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

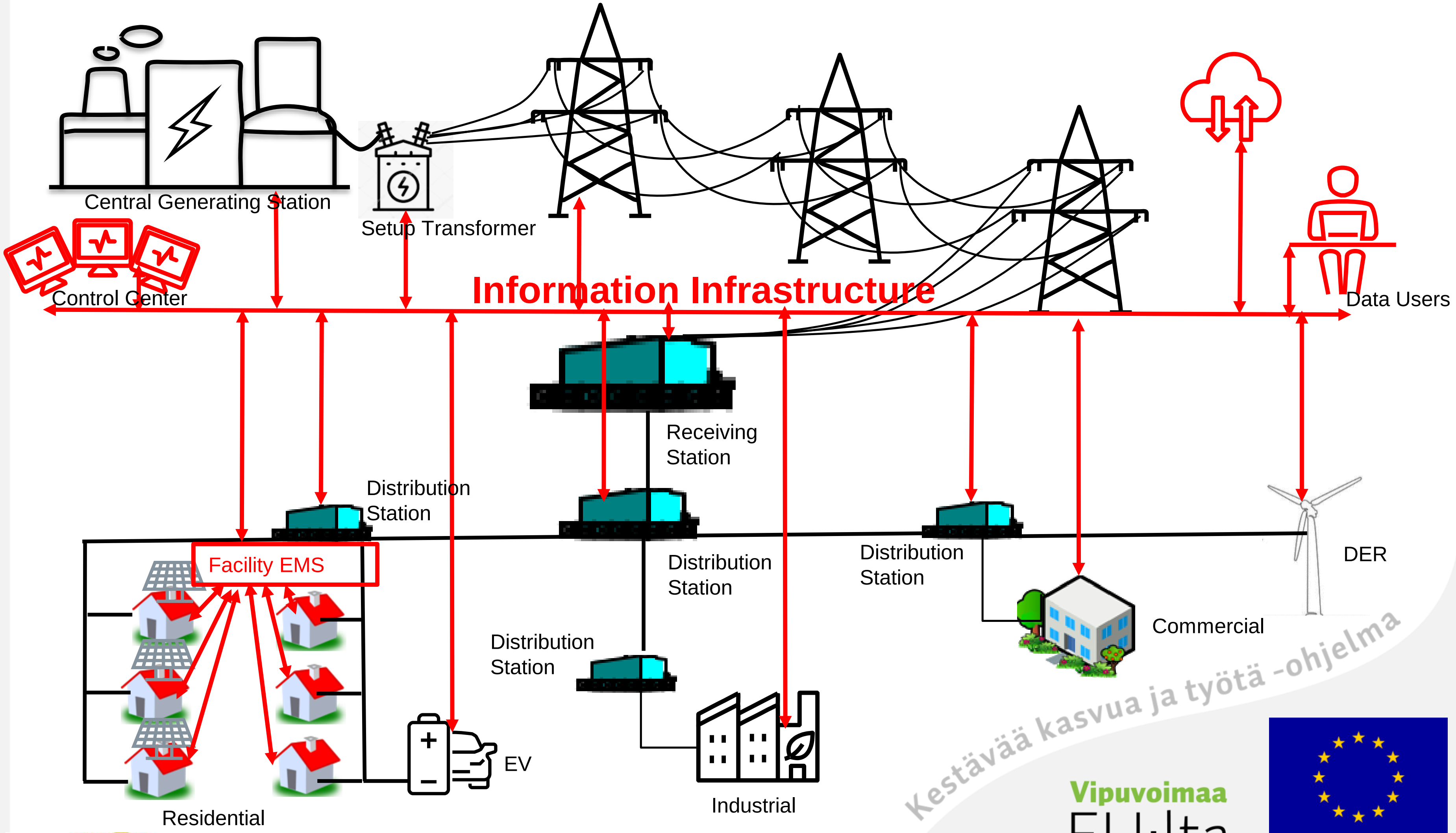
23.8.2021

Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

Digitalization (ICT) for the existing energy system



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

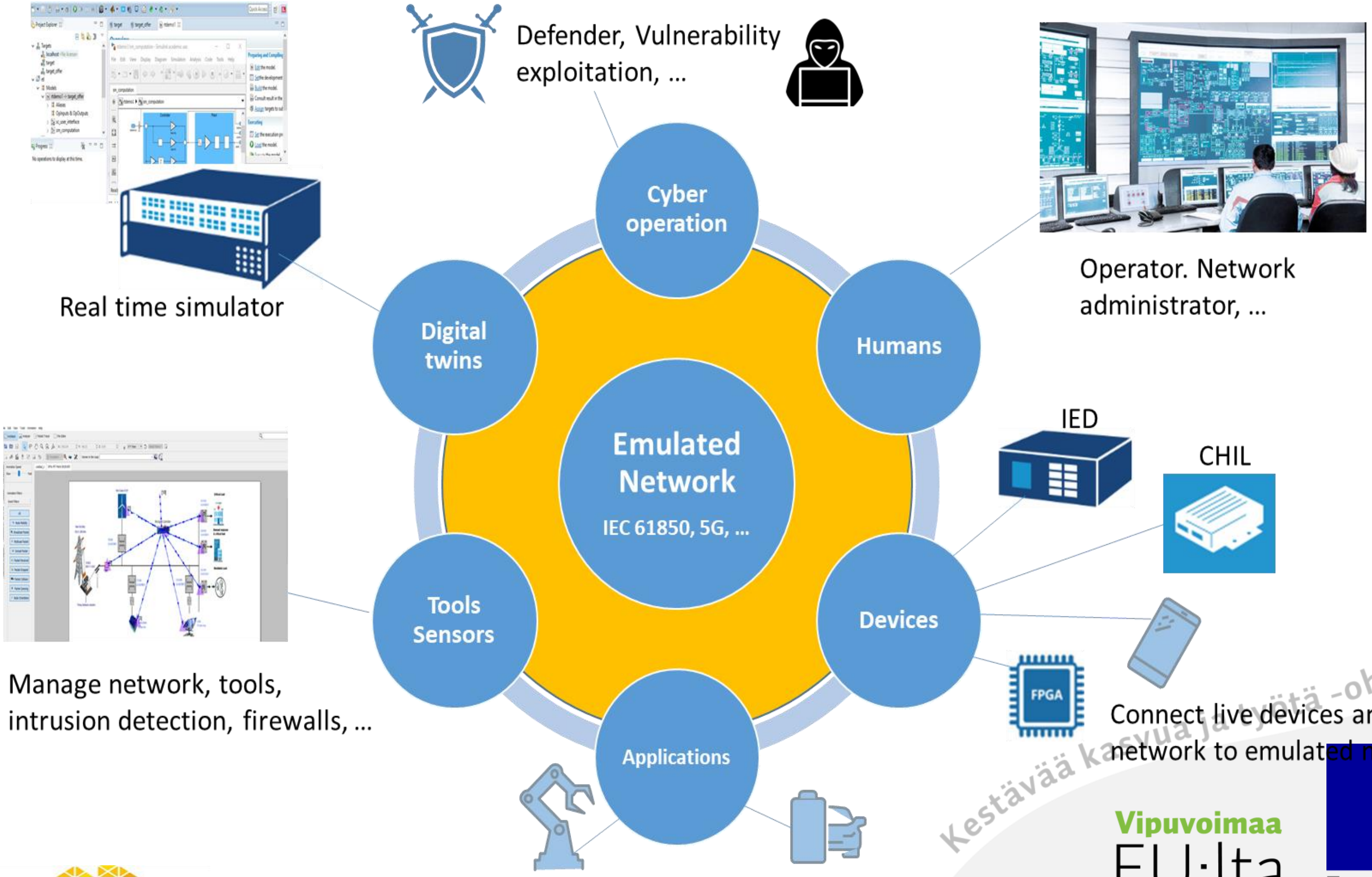
Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

