European Commission

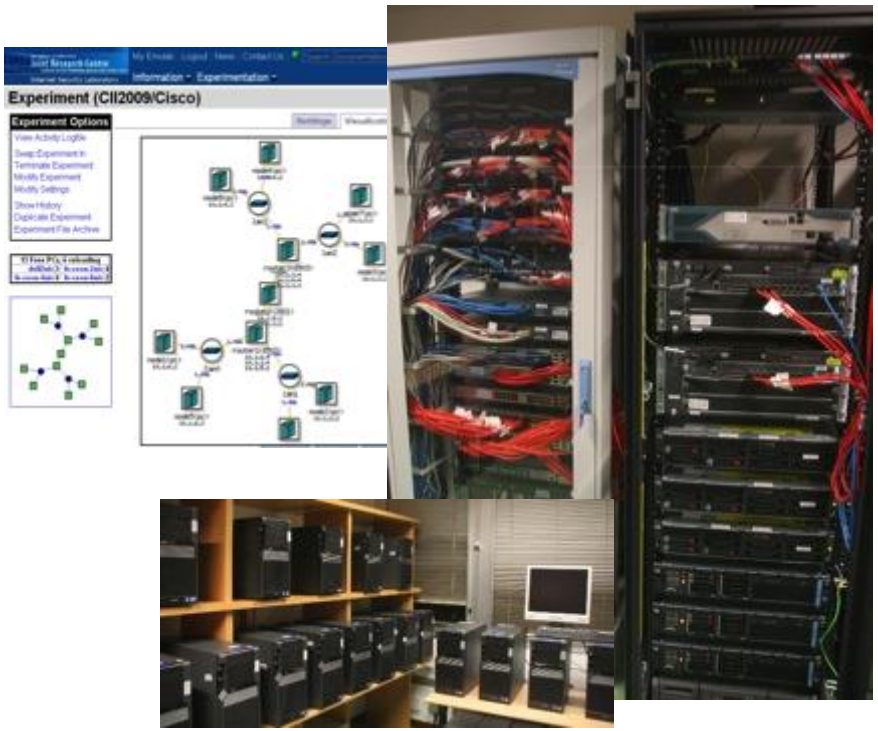
Joint Research Centre

The European Commission's in-house science service

www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

Modelling Cyber-Physical Systems



Neil Mitchison,
Thierry Benoist
Security Technology Assessment Unit

Institute for the Protection and Security of the Citizen (IPSC)

DG Joint Research Centre (JRC)

European Commission

Serving society
Stimulating innovation
Supporting legislation

www.jrc.ec.europa.eu

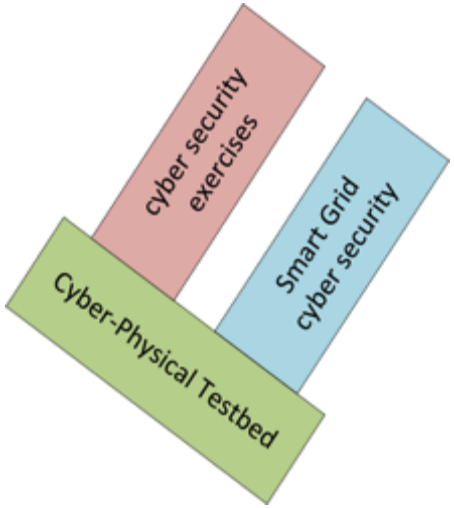
European Commission

Network & Information Security Laboratory (NISlab)

- What is it designed for?
  - Cyber security experiments (botnets, malware, etc)
  - Experimental assessment of cyber infrastructures
  - Technical exercises
  - Technical demonstrations to EU decision-makers

- What are we currently using it for?
  - Security of Cyber-Physical systems: Power Grid, Smart Grid, with emphasis on CI interdependance.
  - Preparedness exercises

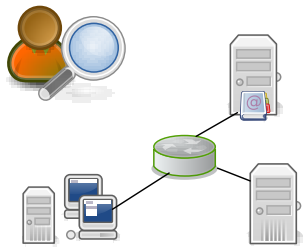
- How is it done?
  - Through EPIC, our in-house emulab flavour



