

# Cyber Physical System Security HYPERSIM and EXata - RT Simulator

CR-DES Project

D 3.3: power point slides on modeling and measuring  
cyber-physical resilience in laboratory

University of Vaasa

Assistance Prof: Mike Mekkanen

[mike.mekkanen@uva.fi](mailto:mike.mekkanen@uva.fi)

23.8.2021



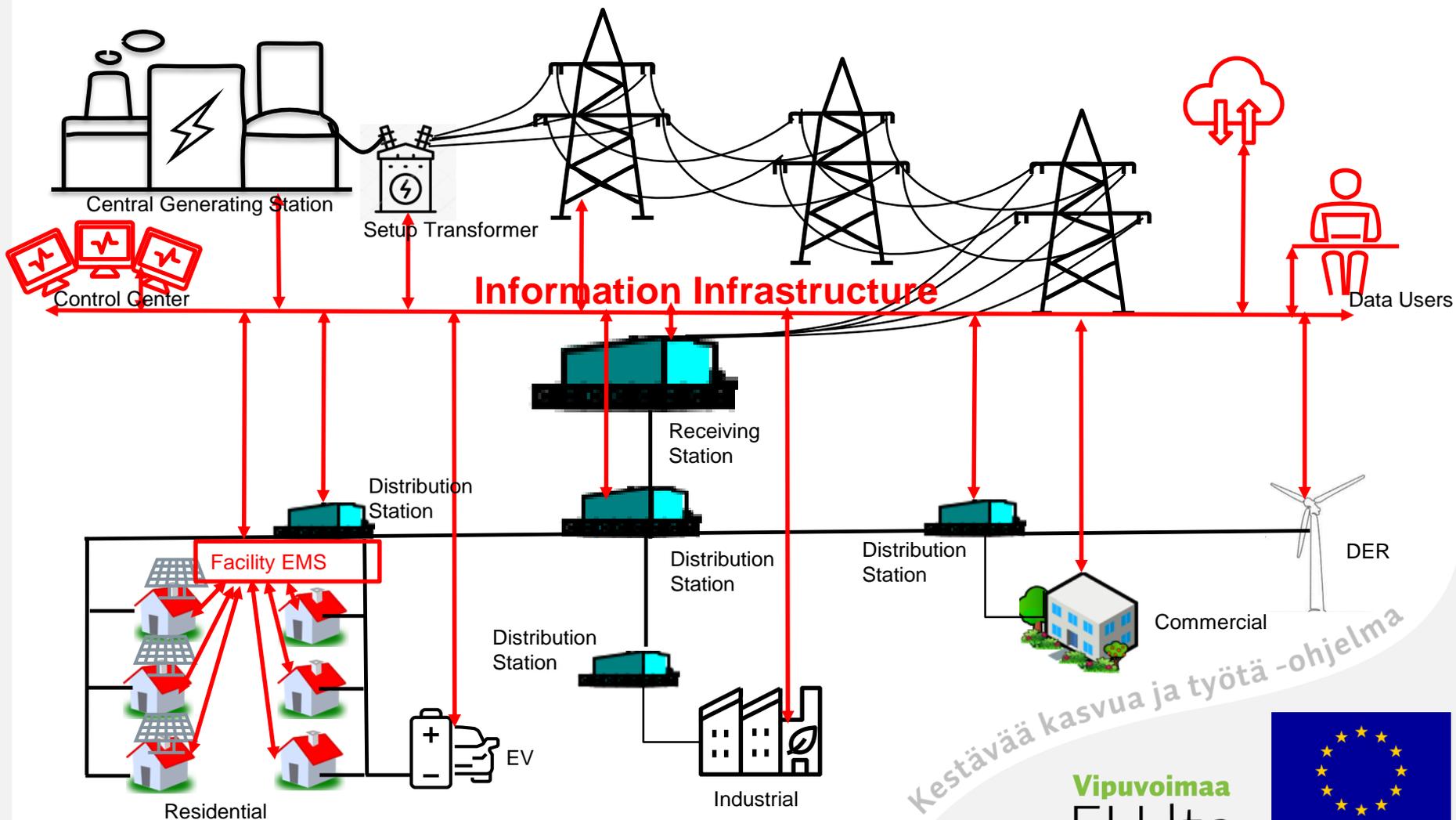
Vipuvoimaa  
EU:lta  
2014–2020



Euroopan unioni  
Euroopan aluekehitysrahasto

Kestävä kasvua ja työtä -ohjelma

# Digitalization (ICT) for the existing energy system



*Kestävää kasvua ja työtä -ohjelma*

# Developing Countermeasures and Validation Them

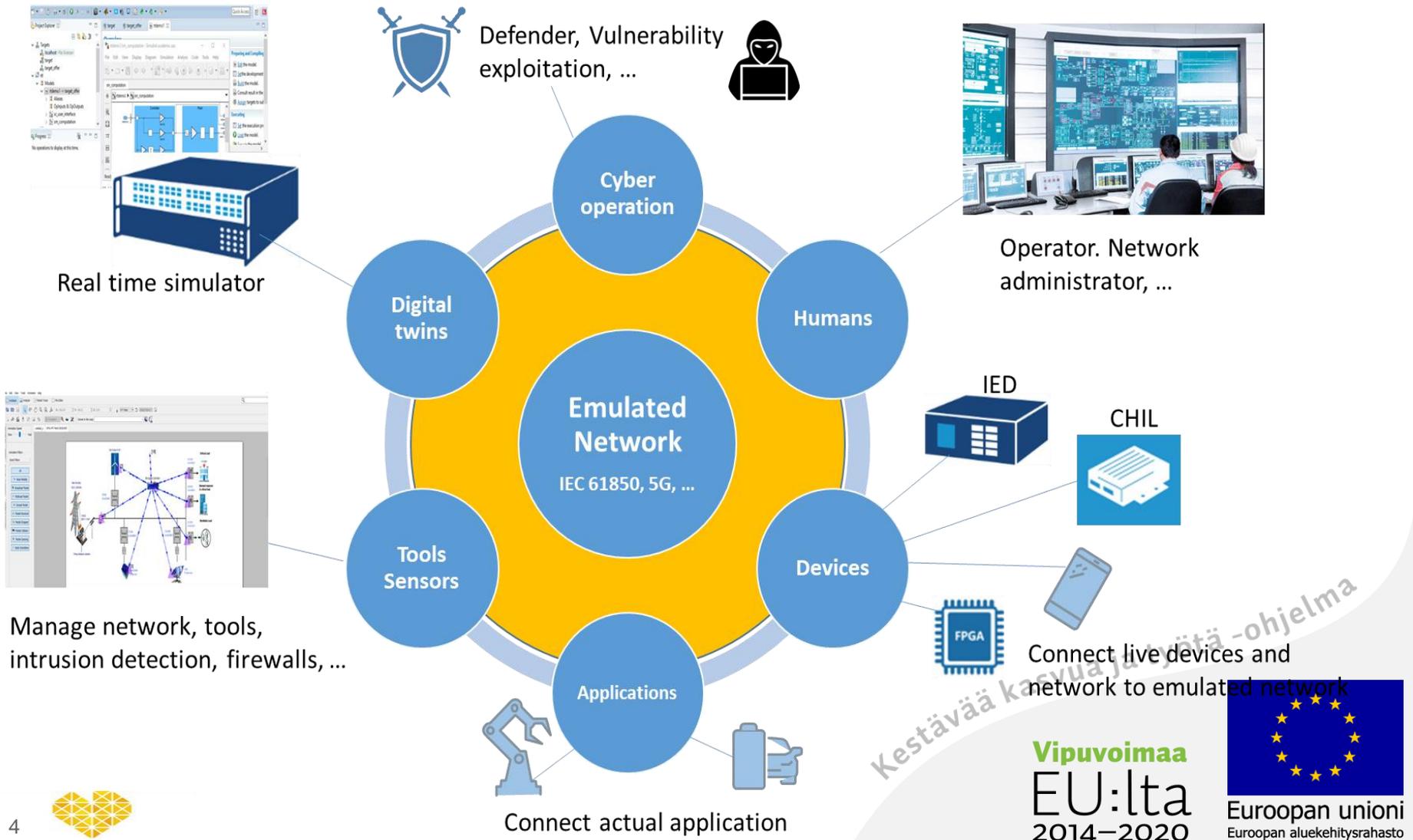
What type of development and test platform can we use