CPS Platform- - RT Simulator

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



Emulated Network

IEC 61850, 5G, …

Cyber operation

Humans

Devices

Applications

Tools Sensors

Digital twins

Defender, Vulnerability exploitation, …

Operator. Network administrator, …

Real time simulator

Manage network, tools, intrusion detection, firewalls, …

Connect live devices and network to emulated network

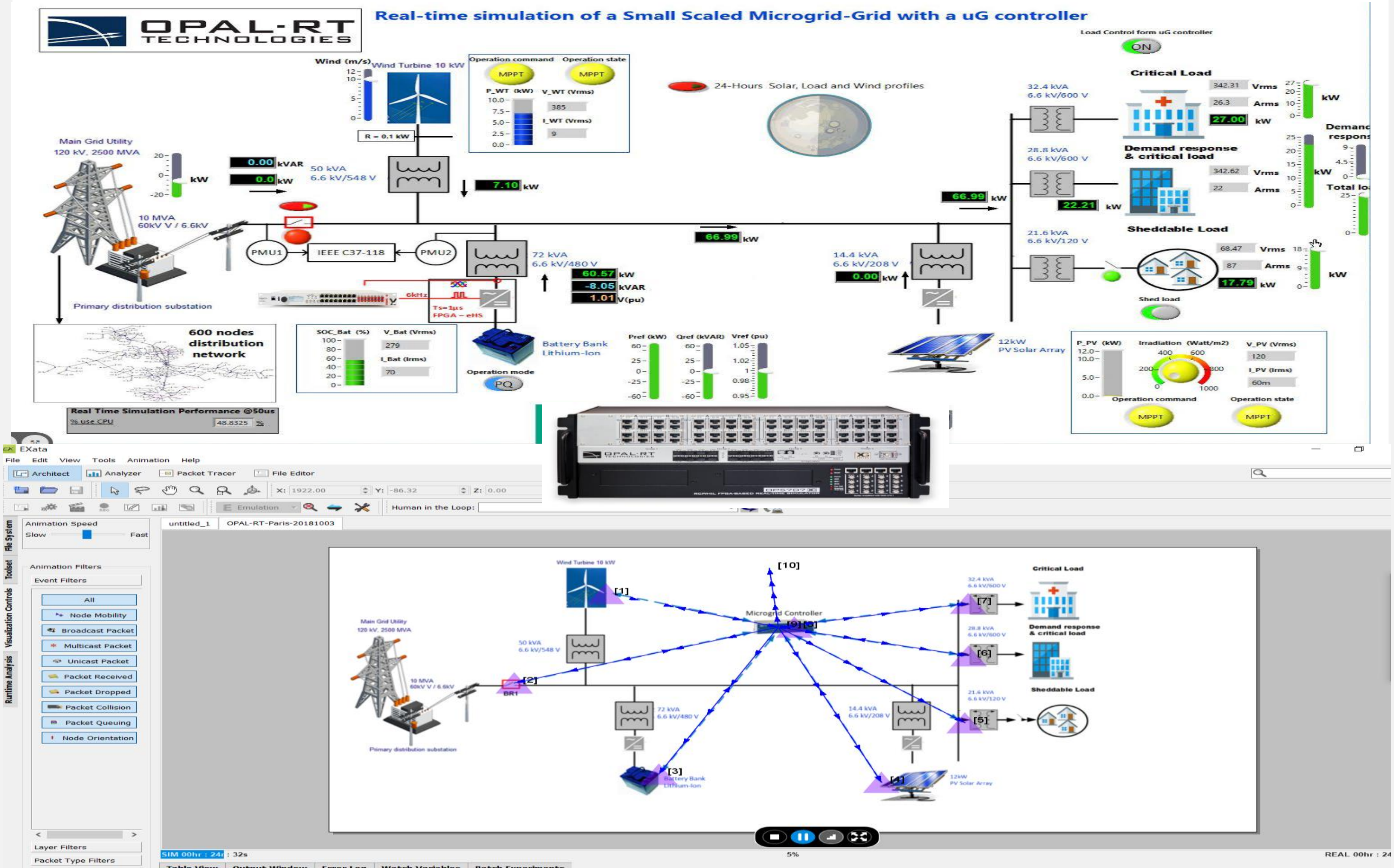
Connect actual application

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

CPS Platform - RT Simulator

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



CPS Platform - RT Simulator

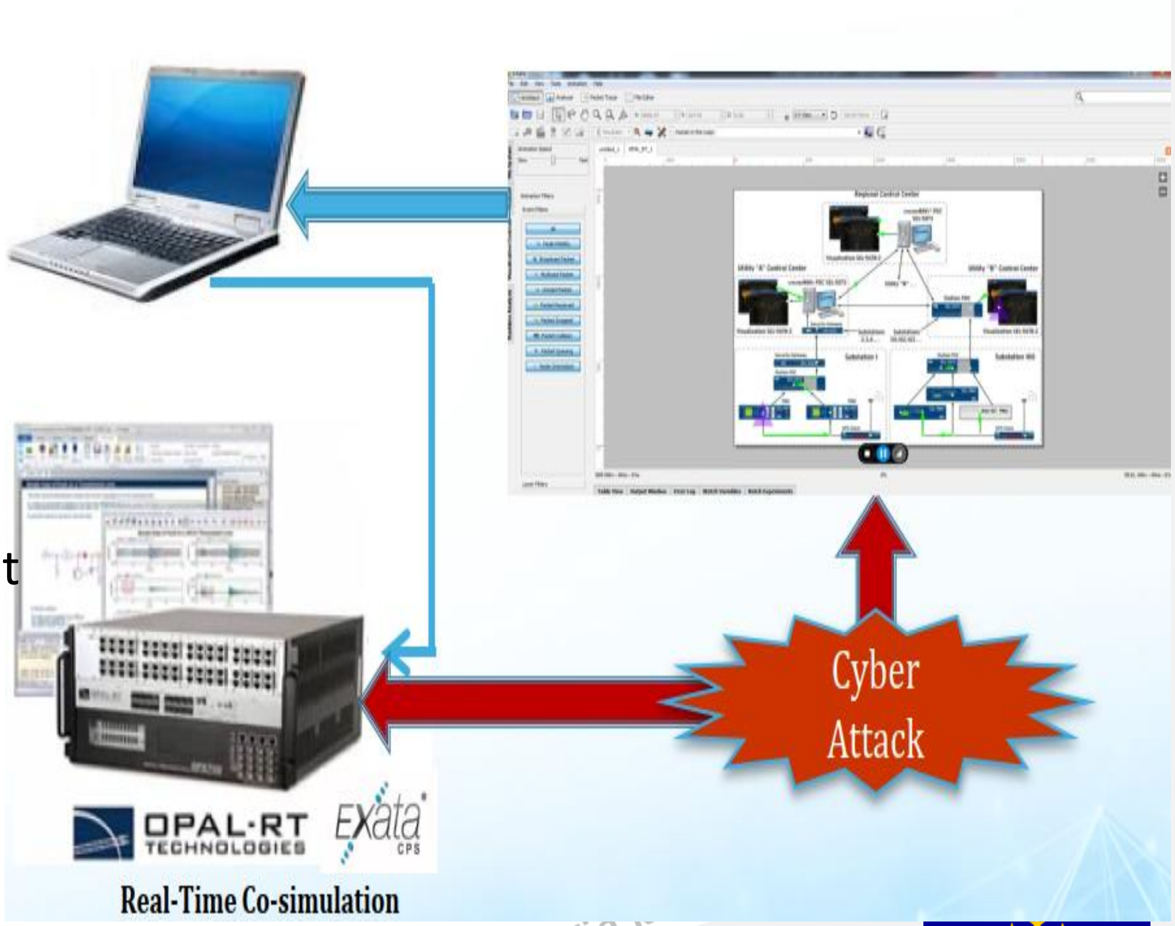
Cybersecurity and Resilience of Digital Energy Systems (CR-DES)

Host PC

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

Real-Time Co-simulation Target

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



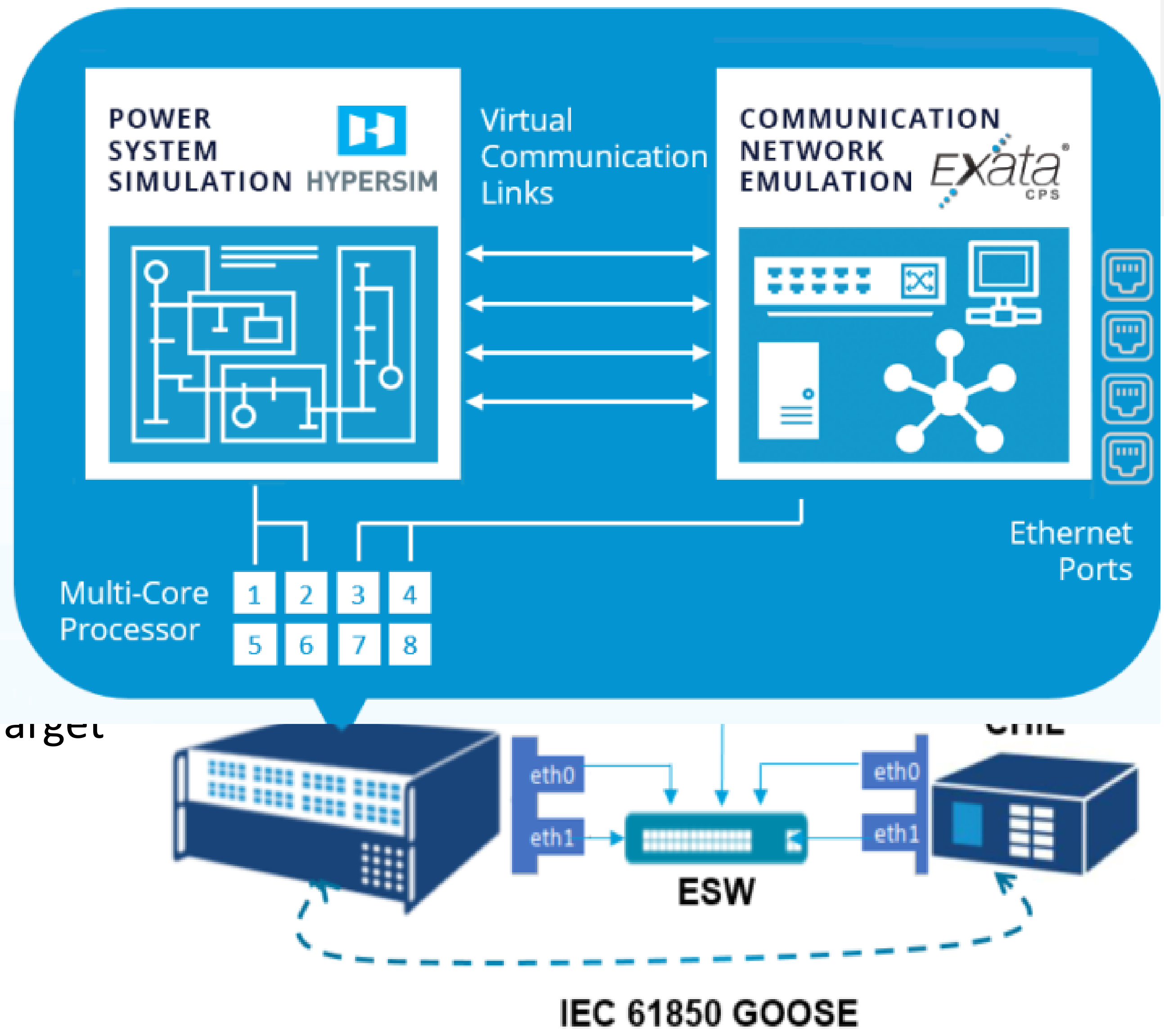
Kestävää
Vipuvoimaa EU:lta 2014–2020
Euroopan unioni
Euroopan aluekehitysrahasto