European Commission

Experimentation options with IP networks

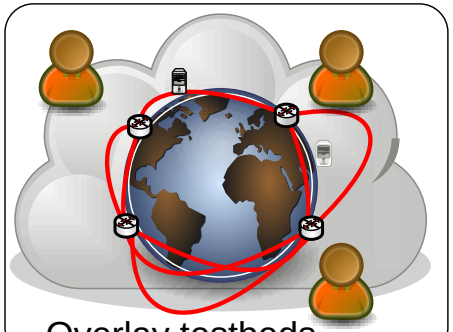
Traditional



Ad-hoc testbeds

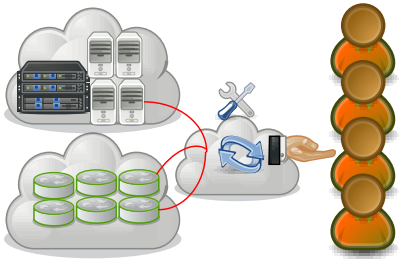
Simulators

Recent



Overlay testbeds

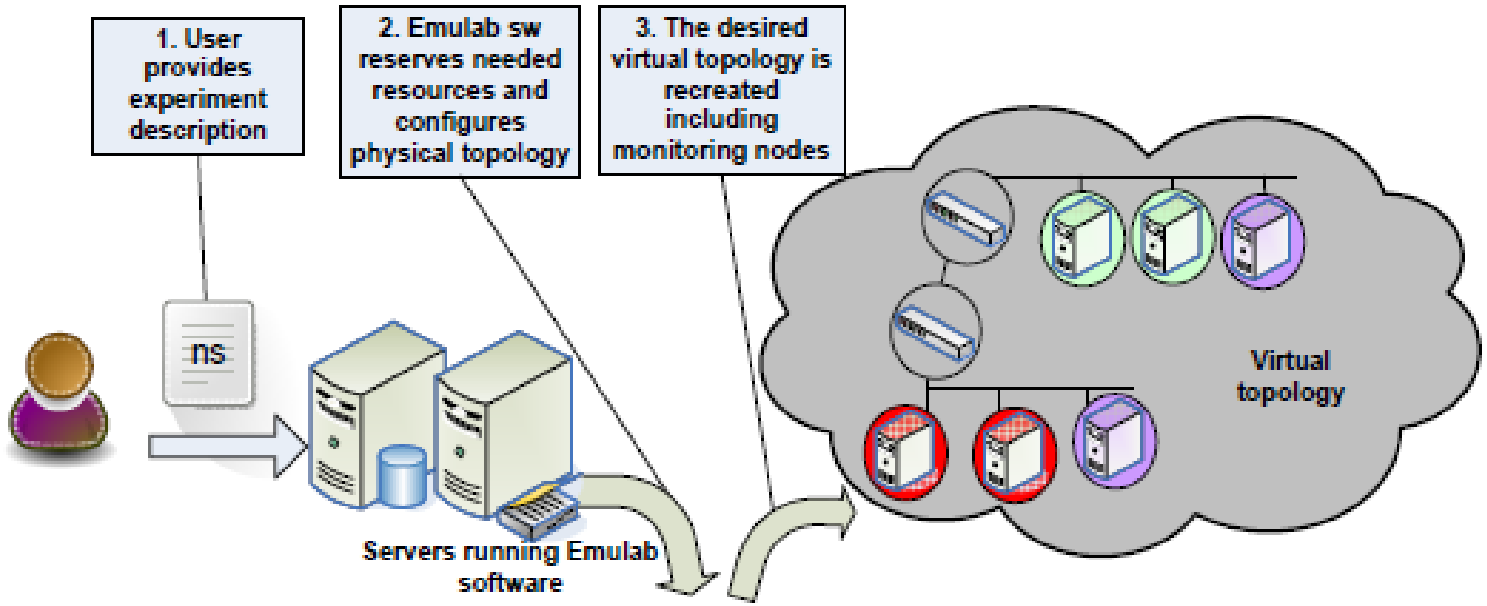
(on top of existing infrastructures)