- Need to address both communication as well as power system domains
- Need to be flexible to cover different network topologies as well as operating conditions
- Need to be user-friendly/efficient

*Kestävää kasvua ja työtä -ohjelma*

# CPS Platform- - RT Simulator

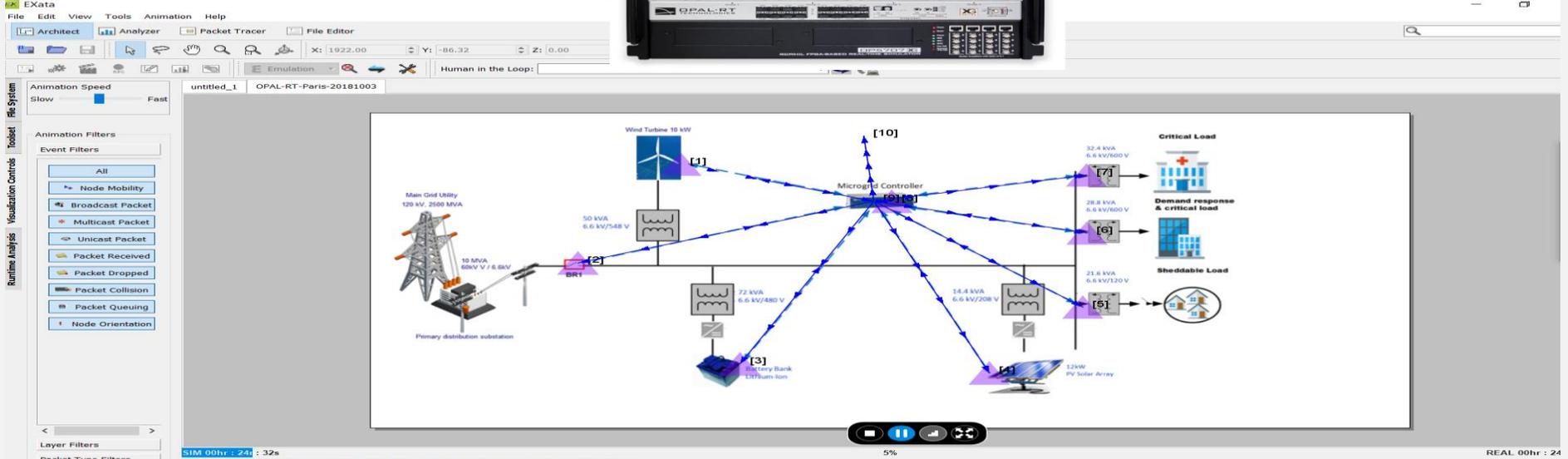
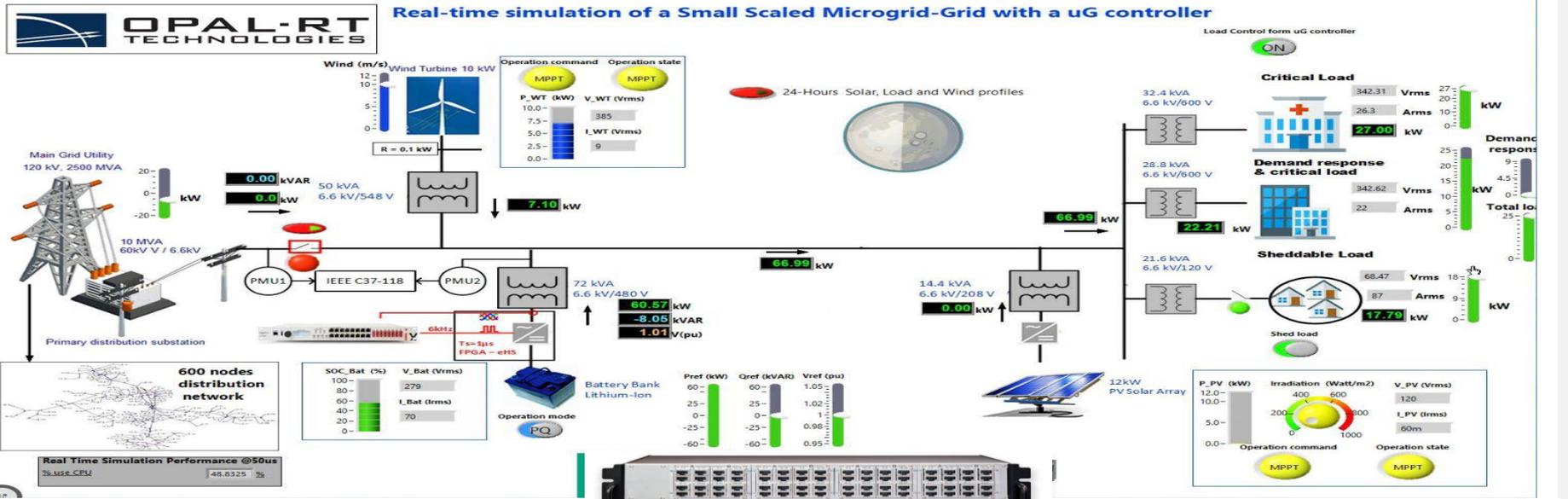
## Cybersecurity and Resilience of Digital Energy Systems (CR-DES)