CPS

Cybersecurity and Resilie

Host PC

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



Real-Time Co-simulation Target

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

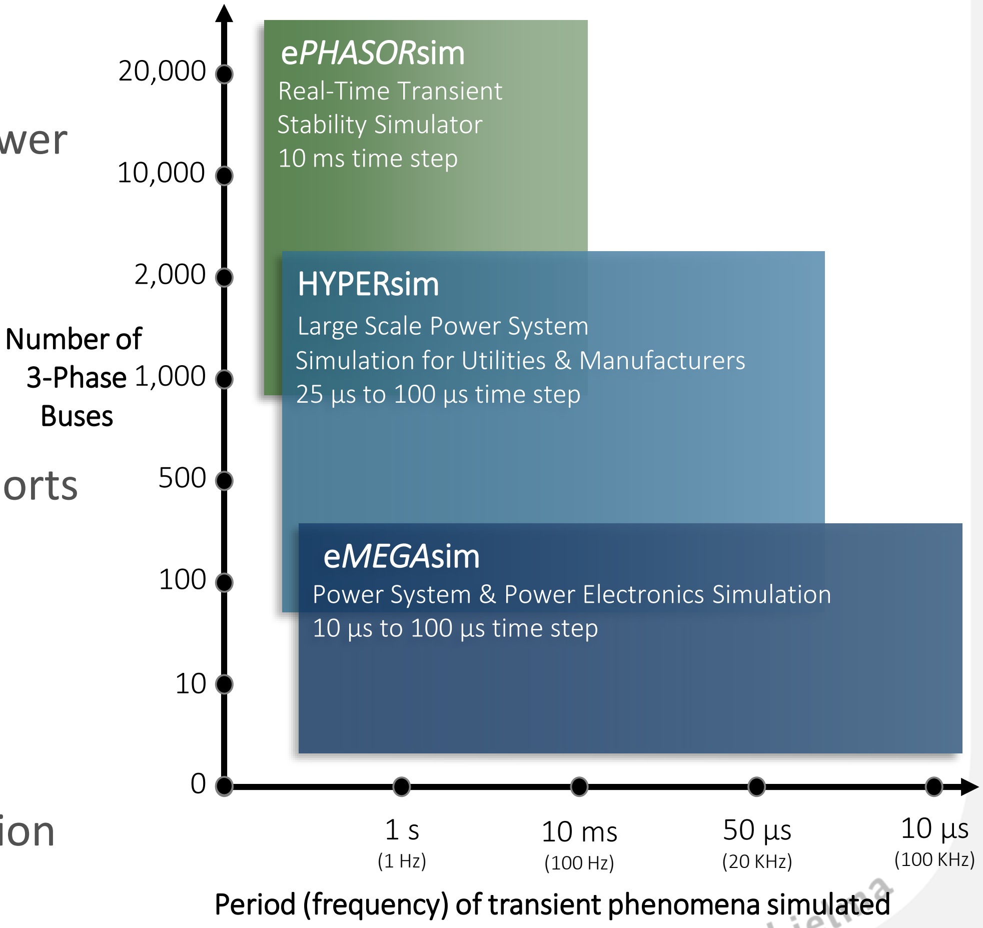
HYPERSIM

- 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

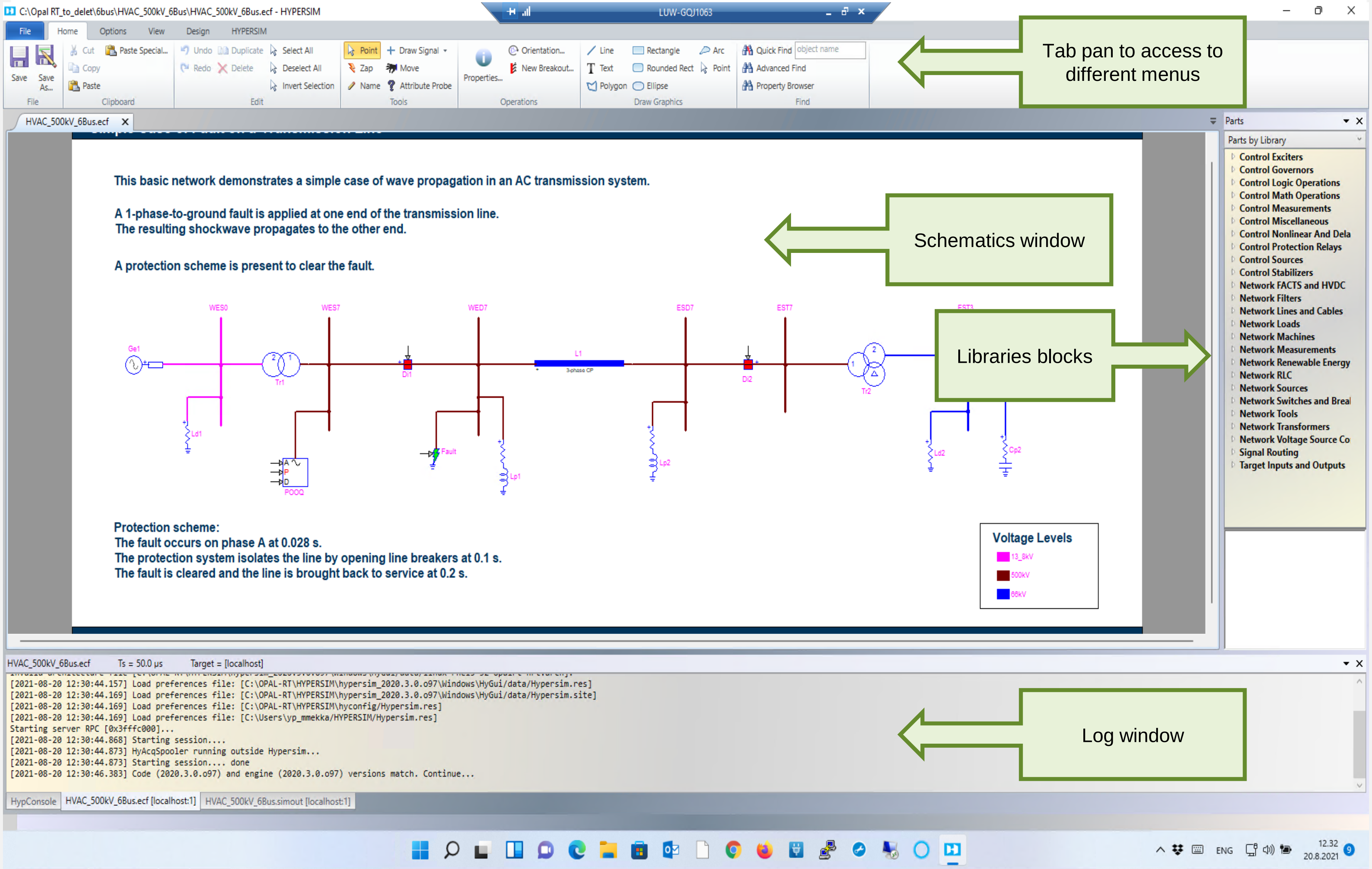
- **TestView**: Automated testing with (supports Python)

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

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



HYPERSIM



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.

```
[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_mmekka/HYPERSIM/Hypersim.res]
Starting server RPC [0x3fffc000]...
[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...
```

