CPS to HYPERSIM device mapping interface

Available Cyberattack Types

Denial of Service (DoS)

Man-in-the-middle

Packet modification

Passive attacks
- Eavesdropping
- Port scanning
- Network 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

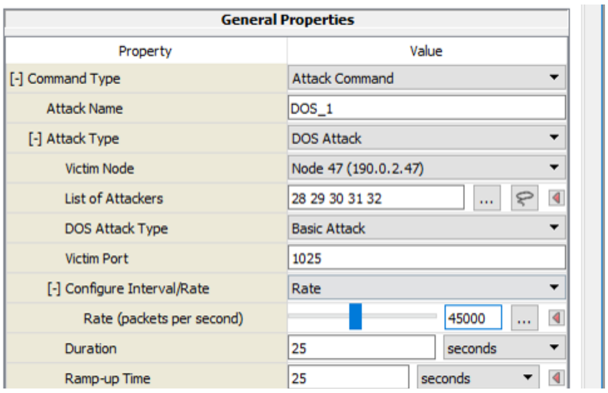
Available Cyberdefense Models

Firewalls

Intrusion Detection System (IDS)

Anti-Virus System (AVS)

Security Logs and Audit Trails



General Properties

Property	Value
[-] Command Type	Attack Command
Attack Name	DOS_1
[-] Attack Type	DOS Attack
Victim Node	Node 47 (190.0.2.47)
List of Attackers	28 29 30 31 32
DOS Attack Type	Basic Attack
Victim Port	1025
[-] Configure Interval/Rate	Rate
Rate (packets per second)	45000
Duration	25 seconds
Ramp-up Time	25 seconds

DOS Attack Configuration

OPAL-RT Requirements

Required Simulator Hardware

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

OP4610XG

OP5033XG

OP5707XG

Required Software

HYPERSIM 2021.3 or later

RT-LAB 2021.3 or later

EXata CPS v1.1 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

ABOUT OPAL-RT TECHNOLOGIES

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.

OPAL-RT TECHNOLOGIES

opal-rt.com/cyber