Kestävää kasvua ja työtä -ohjelma

# CPS Platform - RT Simulator

## Cybersecurity and Resilience of Digital Energy Systems (CR-DES)



# CPS Platform - RT Simulator

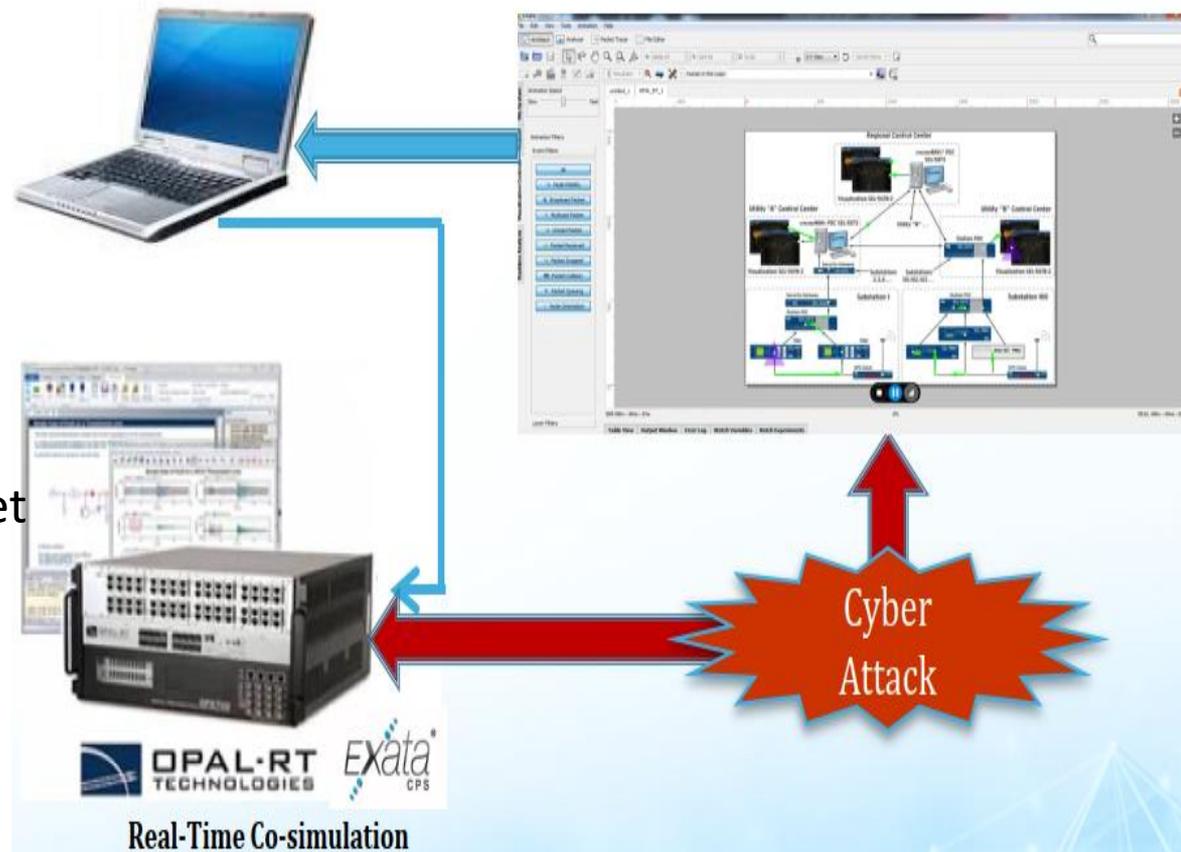
## Cybersecurity and Resilience of Digital Energy Systems (CR-DES)

### Host PC

- Scenario creation
- Interface Mapping
- Execution Control
- Cyber Attacks
- Animation
- Analysis / Results

### Real-Time Co-simulation Target

- Electromagnetic
- Electromechanical
- Mechanical
- Network
- Communications
- Cybersecurity

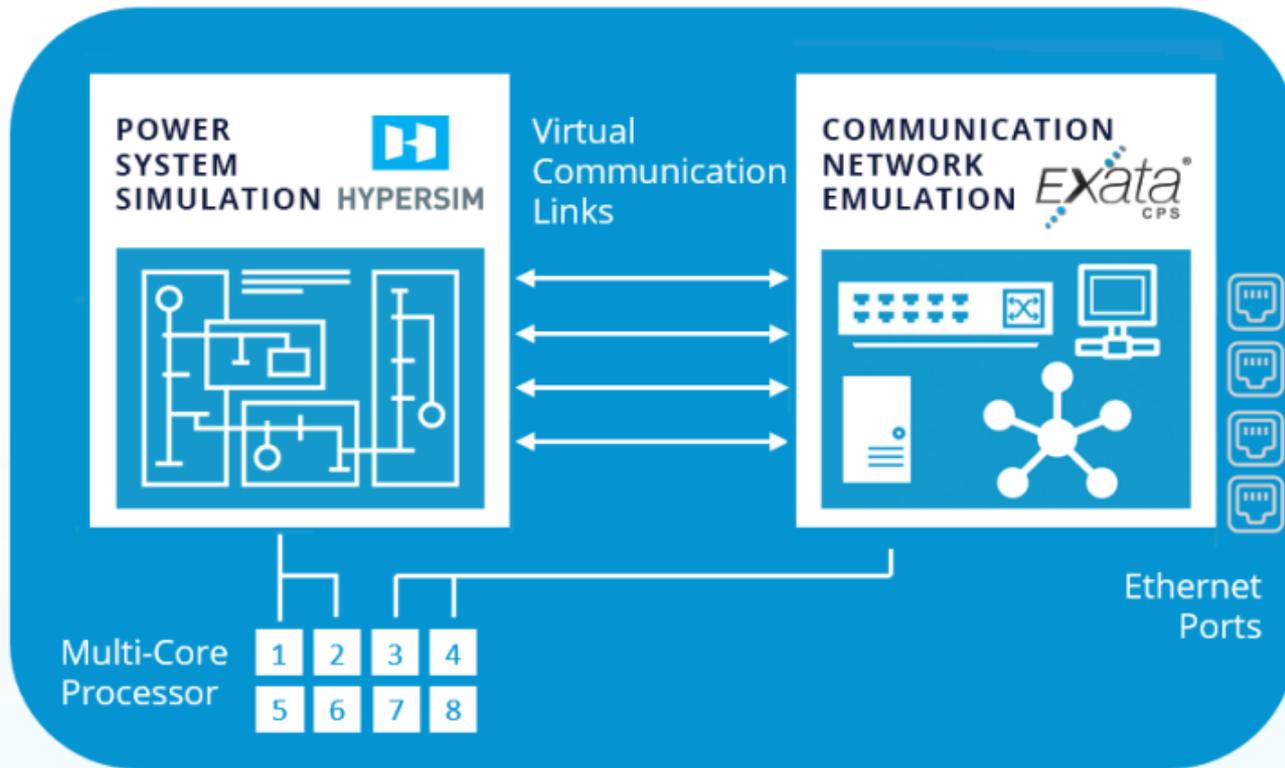


# CPS

## Cybersecurity and Resilience

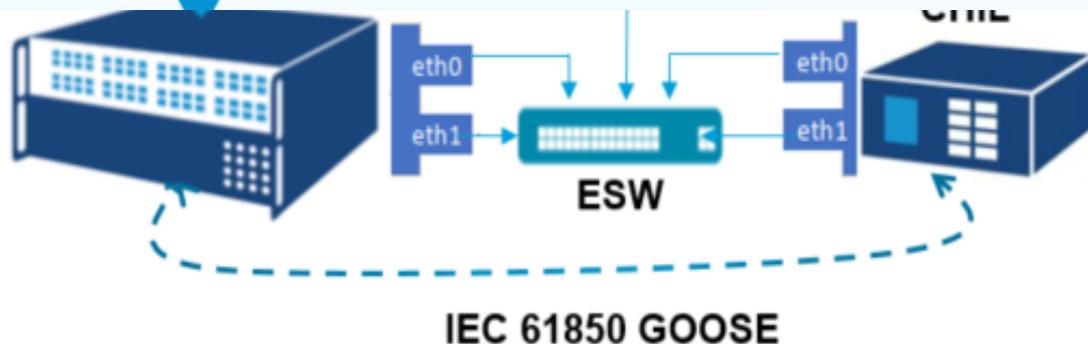
### Host PC

- Scenario creation
- Interface Mapping
- Execution Control
- Cyber Attacks
- Animation
- Analysis / Results



### Real-Time Co-simulation Target

- Electromagnetic
- Electromechanical
- Mechanical
- Network
- Communications
- Cybersecurity