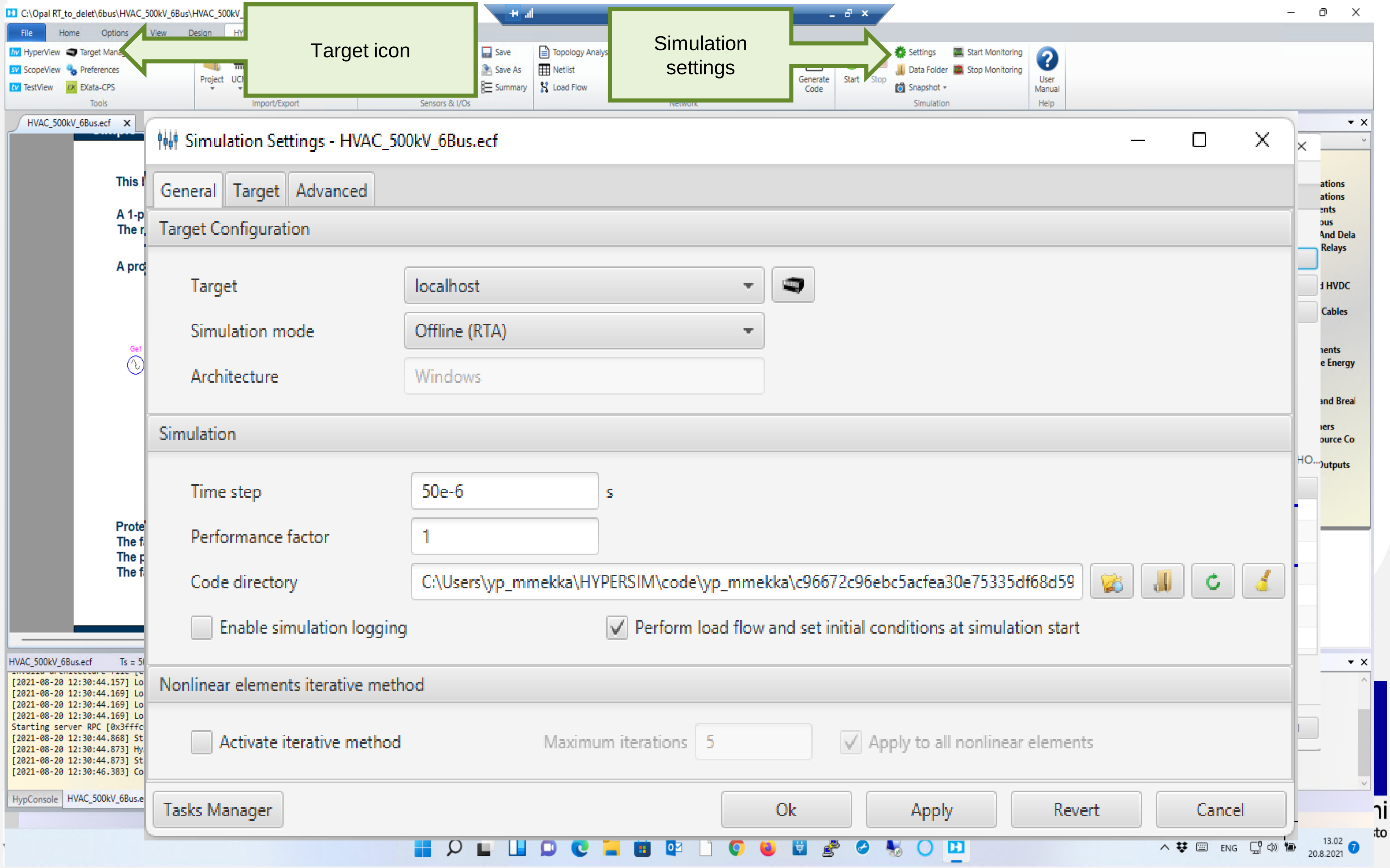
Tab pan to access to different menus

Schematics window

Libraries blocks

Log window

HYPERSIM



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

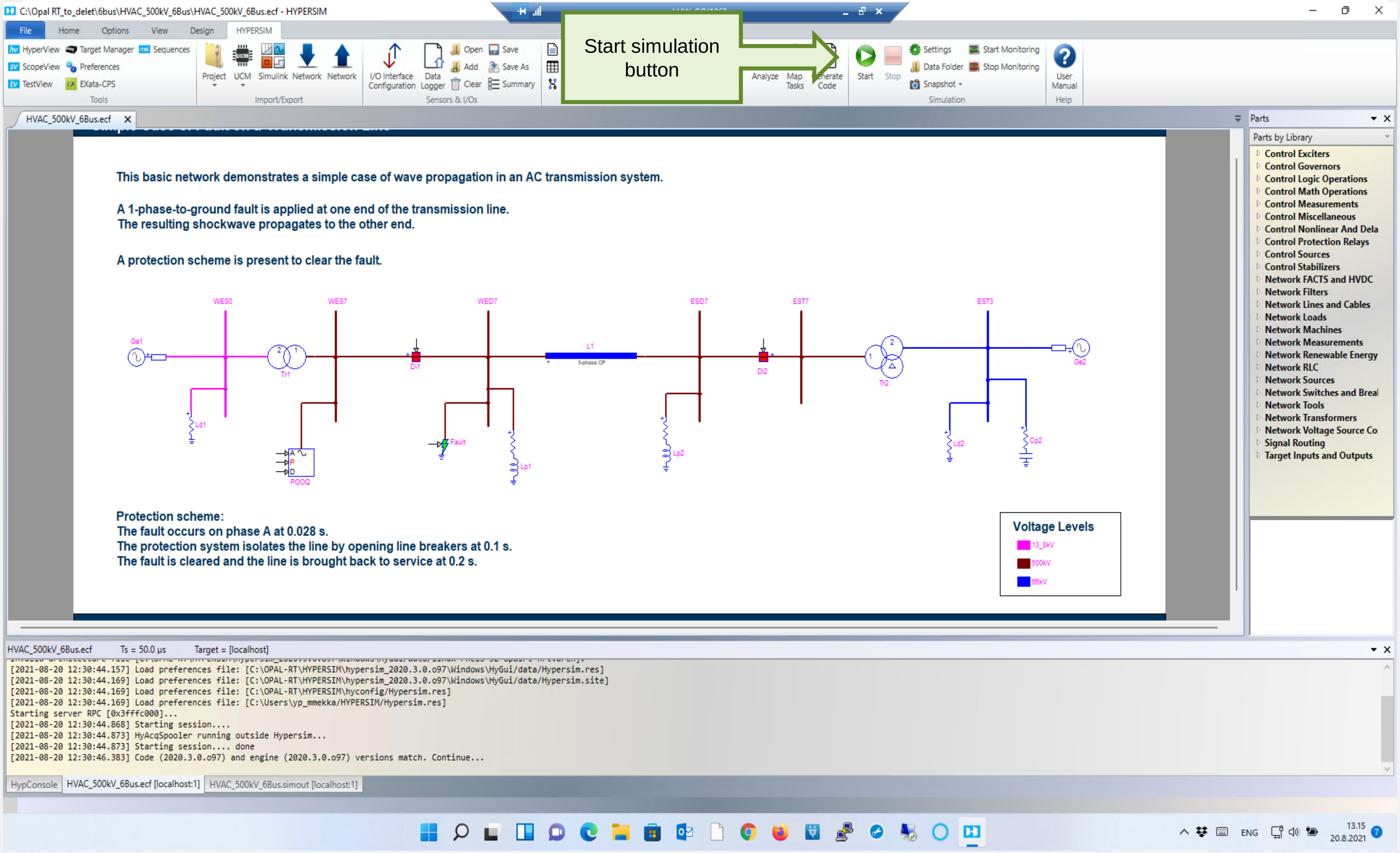
Maximum iterations: 5

☑ Apply to all nonlinear elements

Tasks Manager | Ok | Apply | Revert | Cancel

```
[2021-08-20 12:30:44.157] Lo
[2021-08-20 12:30:44.169] Lo
[2021-08-20 12:30:44.169] Lo
[2021-08-20 12:30:44.169] Lo
Starting server RPC [0x3fffc
[2021-08-20 12:30:44.868] St
[2021-08-20 12:30:44.873] Hy
[2021-08-20 12:30:44.873] St
[2021-08-20 12:30:46.383] Co
```

HYPERSIM



Start simulation button

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

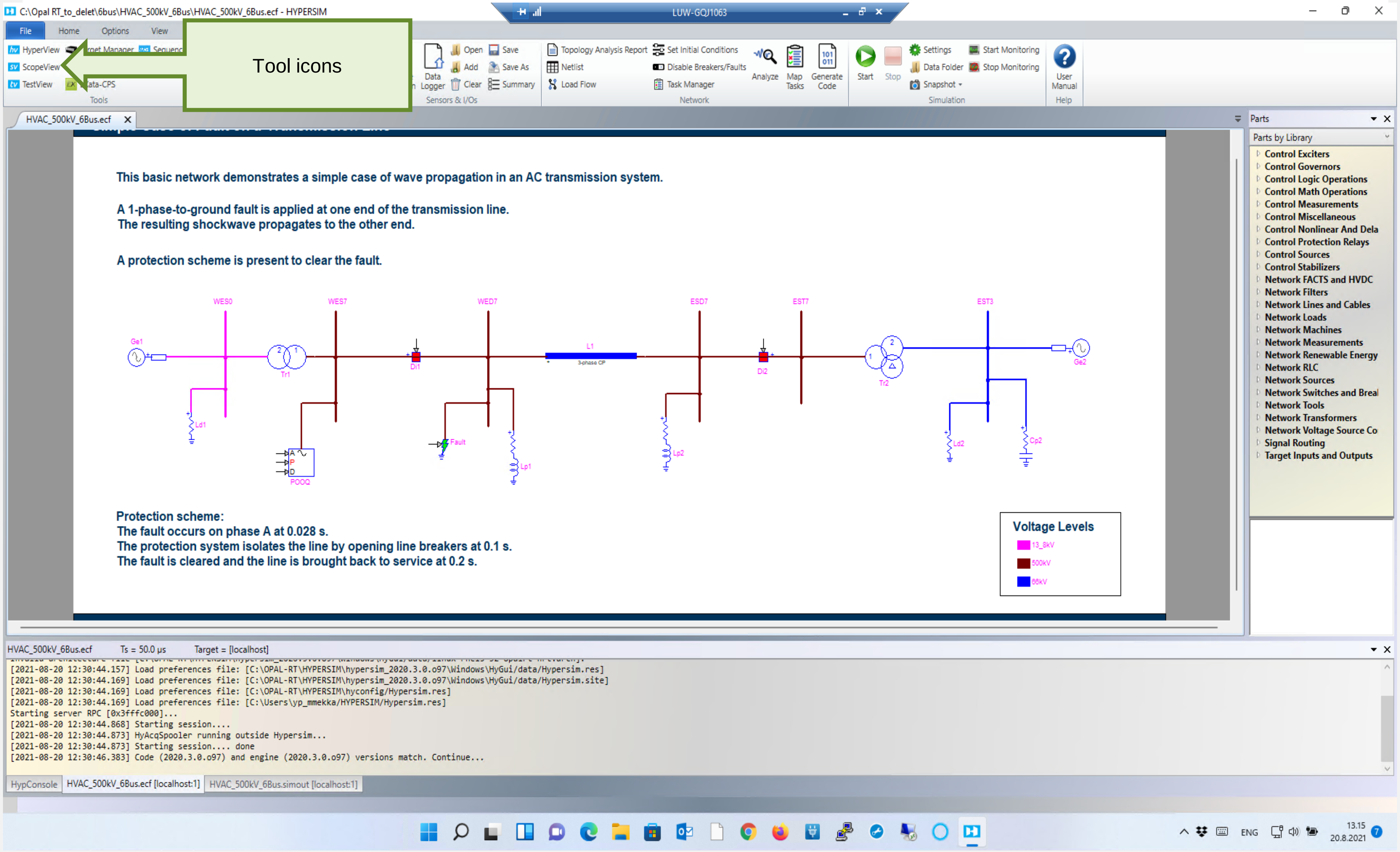
A 1-phase-to-ground fault is applied at one end of the transmission line.
The resulting shockwave propagates to the other end.

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.

```
[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_mmekka/HYPERSIM/Hypersim.res]
Starting server RPC [0x3fffc000]...
[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...
```

