



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.

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.



KEYSIGHT

Solutions Partner





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





# **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

					1
	EXata Node IP Address	IP Address Input Type	OPAL-RT Device		Interface Name
	59> 190.0.2.35	File	publ_BESS1_ref	•	ex_eth17
	65> 190.0.2.32	File	publ_PCC	•	ex_eth12
	61> 190.0.2.26	File	publ_BESS_3	•	ex_eth9
	14> 190.0.2.23	File	publ_PV	-	ex_eth7
	23> 190.0.2.38	File	publ_Load4	•	ex_eth16
	62> 190.0.2.31	File	publ_BESS_2	•	ex_eth8
	21> 190.0.2.13	File	publ_CHP	•	ex_eth11
	9> 190.0.2.9	File	publ_Load3	-	ex_eth15
	18> 190.0.2.36	File	publ_Load1	•	ex_eth13
0	60> 190.0.2.22	File	publ_BESS_1	-	ex_eth6
1	6> 190.0.2.4	File	publ_Wind	•	ex_eth10
2	19> 190.0.2.37	File	publ_Load2	•	ex_eth14
3	Select Interface	File	Select Device	•	
:			Select Device	^	
		Tip: Virtual Nodes can be configured v	publ_BESS1_ref publ_Load1 publ_Load4 publ_PV publ_BESS_2 publ_CHP		] OK Cancel

EXata CPS to HYPERSIM device mapping interface

# **OPAL-RT Requirements**

## **Required Simulator Hardware**

#### **OPAL-RT Real-Time Simulators with:**

- 6 or more processing cores
- OPAL-RT-optimized Linux Operating System



# **Available Cyberattack Types**

Denial of Service (DoS)

Man-in-the-middle

Packet modification

#### Passive attack: network and port scanning Vulnerability exploitation

- Attacks to corrupt files and databases
- Hacking attacks

Virus and Worm propagation

#### Rootkit and botnet

Coordinated and adaptive

**Available Cyberdefense Models** 

**Firewalls** 

## Host Model

Modeling the operational characteristics

Host profile with resource, processes, vulnerability modeling

User profile with modeling pattern of communication

	General Properties		
Property	Value		
[-] Command Type	Attack Command		
Attack Name	MOPD_Multiply		
[-] Attack Type	Modify Packets	~	
Attacker Node	8		
[-] Layer Type	MAC	~	
[-] MAC Layer Filter	Yes		
Source MAC Address	ANY		
Destination MAC Address	01:0C:CD:01:0D:19		]
Ethernet Type	ANY		
[-] MODP Attack Type	Flow Modification		
Number of Flow Modifications	0		
[-] MODP Attack Type	Data Modification		
[-] Number of Data Modifications	1		
[-] Data Modification Type [0]	Multiply	~	1
[-] Multiply Type [0]	Value		
Value Type [0]	16 Bit Unsigned Integer	~	
Start Byte [0]	114		
Multiply Value [0]	2		

Packet Modification Attack Configuration

## **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 • DNP3

• IEC 60870-5-104 • OPC-UA

• 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.com/cyber