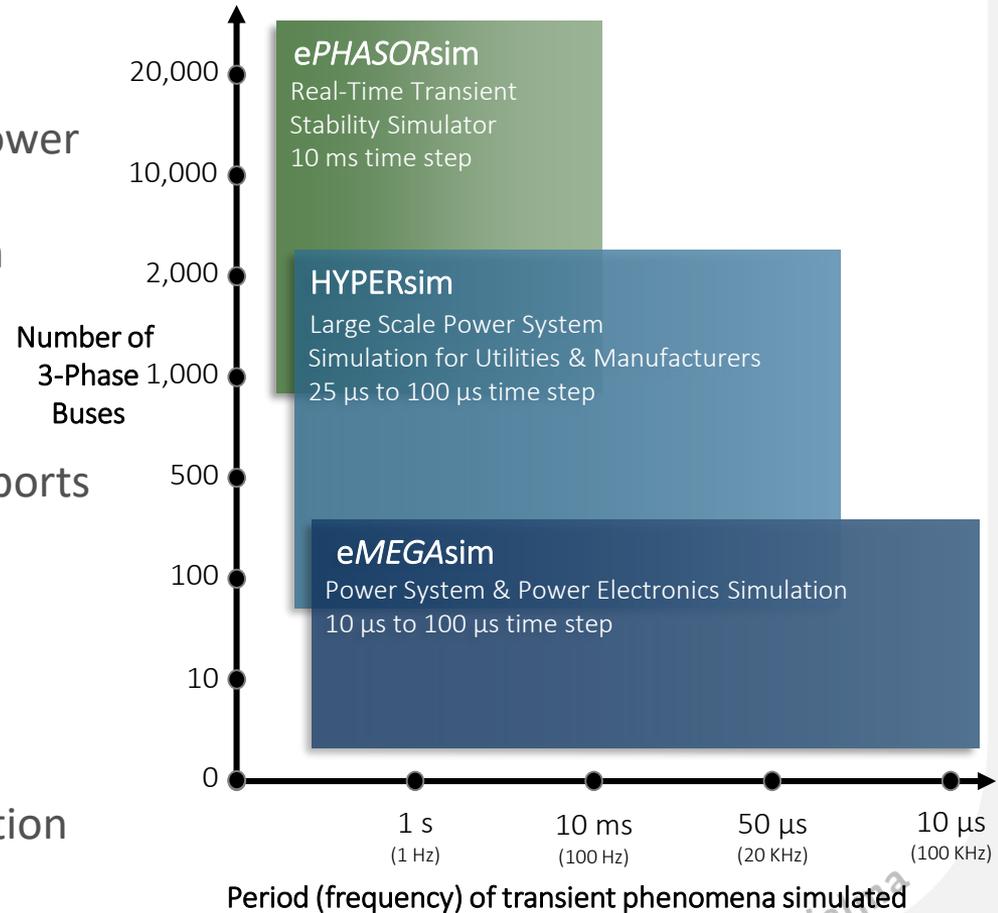


# HYPERSIM



## HYPERsim

- Windows based Detailed Large-Scale Power System software developed by Hydro-Québec (over 1000 3-phase buses) with more than 300 validated power system components and controllers
- **TestView:** Automated testing with (supports Python)
- **ScopeView:** Signal visualization, data analysis and monitoring
- **HyperView:** enables monitoring simulation performance in real-time



Kestävää kasvua ja työtä -ohjelma

# HYPERSIM



C:\Opal\_RT\_to\_delet\6bus\HVAC\_500kV\_6Bus\HVAC\_500kV\_6Bus.ecf - HYPERSIM

File Home Options View Design HYPERSIM

Save Save As... Copy Paste Undo Redo Delete Deselect All Invert Selection Point Zap Name Move Attribute Probe Draw Signal Draw Graphics Find

Orientation... New Breakout... Properties... Line Rectangle Arc Text Rounded Rect Ellipse Polygon Ellipse Quick Find Advanced Find Property Browser

HVAC\_500kV\_6Bus.ecf

Parts

Parts by Library

- Control Exciters
- Control Governors
- Control Logic Operations
- Control Math Operations
- Control Measurements
- Control Miscellaneous
- Control Nonlinear And Dela
- Control Protection Relays
- Control Sources
- Control Stabilizers
- Network FACTS and HVDC
- Network Filters
- Network Lines and Cables
- Network Loads
- Network Machines
- Network Measurements
- Network Renewable Energy
- Network RLC
- Network Sources
- Network Switches and Break
- Network Tools
- Network Transformers
- Network Voltage Source Co
- Signal Routing
- Target Inputs and Outputs

This basic network demonstrates a simple case of wave propagation in an AC transmission system.

A 1-phase-to-ground fault is applied at one end of the transmission line.  
The resulting shockwave propagates to the other end.

A protection scheme is present to clear the fault.

Protection scheme:  
The fault occurs on phase A at 0.028 s.  
The protection system isolates the line by opening line breakers at 0.1 s.  
The fault is cleared and the line is brought back to service at 0.2 s.

Voltage Levels

- 13.8kV
- 500kV
- 69kV

Log window

```
[2021-08-20 12:30:44.157] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.o97\Windows\HYGui\data\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.o97\Windows\HYGui\data\Hypersim.site]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hyconfig\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\Users\yp_mmecca\HYPERMIM\Hypersim.res]
Starting server RPC [0x3ffff000]...
[2021-08-20 12:30:44.868] Starting session...
[2021-08-20 12:30:44.873] HyAcqSpooler running outside Hypersim...
[2021-08-20 12:30:44.873] Starting session... done
[2021-08-20 12:30:46.383] Code (2020.3.0.o97) and engine (2020.3.0.o97) versions match. Continue...
```

HypConsole HVAC\_500kV\_6Bus.ecf [localhost:1] HVAC\_500kV\_6Bus.simout [localhost:1]

# HYPERSIM



The screenshot displays the HYPER SIM software interface. The main window is titled "Simulation Settings - HVAC\_500kV\_6Bus.ecf". The dialog box has three tabs: "General", "Target", and "Advanced". The "Target" tab is selected, showing the following configuration:

- Target Configuration:**
  - Target: localhost
  - Simulation mode: Offline (RTA)
  - Architecture: Windows
- Simulation:**
  - Time step: 50e-6 s
  - Performance factor: 1
  - Code directory: C:\Users\yp\_mmekka\HYPERSIM\code\yp\_mmekka\c96672c96ebc5acfea30e75335df68d59
  - Enable simulation logging
  - Perform load flow and set initial conditions at simulation start
- Nonlinear elements iterative method:**
  - Activate iterative method
  - Maximum iterations: 5
  - Apply to all nonlinear elements

At the bottom of the dialog box are buttons for "Ok", "Apply", "Revert", and "Cancel".

Green arrows in the image point from the "Target icon" label to the target dropdown menu and from the "Simulation settings" label to the "Simulation" section of the dialog box.

Target icon

Simulation settings

Simulation Settings - HVAC\_500kV\_6Bus.ecf

General Target Advanced

Target Configuration

Target

localhost

Simulation mode

Offline (RTA)

Architecture

Windows

Simulation

Time step

50e-6

s

Performance factor

1

Code directory

C:\Users\yp\_mmekka\HYPERSIM\code\yp\_mmekka\c96672c96ebc5acfea30e75335df68d59

Enable simulation logging

Perform load flow and set initial conditions at simulation start

Nonlinear elements iterative method

Activate iterative method

Maximum iterations

5

Apply to all nonlinear elements

Tasks Manager

Ok

Apply

Revert

Cancel

ni

to

13.02  
20.8.2021

# HYPERSIM



HYPER SIM

Start simulation button

This basic network demonstrates a simple case of wave propagation in an AC transmission system.