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

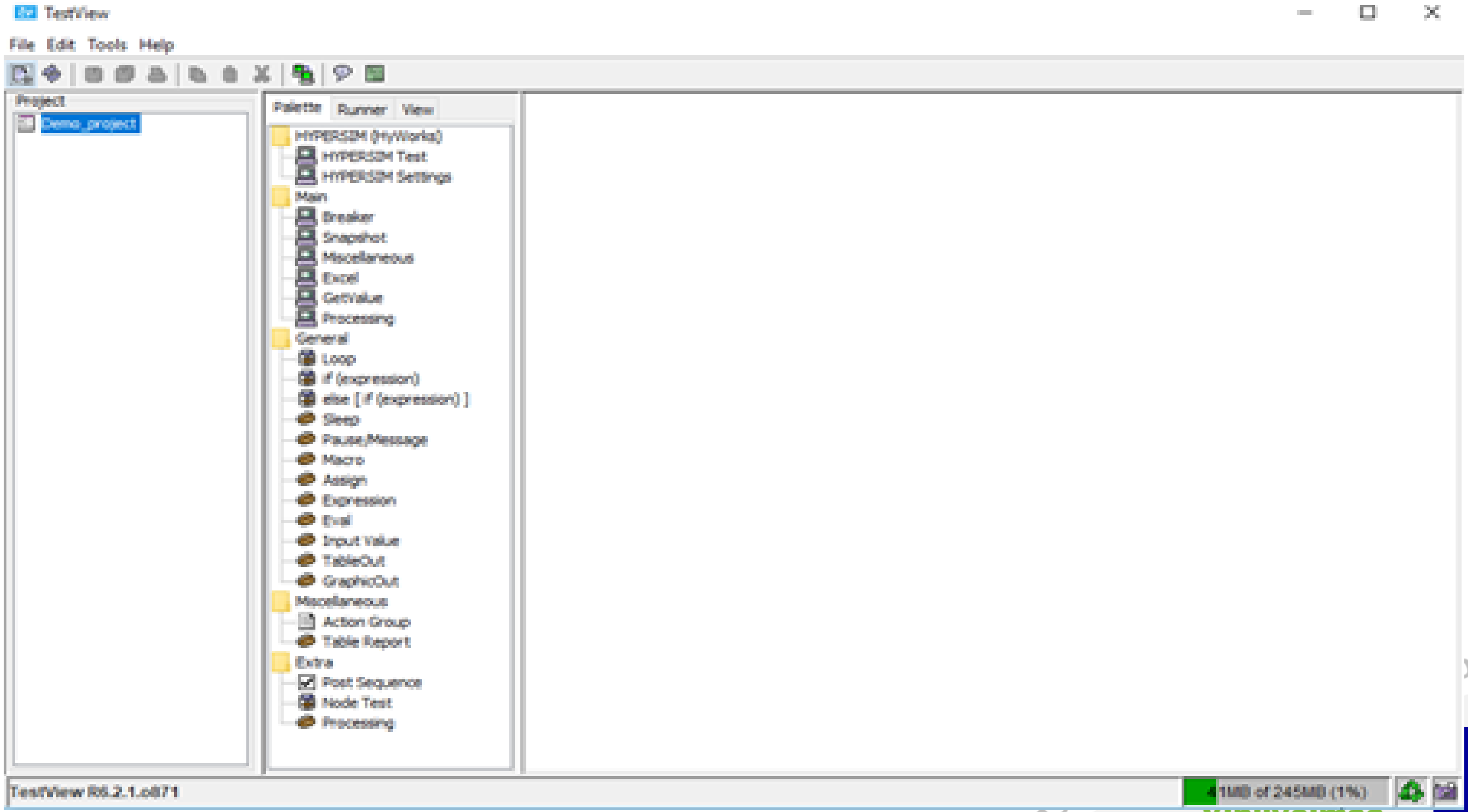
🟪	13_8kV
🟥	500kV
🟦	66kV

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_mmekka/HYPERSIM/Hypersim.res]
Starting server RPC [0x3fffc000]...
[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...
```

HYPERSIM

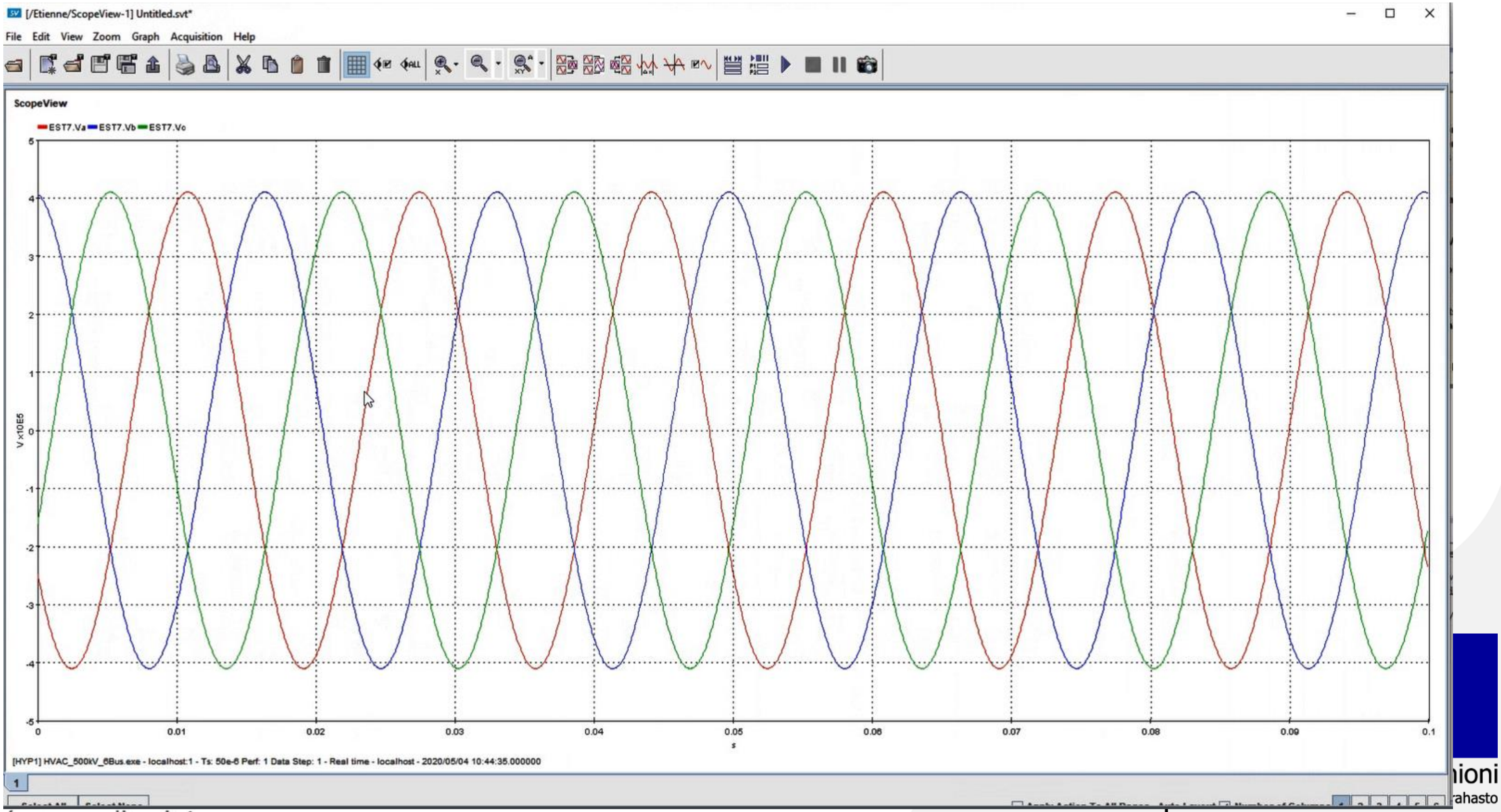
- **TestView**: Automated testing with (supports Python)



HYPERSIM

HYPERSIM

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

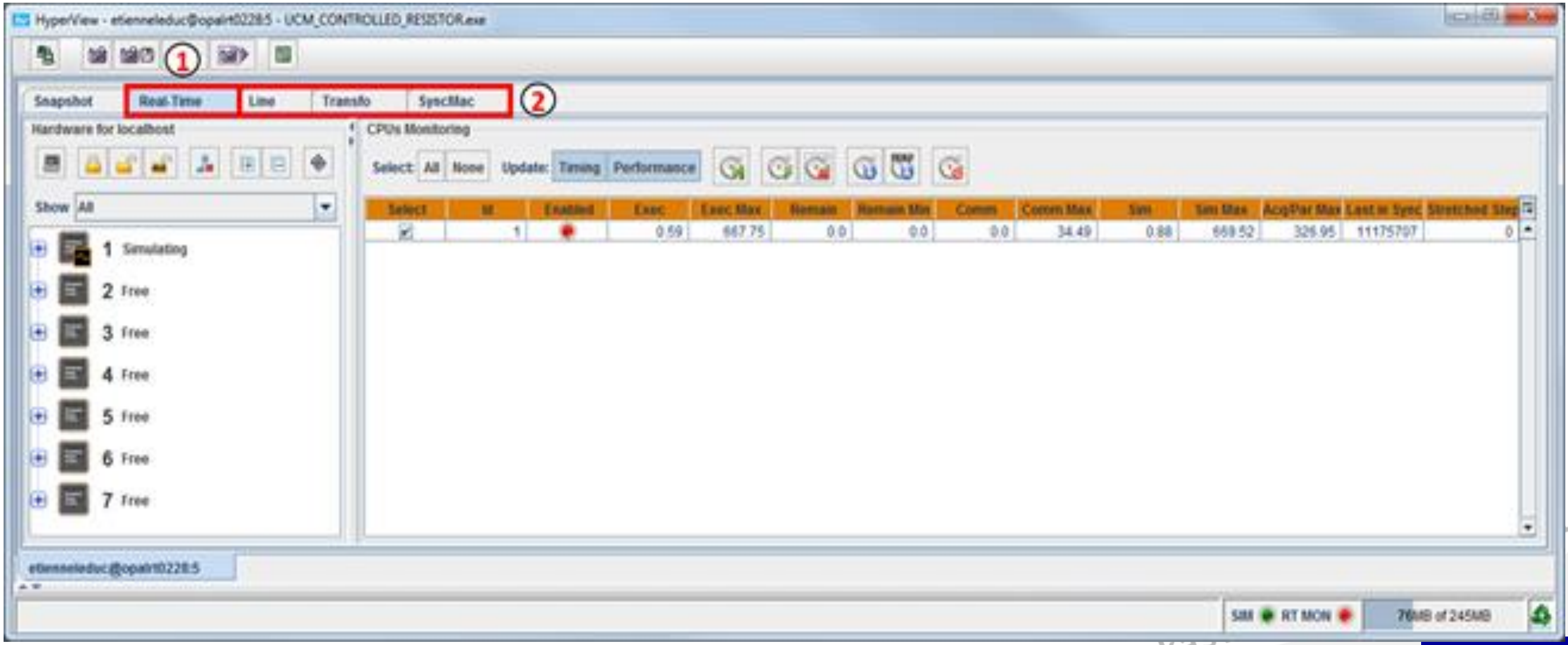


[HYP1] HVAC_500kV_6Bus.exe - localhost:1 - Ts: 50e-6 Perf: 1 Data Step: 1 - Real time - localhost - 2020/05/04 10:44:35.000000

HYPERSIM

HYPERSIM

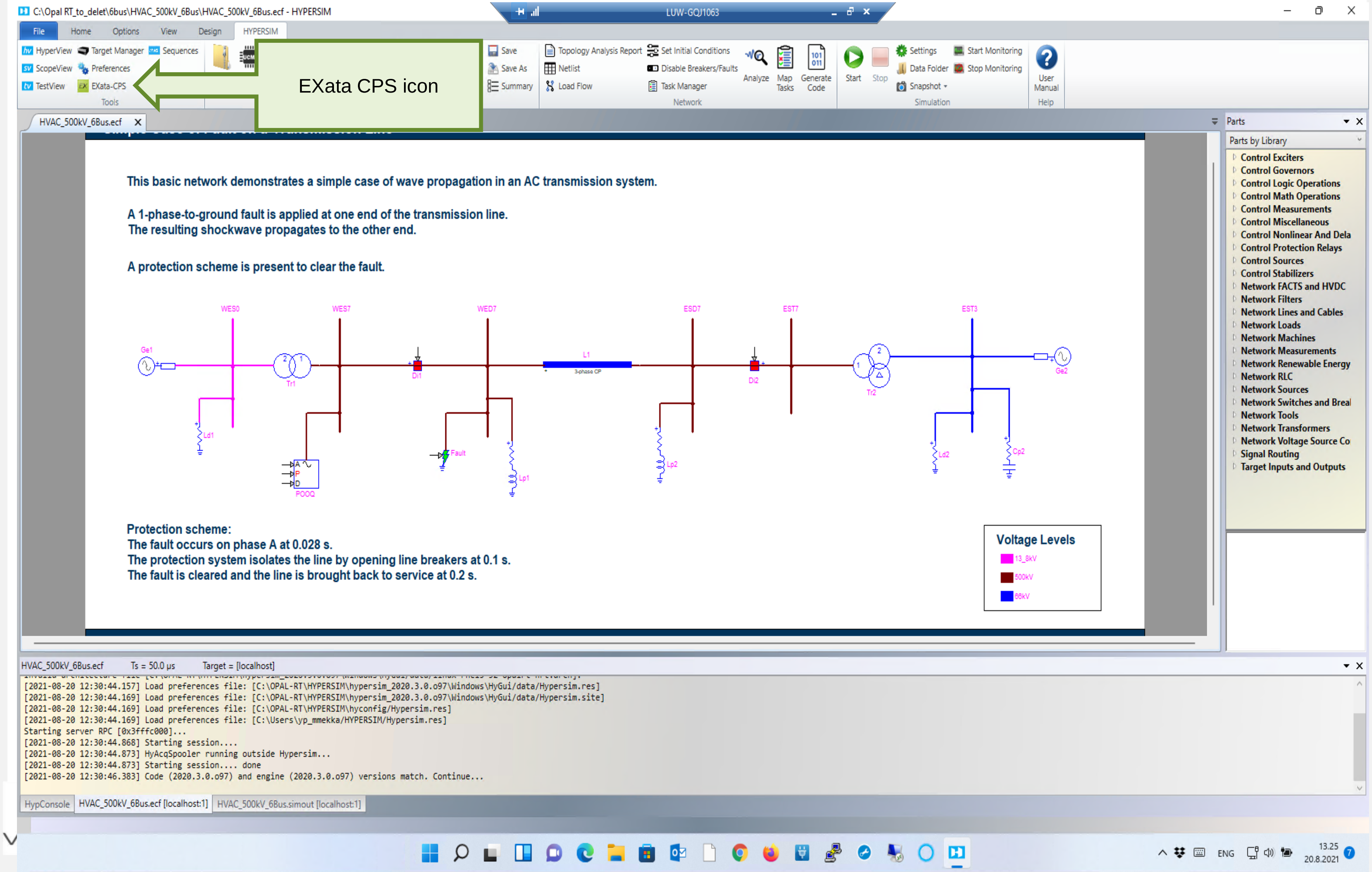
- **HyperView**: enables monitoring simulation performance in real-time



1 Simulating
2 Free
3 Free
4 Free
5 Free
6 Free
7 Free

Select	Id	Enabled	Exec	Exec Max	Remain	Remain Min	Comm	Comm Max	Sim	Sim Max	AcqPar Max	Last in Sync	Stretched Step
☑	1	●	0.59	667.75	0.0	0.0	0.0	34.49	0.88	669.52	326.95	11175707	0

HYPERSIM



EXata CPS icon

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.