A 1-phase-to-ground fault is applied at one end of the transmission line.  
The resulting shockwave propagates to the other end.

A protection scheme is present to clear the fault.

Protection scheme:  
The fault occurs on phase A at 0.028 s.  
The protection system isolates the line by opening line breakers at 0.1 s.  
The fault is cleared and the line is brought back to service at 0.2 s.

Parts

- Control Exciters
- Control Governors
- Control Logic Operations
- Control Math Operations
- Control Measurements
- Control Miscellaneous
- Control Protection Relays
- Control Sources
- Control Stabilizers
- Network FACTS and HVDC
- Network Filters
- Network Lines and Cables
- Network Loads
- Network Machines
- Network Measurements
- Network Renewable Energy
- Network RLC
- Network Sources
- Network Switches and Break
- Network Tools
- Network Transformers
- Network Voltage Source Co
- Signal Routing
- Target Inputs and Outputs

Parts by Library

Voltage Levels

- 11\_kV
- 500kV
- 68kV

HVAC\_500kV\_6Bus.ecf Ts = 50.0 μs Target = [localhost]

```
[2021-08-20 12:30:44.157] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.097\Windows\HyGui\data\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.097\Windows\HyGui\data\Hypersim.site]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hyconfig\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\Users\yp_mme\kka\HYPERSIM\Hypersim.res]
Starting server RPC [0x3ffff000]...
[2021-08-20 12:30:44.868] Starting session...
[2021-08-20 12:30:44.873] HyAcqSpooler running outside Hypersim...
[2021-08-20 12:30:44.873] Starting session... done
[2021-08-20 12:30:46.383] Code (2020.3.0.097) and engine (2020.3.0.097) versions match. Continue...
```

HypConsole HVAC\_500kV\_6Bus.ecf [localhost:1] HVAC\_500kV\_6Bus.simout [localhost:1]

# HYPERSIM

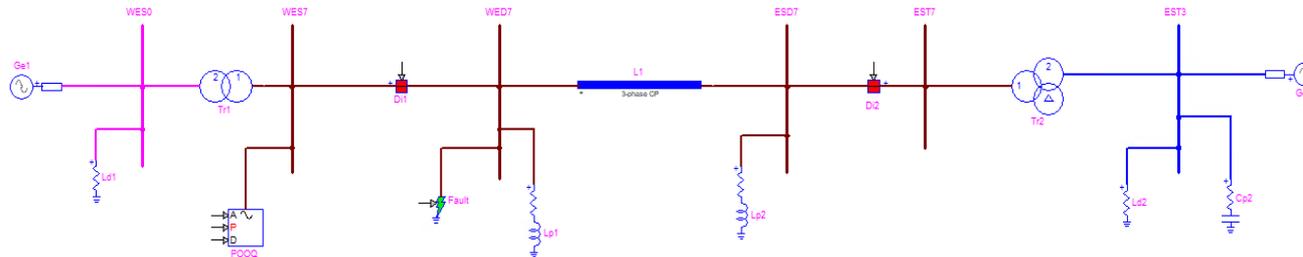


Tool icons

This basic network demonstrates a simple case of wave propagation in an AC transmission system.

A 1-phase-to-ground fault is applied at one end of the transmission line.  
The resulting shockwave propagates to the other end.

A protection scheme is present to clear the fault.



**Protection scheme:**  
The fault occurs on phase A at 0.028 s.  
The protection system isolates the line by opening line breakers at 0.1 s.  
The fault is cleared and the line is brought back to service at 0.2 s.

**Voltage Levels**

- 11.8kV
- 500kV
- 58kV

- Parts
- Parts by Library
- Control Exciters
  - Control Governors
  - Control Logic Operations
  - Control Math Operations
  - Control Measurements
  - Control Miscellaneous
  - Control Protection Relays
  - Control Protection Relays
  - Control Sources
  - Control Stabilizers
  - Network FACTS and HVDC
  - Network Filters
  - Network Lines and Cables
  - Network Loads
  - Network Machines
  - Network Measurements
  - Network Renewable Energy
  - Network RLC
  - Network Sources
  - Network Switches and Breakers
  - Network Tools
  - Network Transformers
  - Network Voltage Source Co
  - Signal Routing
  - Target Inputs and Outputs

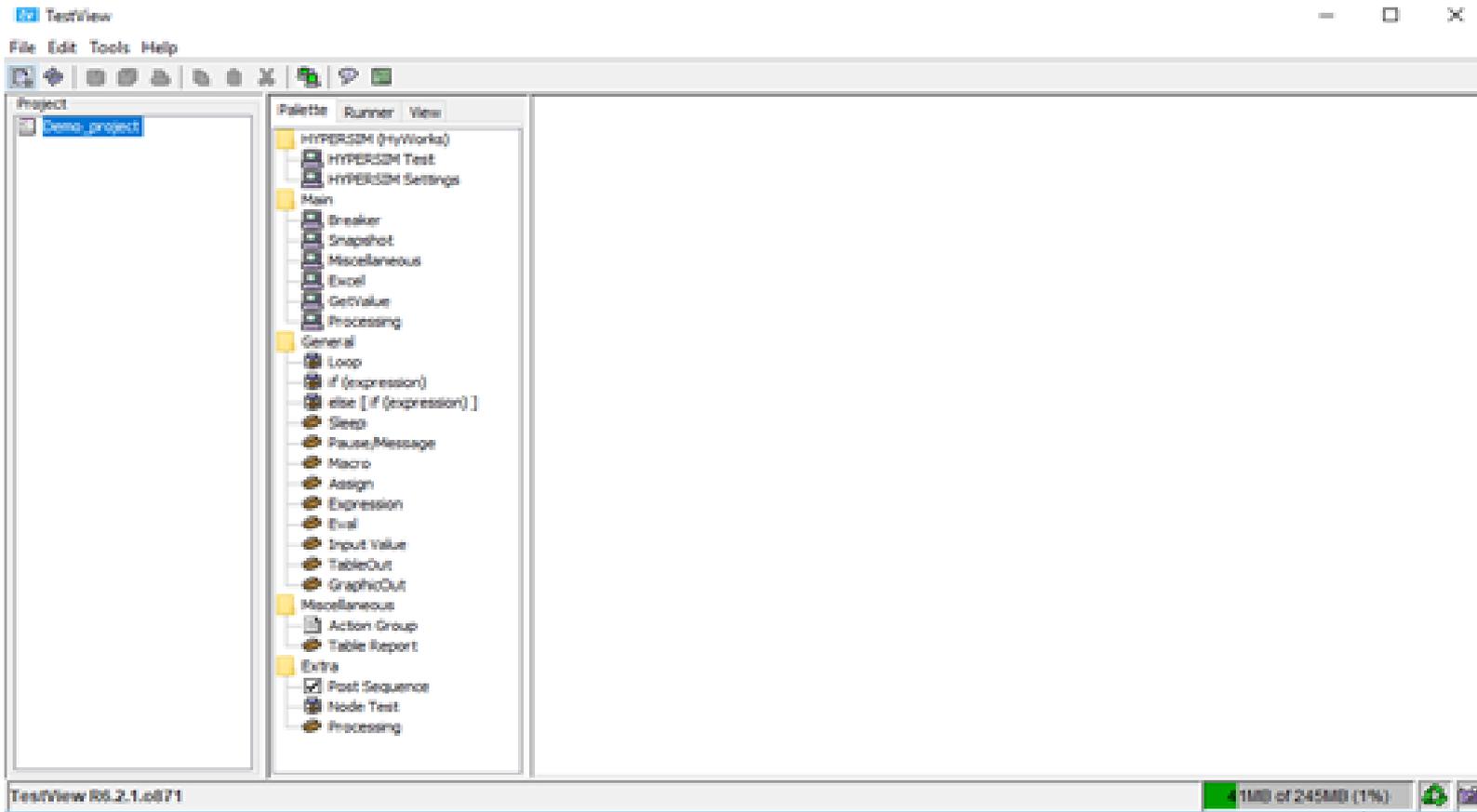
```
HVAC_500kV_6Bus.ecf Ts = 50.0 μs Target = [localhost]
[2021-08-20 12:30:44.157] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.097\Windows\HyGui\data\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.097\Windows\HyGui\data\Hypersim.site]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hyconfig\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\Users\yp_mme\kka\HYPERSIM\Hypersim.res]
Starting server RPC [0x3ffff000]...
[2021-08-20 12:30:44.868] Starting session...
[2021-08-20 12:30:44.873] HyAcqSpooler running outside Hypersim...
[2021-08-20 12:30:44.873] Starting session... done
[2021-08-20 12:30:46.383] Code (2020.3.0.097) and engine (2020.3.0.097) versions match. Continue...
```