```
[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_mmekka/HYPERSIM/Hypersim.res]
Starting server RPC [0x3fffc000]...
[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...
```

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.

EXata

EXata® CPS

SCALABLE NETWORK TECHNOLOGIES

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

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

EXata

EXata CPS

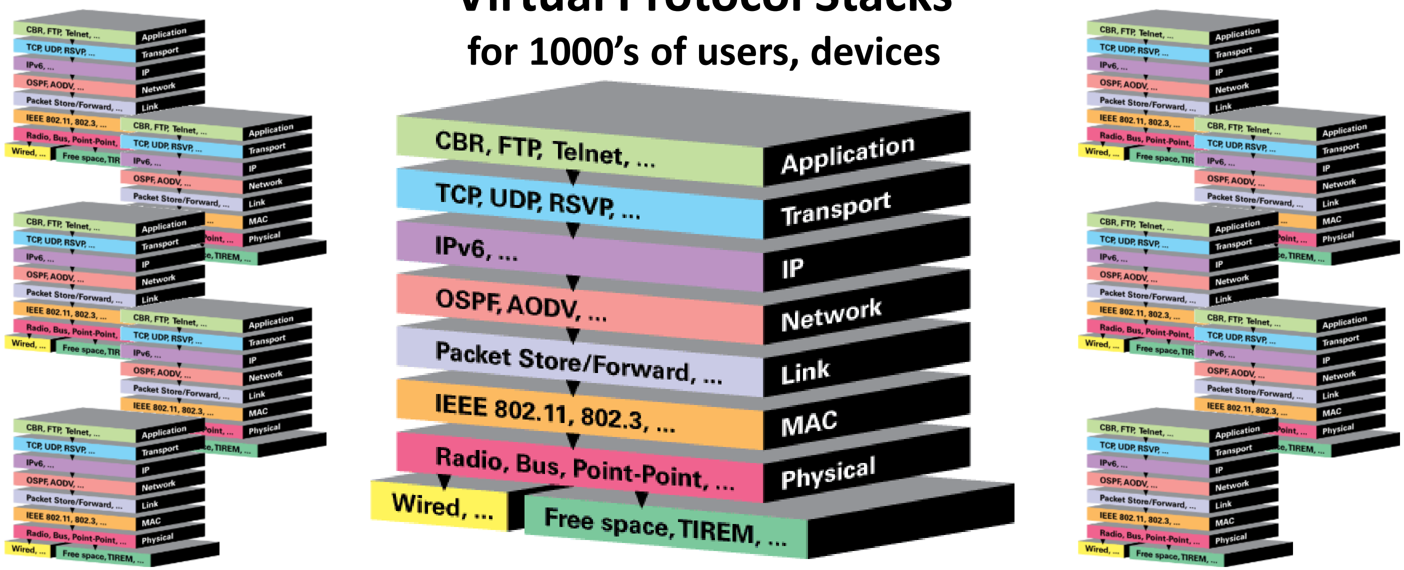
SCALABLE NETWORK TECHNOLOGIES

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

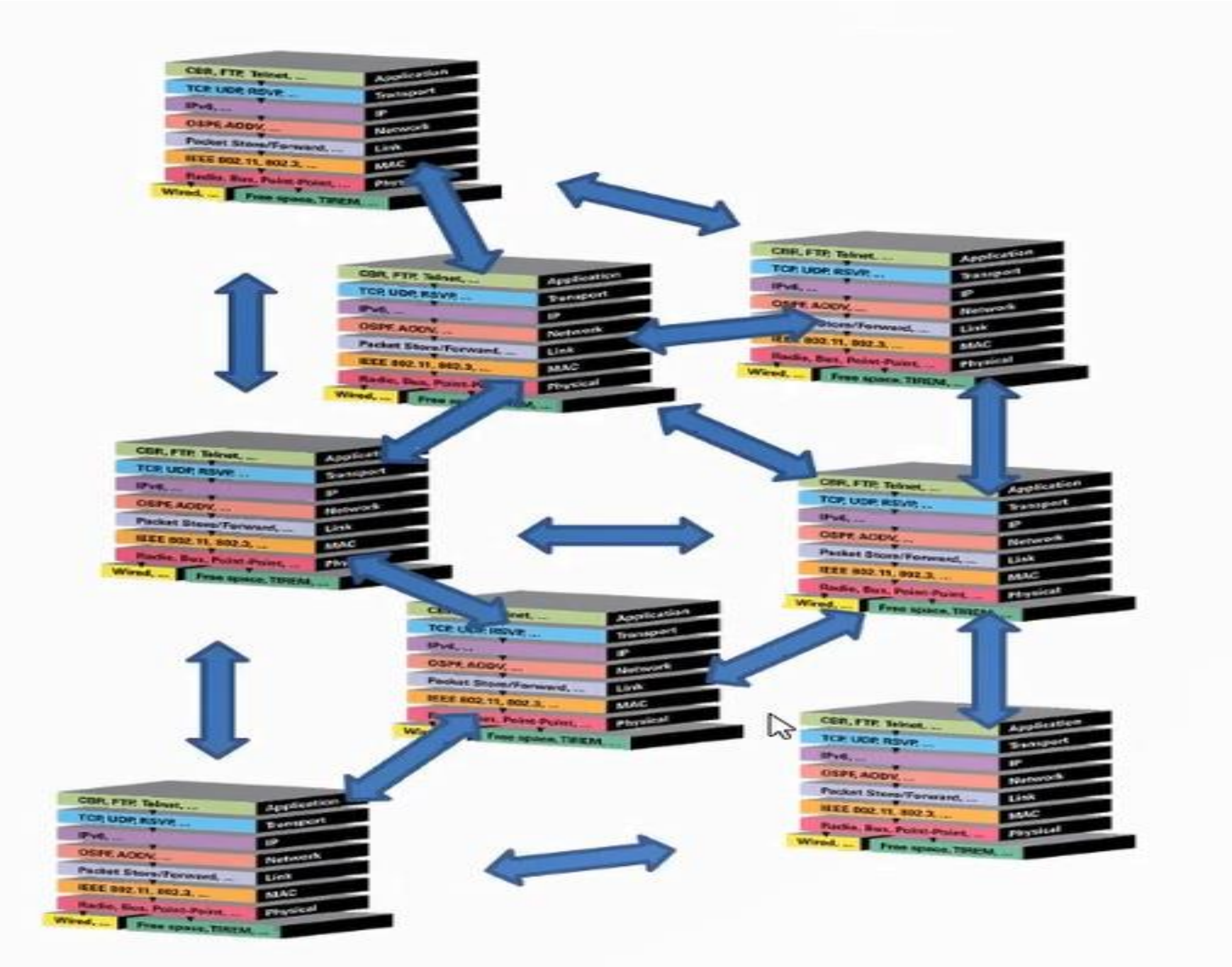
Kernel for Simulation & Emulation

Packet Sniffer + SNMP Interfaces

EXata

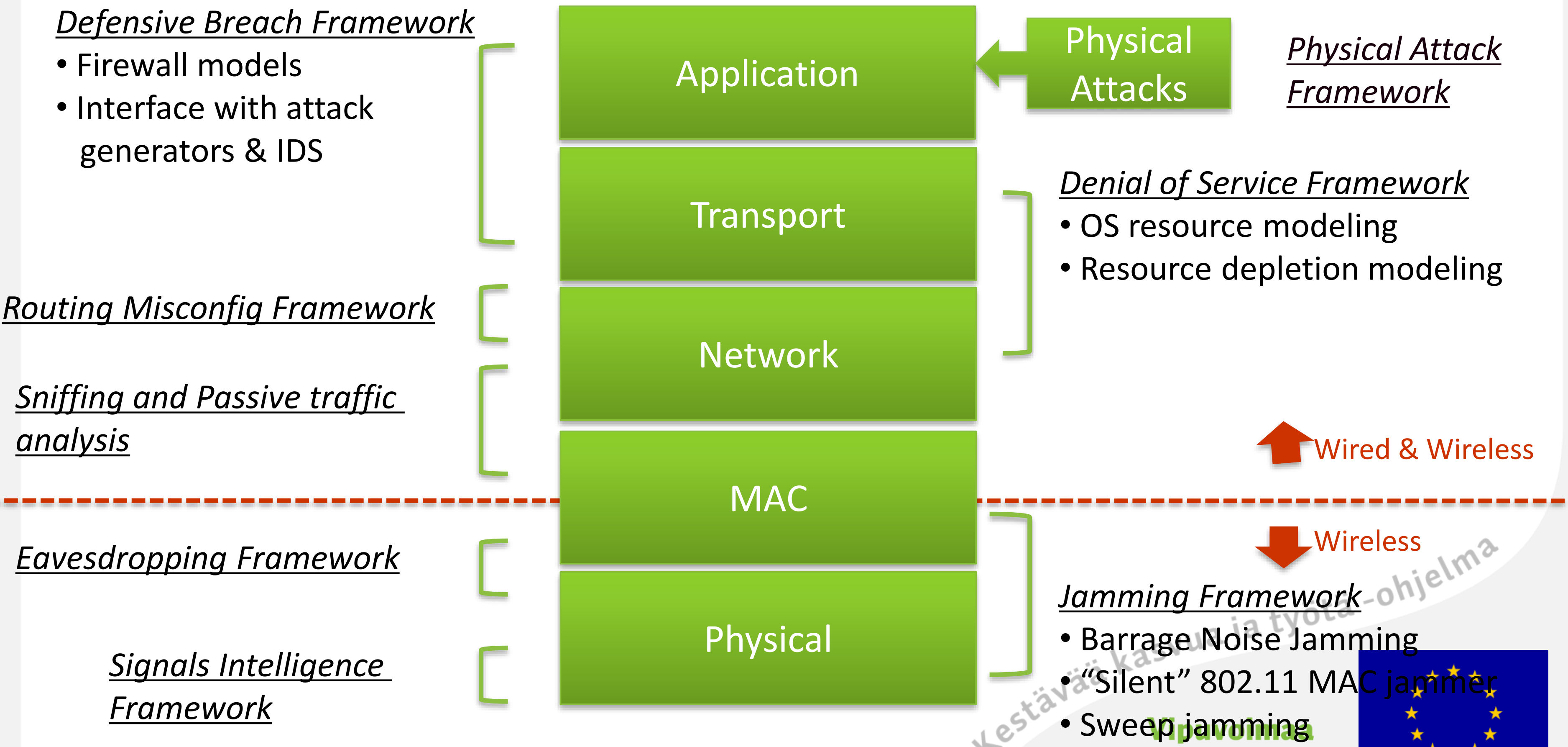
EXata CPS®

SCALABLE NETWORK TECHNOLOGIES



EXata

Attack models encompassing the protocol stack :



Defensive Breach Framework

- Firewall models
- Interface with attack generators & IDS

Routing Misconfig Framework

Sniffing and Passive traffic analysis

Eavesdropping Framework

Signals Intelligence Framework

Physical Attack Framework