HypConsole HVAC\_500kV\_6Bus.ecf [localhost:1] HVAC\_500kV\_6Bus.simout [localhost:1]

# HYPERSIM



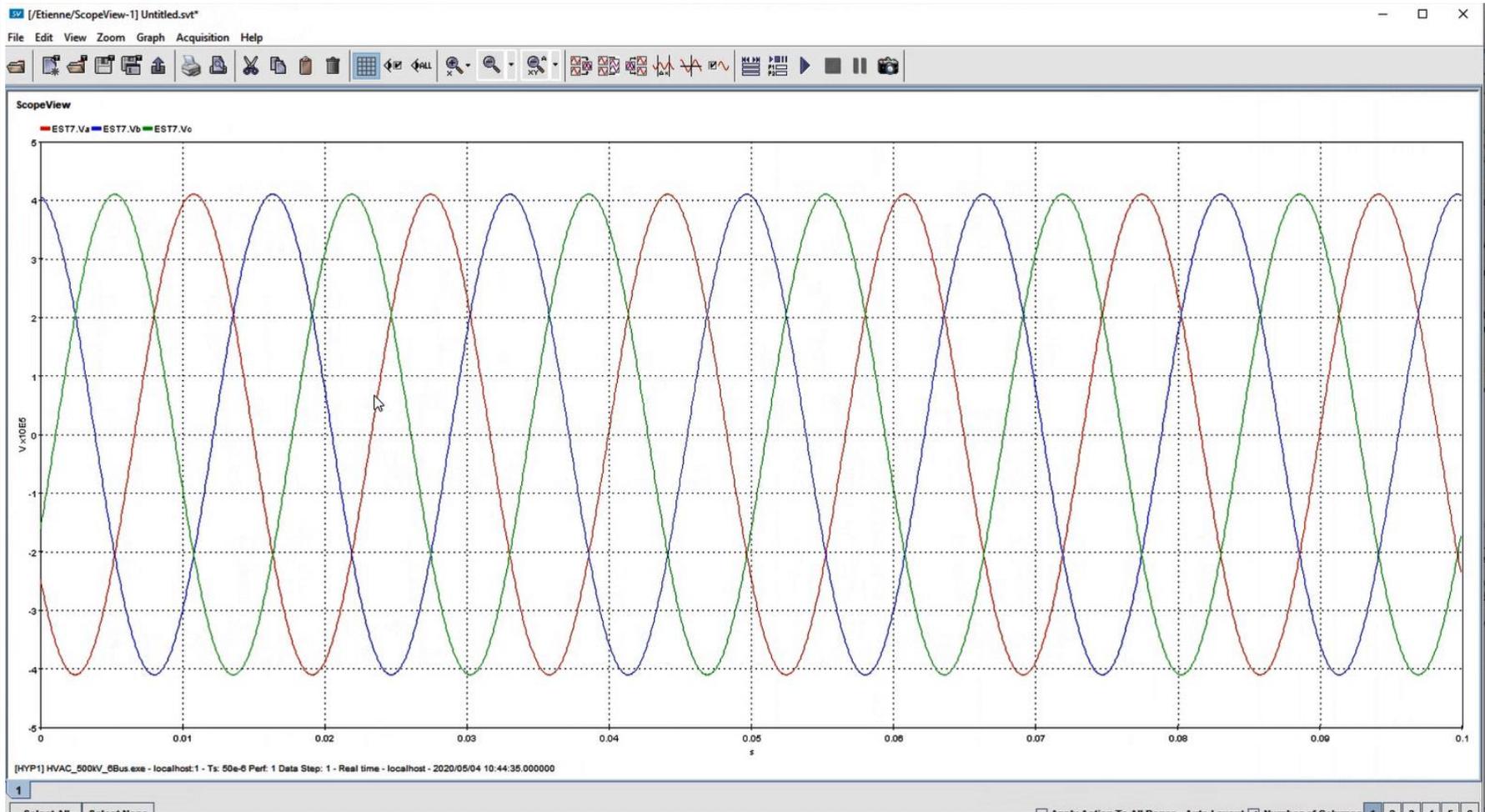
- **TestView:** Automated testing with (supports Python)



# HYPERSIM



- **ScopeView:** Signal visualization, data analysis and monitoring



# HYPERSIM



## HYPERSIM

- **HyperView:** enables monitoring simulation performance in real-time

The screenshot displays the HyperView application window titled "HyperView - etienne@educ@opal102285 - UCM\_CONTROLLED\_RESISTOR.Exe". The interface includes a toolbar with a red circle '1' around a play button, and a menu bar with "Real-Time" selected and a red circle '2' around the "SysMac" option. On the left, a "Hardware for localhost" panel lists seven components, with the first one "1 Simulating" and others "2 Free" through "7 Free". The main area is titled "CPU's Monitoring" and features a table with columns: Select, ID, Enabled, Exec, Exec Max, Remain, Remain Min, Comm, Comm Max, Sim, Sim Max, Acq/Plat Max, Last in Spec, and Stretched Step. The table contains one row of data: a checked checkbox, ID 1, Enabled status, Exec 0.59, Exec Max 667.75, Remain 0.0, Remain Min 0.0, Comm 0.0, Comm Max 34.49, Sim 0.88, Sim Max 669.52, Acq/Plat Max 326.95, Last in Spec 11175707, and Stretched Step 0. The bottom status bar shows "SIM" with a green dot, "RT MON" with a red dot, and "76MB of 245MB".

# HYPERSIM



C:\Opal\_RT\_to\_delete\6bus\HVAC\_500kV\_6Bus\HVAC\_500kV\_6Bus.ecf - HYPERSIM

File Home Options View Design HYPERSIM

HyperView Target Manager Sequences  
ScopeView Preferences  
TestView EXata-CPS

Save Save As Topology Analysis Report Netlist Load Flow  
Set Initial Conditions Disable Breakers/Faults Task Manager  
Analyze Map Tasks Generate Code  
Start Stop Settings Start Monitoring Stop Monitoring Snapshot  
User Manual Help

EXata CPS icon

HVAC\_500kV\_6Bus.ecf

Parts

Parts by Library

- Control Exciters
- Control Governors
- Control Logic Operations
- Control Math Operations
- Control Measurements
- Control Miscellaneous
- Control Nonlinear And Dela
- Control Protection Relays
- Control Sources
- Control Stabilizers
- Network FACTS and HVDC
- Network Filters
- Network Lines and Cables
- Network Loads
- Network Machines
- Network Measurements
- Network Renewable Energy
- Network RLC
- Network Sources
- Network Switches and Brea
- Network Tools
- Network Transformers
- Network Voltage Source Co
- Signal Routing
- Target Inputs and Outputs

This basic network demonstrates a simple case of wave propagation in an AC transmission system.

A 1-phase-to-ground fault is applied at one end of the transmission line.  
The resulting shockwave propagates to the other end.

A protection scheme is present to clear the fault.

Protection scheme:  
The fault occurs on phase A at 0.028 s.  
The protection system isolates the line by opening line breakers at 0.1 s.  
The fault is cleared and the line is brought back to service at 0.2 s.

Voltage Levels

- 13.8kV
- 100kV
- 98kV

HVAC\_500kV\_6Bus.ecf Ts = 50.0 μs Target = [localhost]

```
[2021-08-20 12:30:44.157] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.o97\Windows\HyGui\data\hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hypersim_2020.3.0.o97\Windows\HyGui\data\hypersim.site]
[2021-08-20 12:30:44.169] Load preferences file: [C:\OPAL-RT\HYPERSIM\hyconfig\Hypersim.res]
[2021-08-20 12:30:44.169] Load preferences file: [C:\Users\yp_mme\kka\HYPERSIM\Hypersim.res]
Starting server RPC [0x3fffc900]...
[2021-08-20 12:30:44.068] Starting session...
[2021-08-20 12:30:44.873] HyAcaSpooler running outside Hypersim...
[2021-08-20 12:30:44.873] Starting session... done
[2021-08-20 12:30:46.383] Code (2020.3.0.o97) and engine (2020.3.0.o97) versions match. Continue...
```

HypConsole HVAC\_500kV\_6Bus.ecf [localhost:1] HVAC\_500kV\_6Busimout [localhost:1]



## EXata



- Windows based high-fidelity network emulator/simulation, which simulates the network communications of electrical grids, attacks, defenders etc. EXata CPS is integrated with OPAL-RT's HYPERSIM real-time simulator on the same hardware to offer a complete real-time cyber-physical solution for the development, testing, and assessment of electrical grids, support more than 1000 of devices.
- Develop emulation/simulation models for new networking technologies. Design new communications protocol models using the OSI-style
- Connect real networks, applications, and devices with EXata emulated network
- Analyze and manage EXata virtual networks with popular, industry-standard, tools
- Develop, test and evaluate, and train users on cyber warfare and network security technologies.

Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa  
EU:lta  
2014–2020



Euroopan unioni  
Euroopan aluekehitysrahasto



EXata



## Common Attack Vectors

- Backdoors and holes in network perimeter
- Exploitation of vulnerabilities in SCADA protocols
- Communications hijacking and man-in-the-middle attacks
- Database attacks
- Bogus input data to the controller introduced by compromised sensors and/or exploited network link between the controller and the sensors
- Manipulated and misleading output data to the actuators/reactors from the controller due to compromised network link between the controller and the actuators
- Attacks on timing and synchronization