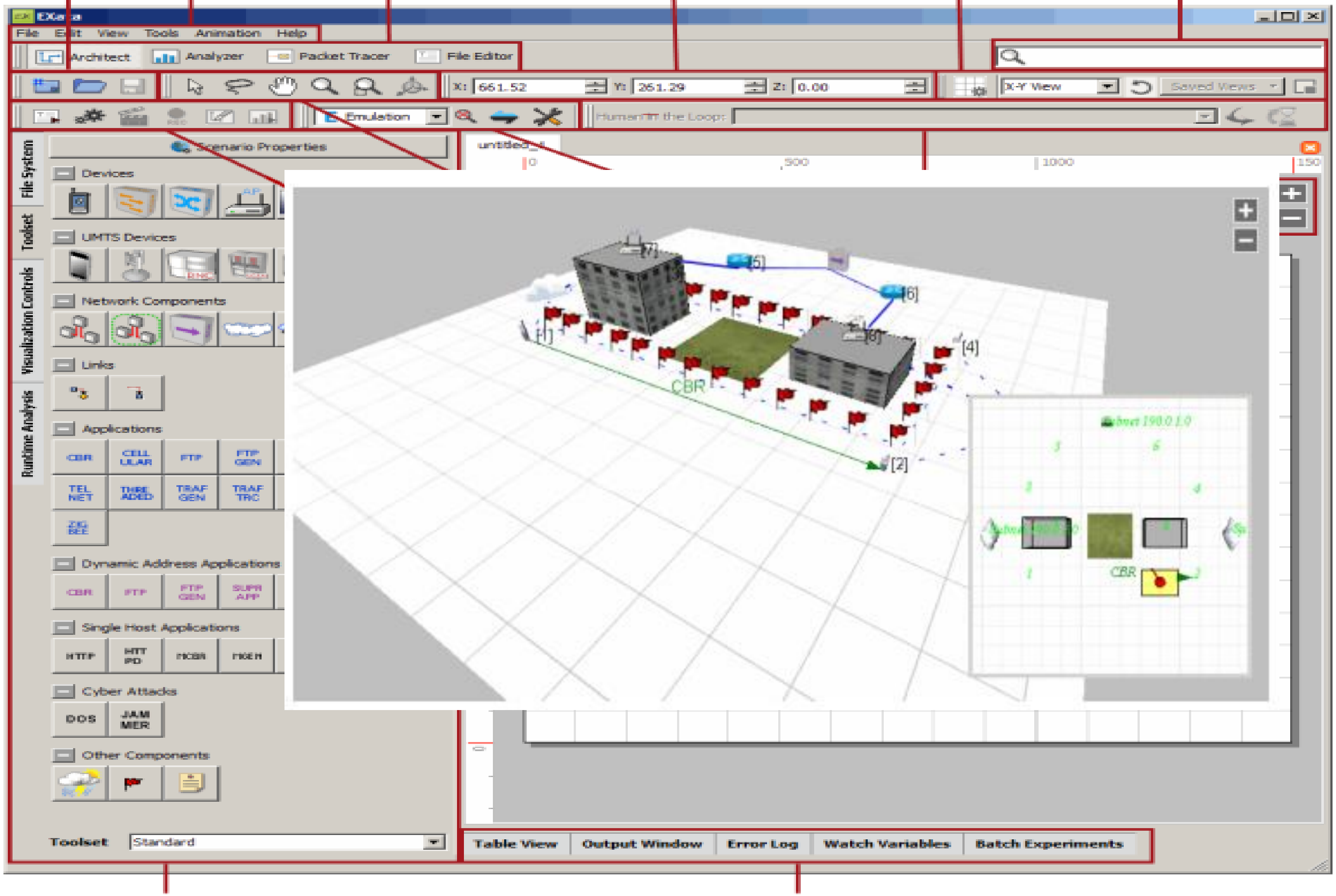
Denial of Service Framework

- OS resource modeling
- Resource depletion modeling

Jamming Framework

- Barrage Noise Jamming
- “Silent” 802.11 MAC jammer
- Sweep jamming

EXata



Standard Toolbar

Menu Bar

Components Toolbar

Coordinates Toolbar

View Toolbar

Keyword Search Box

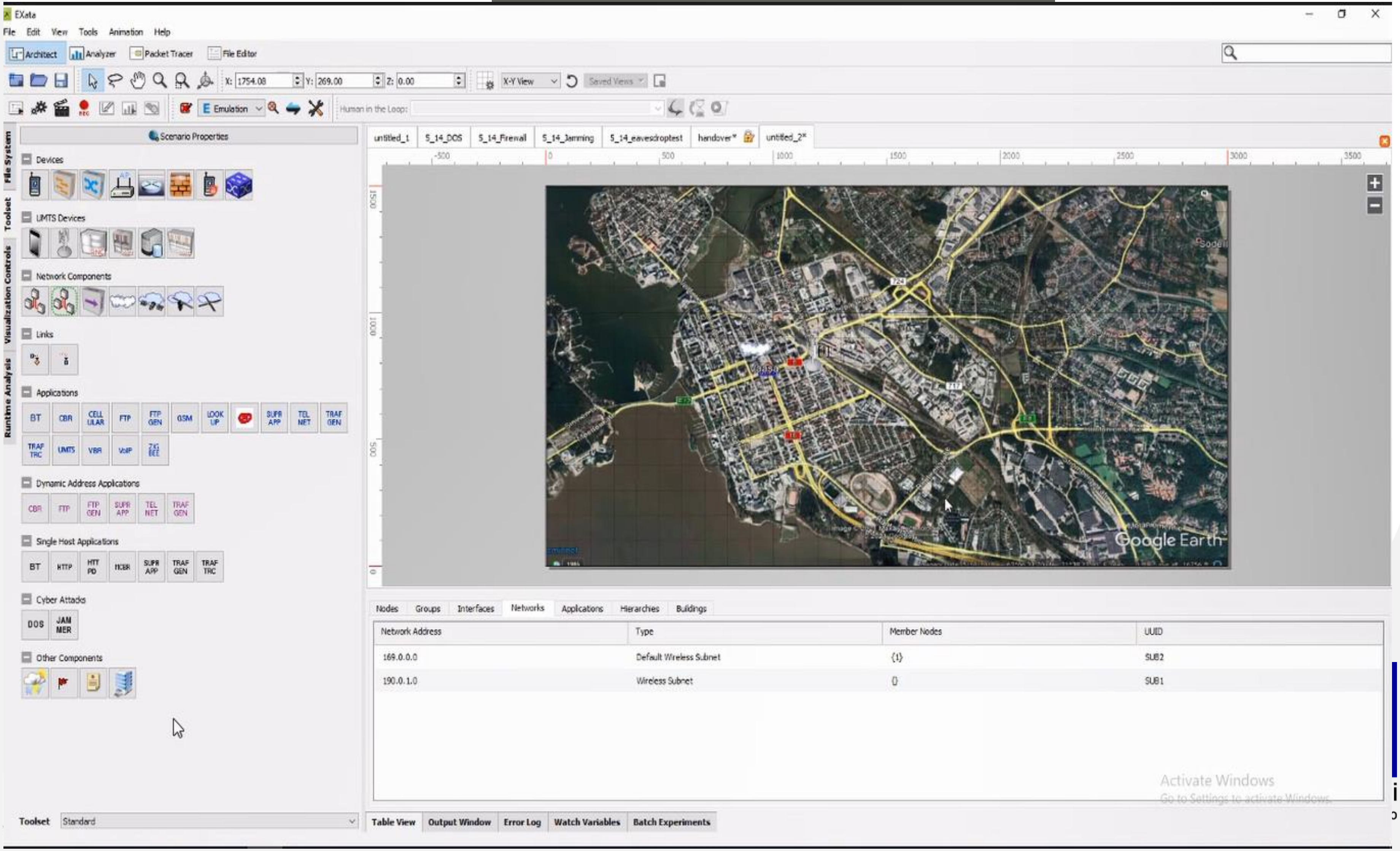
Left Panels
(Toolset Panel open)

Bottom Panels

EXata

EXata® CPS

SCALABLE NETWORK TECHNOLOGIES


EXata
File Edit View Tools Animation Help
Architect Analyzer Packet Tracer File Editor
Human in the Loop:
File System Toolset Visualization Controls Runtime Analysis
Scenario Properties
Devices
UMTS Devices
Network Components
Links
Applications
BT CBR CELLULAR FTP FTP GEN GSM LOOK UP SUPR APP TEL NET TRAF GEN TRAF TRC UMTS VBR VoIP ZIG BEE
Dynamic Address Applications
CBR FTP FTP GEN SUPR APP TEL NET TRAF GEN
Single Host Applications
BT HTTP HTTPD MCBR SUPR APP TRAF GEN TRAF TRC
Cyber Attacks
DOS JAMMER
Other Components
untitled_1 5_14_DOS 5_14_Firewall 5_14_Jamming 5_14_eavesdroptest handover* untitled_2*
Google Earth
Nodes Groups Interfaces Networks Applications Hierarchies Buildings
Table View Output Window Error Log Watch Variables Batch Experiments
Activate Windows
Go to Settings to activate Windows.

X: 1754.08 Y: 269.00 Z: 0.00

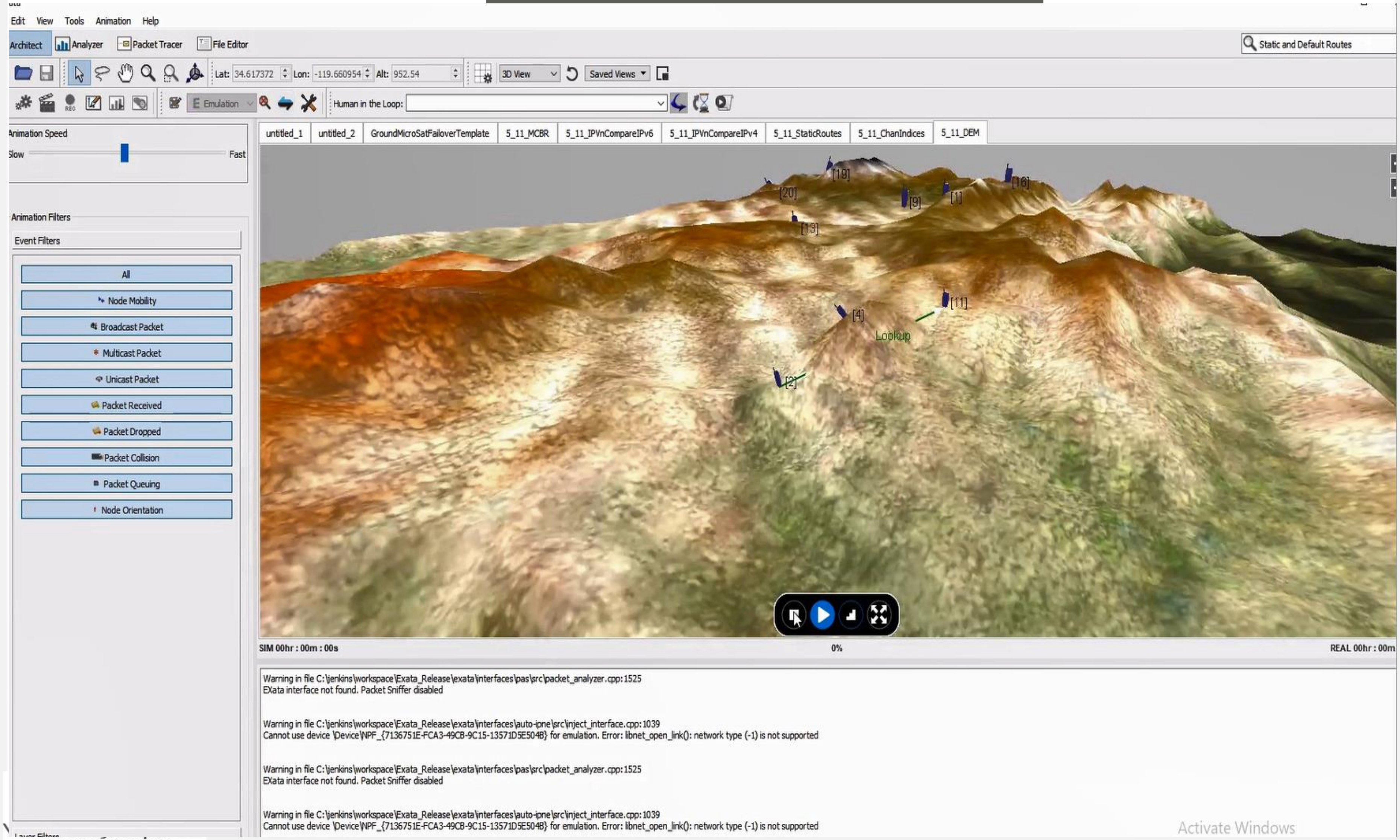
X-Y View

Emulation

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

Toolset Standard

EXata



Lat: 34.617372 Lon: -119.660954 Alt: 952.54

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

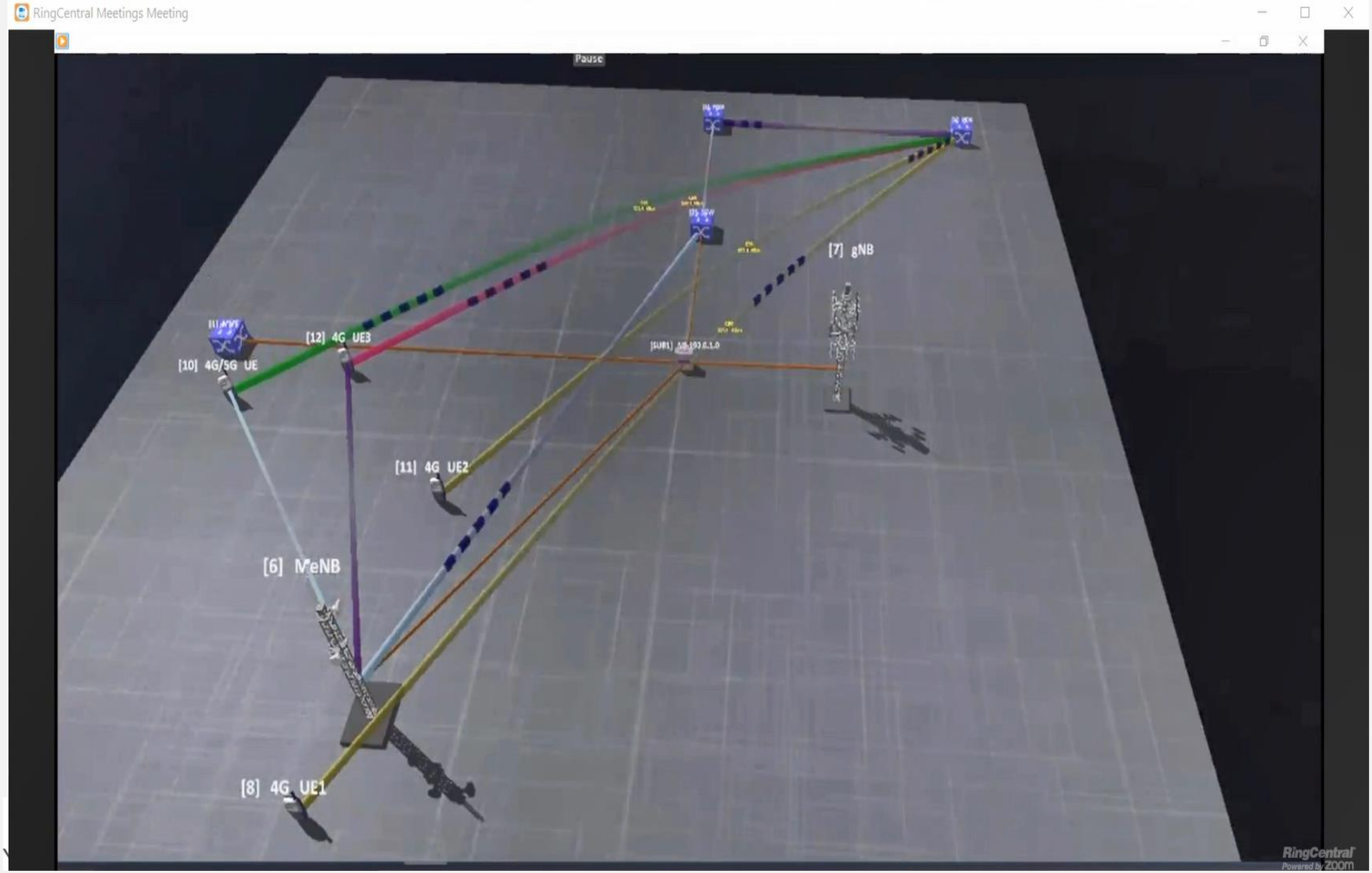
```
Warning in file C:\jenkins\workspace\Exata_Release\exata\interfaces\pas\src\packet_analyzer.cpp:1525
EXata interface not found. Packet Sniffer disabled


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
```

EXata


RingCentral Meetings Meeting
Pause
[12] 4G UE3
[10] 4G/5G UE
[11] 4G UE2
[7] gNB
[6] MeNB
[8] 4G UE1
RingCentral
Powered by zoom

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.

Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

Vaasan yliopisto
UNIVERSITY OF VAASA