*Kestävää kasvua ja työtä -ohjelma*



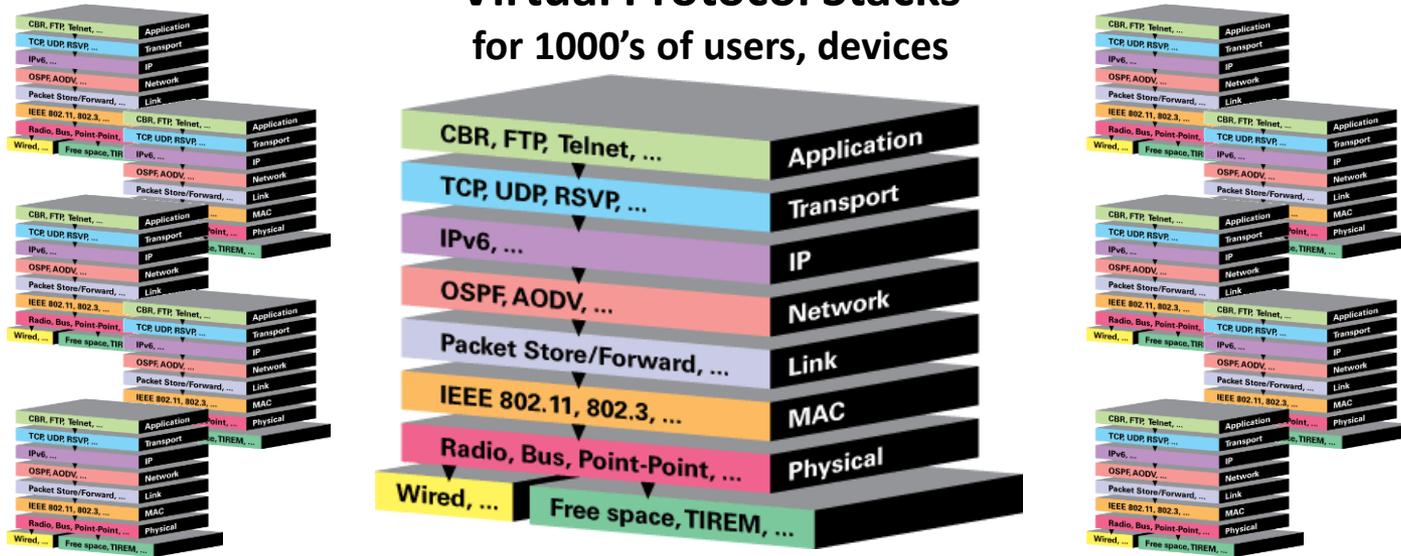
EXata



Command-Line

GUI: Design, Visualize, Analyze

### Virtual Protocol Stacks for 1000's of users, devices



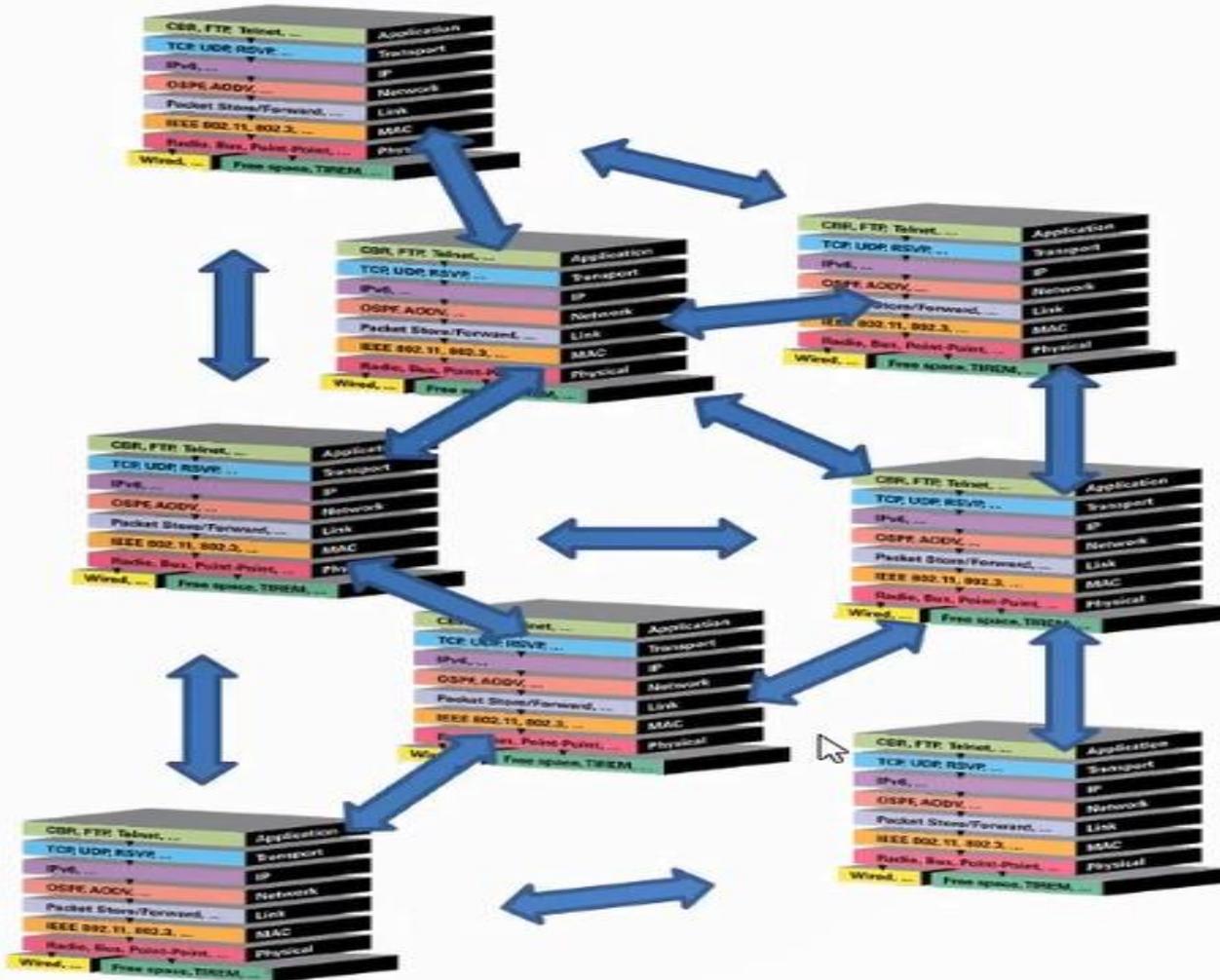
Hardware In The Loop + External Interfaces

Communication Channels, Mobility & Terrain Models

Kernel for Simulation & Emulation

Packet Sniffer + SNMP Interfaces

# EXata



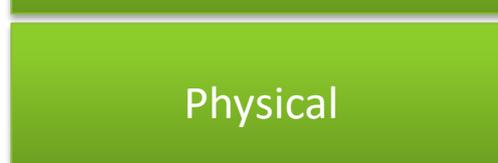
työtä -ohjelma



## Attack models encompassing the protocol stack :

### Defensive Breach Framework

- Firewall models
- Interface with attack generators & IDS



Physical Attacks

### Physical Attack Framework

### Denial of Service Framework

- OS resource modeling
- Resource depletion modeling



### Routing Misconfig Framework



### Sniffing and Passive traffic analysis



↑ Wired & Wireless

### Eavesdropping Framework

↓ Wireless

### Signals Intelligence Framework

### Jamming Framework

- Barrage Noise Jamming
- "Silent" 802.11 MAC jammer
- Sweep jamming

Kestävä kasvu ja työllisyys-ohjelma





EXata



Standard Toolbar      Components Toolbar      View Toolbar      Keyword Search Box

Menu Bar      Coordinates Toolbar

The screenshot displays the EXata software interface. At the top, there is a menu bar with options: File, Edit, View, Tools, Animation, Help. Below the menu bar is a toolbar containing icons for Architect, Analyzer, Packet Tracer, and File Editor. A search box is located on the right side of the toolbar. Below the toolbar is a status bar showing coordinates: X: 661.52, Y: 261.29, Z: 0.00. The main workspace is a 3D grid with a central green field labeled 'CBR'. Several buildings are visible, with red markers and numbers (2, 4, 6) indicating network components. A zoom control is on the right side of the grid. On the left side, there are several panels: 'File System', 'Toolset', 'Visualization Controls', and 'Runtime Analysis'. The 'Runtime Analysis' panel is open, showing various application categories like CBR, TEL NET, and Dynamic Address Applications. At the bottom, there are several panels: 'Table View', 'Output Window', 'Error Log', 'Watch Variables', and 'Batch Experiments'. A 'Toolset' dropdown menu is also visible at the bottom left.

Left Panels  
(Toolset Panel open)

Bottom Panels



# EXata



## SCALABLE NETWORK TECHNOLOGIES

The screenshot displays the EXata software interface. The main window shows a 3D city map (Google Earth) with network overlays in yellow and red. The interface includes a menu bar (File, Edit, View, Tools, Animation, Help), a toolbar, and a left sidebar with categories: File System, Toolkit, Visualization Controls, Runtime Analysis, and Cyber Attacks. The bottom right features a table with network data and a status bar with options like Table View, Output Window, Error Log, Watch Variables, and Batch Experiments.

Network Address	Type	Member Nodes	UUID
169.0.0.0	Default Wireless Subnet	{1}	SUB2
190.0.1.0	Wireless Subnet	0	SUB1

Activate Windows  
Go to Settings to activate Windows.



# EXata



EXata Network Emulation Interface

Architecture: Analyzer, Packet Tracer, File Editor

Static and Default Routes

Lat: 34.617372 Lon: -119.660954 Alt: 952.54

3D View Saved Views

Human in the Loop:

untitled\_1 untitled\_2 GroundMicroSatFailoverTemplate 5\_11\_MCBR 5\_11\_IPvNCompareIPv6 5\_11\_IPvNCompareIPv4 5\_11\_StaticRoutes 5\_11\_ChanIndices 5\_11\_DEM

Animation Speed: Slow Fast

Animation Filters

Event Filters

- All
- Node Mobility
- Broadcast Packet
- Multicast Packet
- Unicast Packet
- Packet Received
- Packet Dropped
- Packet Collision
- Packet Queuing
- Node Orientation

SIM 00hr : 00m : 00s 0% REAL 00hr : 00m

Warning in file C:\jenkins\workspace\Exata\_Release\exata\interfaces\pas\src\packet\_analyzer.cpp:1525  
EXata interface not found. Packet Sniffer disabled

Warning in file C:\jenkins\workspace\Exata\_Release\exata\interfaces\auto-ipne\src\inject\_interface.cpp:1039  
Cannot use device \Device\NPF\_{7136751E-FCA3-49CB-9C15-13571D5E504B} for emulation. Error: libnet\_open\_link(): network type (-1) is not supported

Warning in file C:\jenkins\workspace\Exata\_Release\exata\interfaces\pas\src\packet\_analyzer.cpp:1525  
EXata interface not found. Packet Sniffer disabled

Warning in file C:\jenkins\workspace\Exata\_Release\exata\interfaces\auto-ipne\src\inject\_interface.cpp:1039  
Cannot use device \Device\NPF\_{7136751E-FCA3-49CB-9C15-13571D5E504B} for emulation. Error: libnet\_open\_link(): network type (-1) is not supported



# Cybersecurity and Resilience of Digital Energy Systems (CR-DES ) Value

- Test and predict power systems and communication networks behavior under attack.
- Ability to scale to represent the entire network.
- Integration of the developed real time simulation models with equipment and power grid HIL, PHIL etc.
- Run 'what-if' scenarios about critical infrastructure under cyber-attack without threatening operations.
- Assess effectiveness of tools, techniques and architectures to ensure system availability.
- Measure and improve system resiliency.