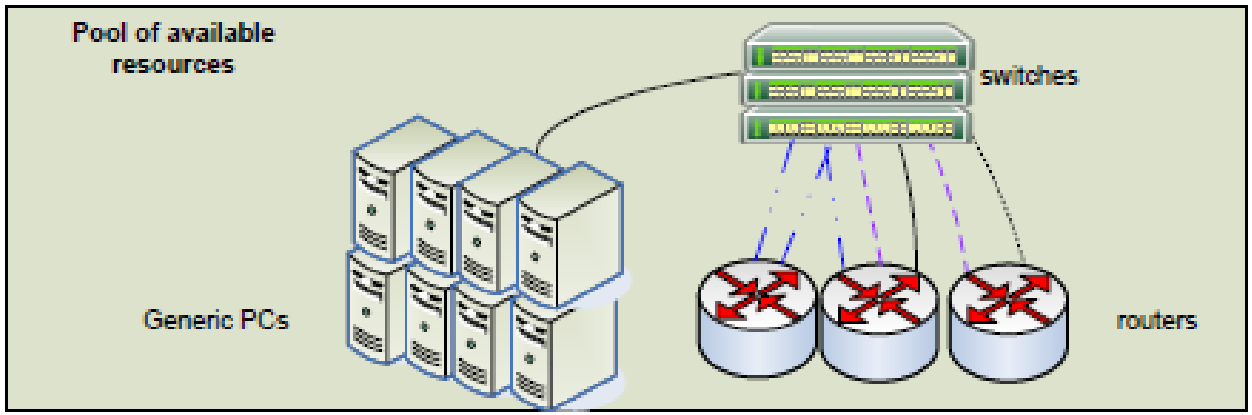


Emulation testbeds

(dedicated physical resources)

EPIC





Advantages:

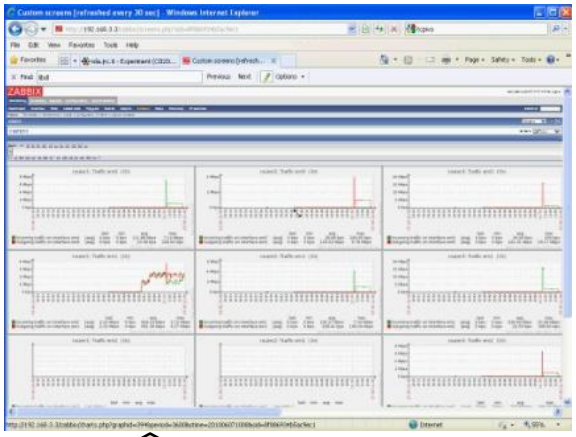
Controllability

Repeatability

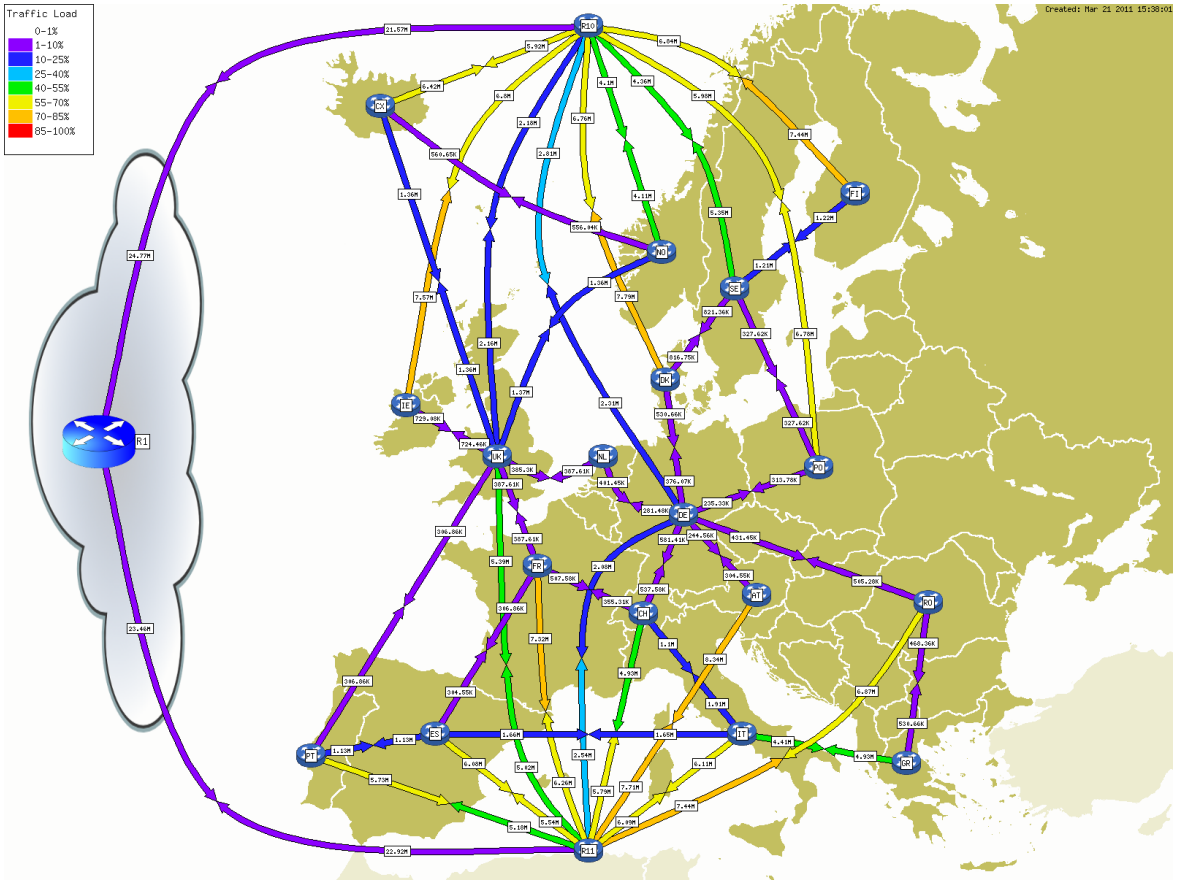
Fidelity

European Commission

Experimental scenario: BGP MiM attack

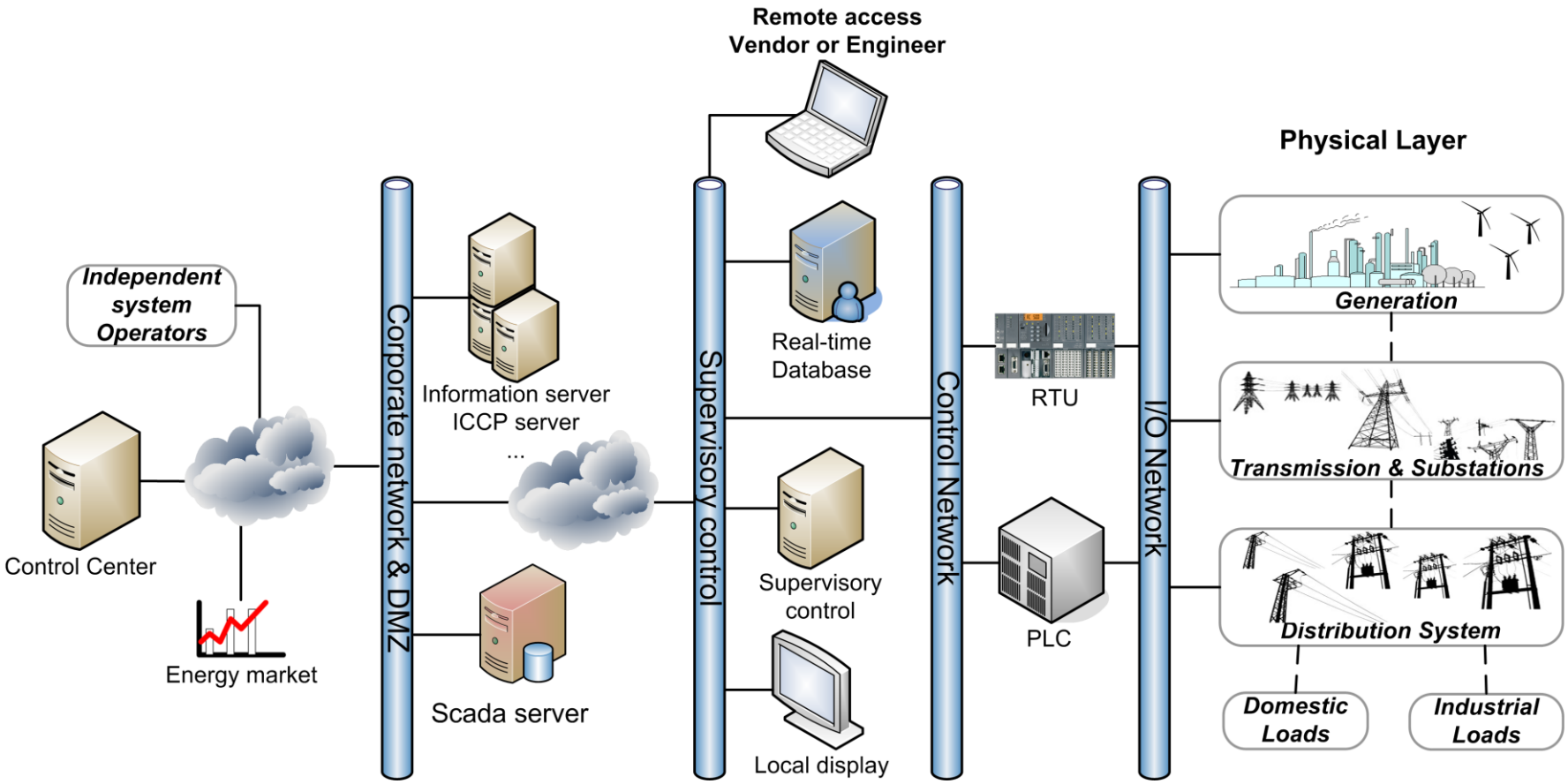


Voice communications / PSTN

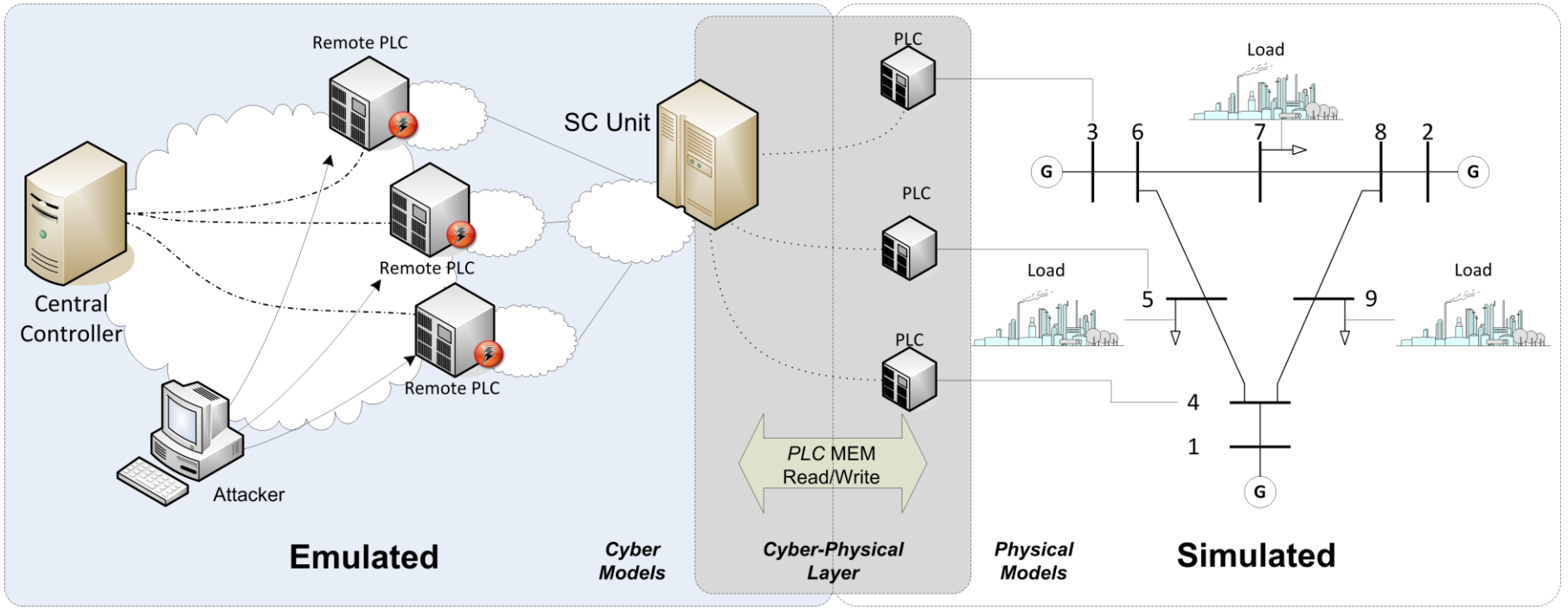


Joint Research Centre

Beyond IP networks… Cyber-physical systems



Hybrid architecture: Emulation + Simulation



Physical layer:

- Soft real-time execution of a model of the physical system

Cyber layer:

- Emulab testbed architecture and software

Cyber-physical layer:

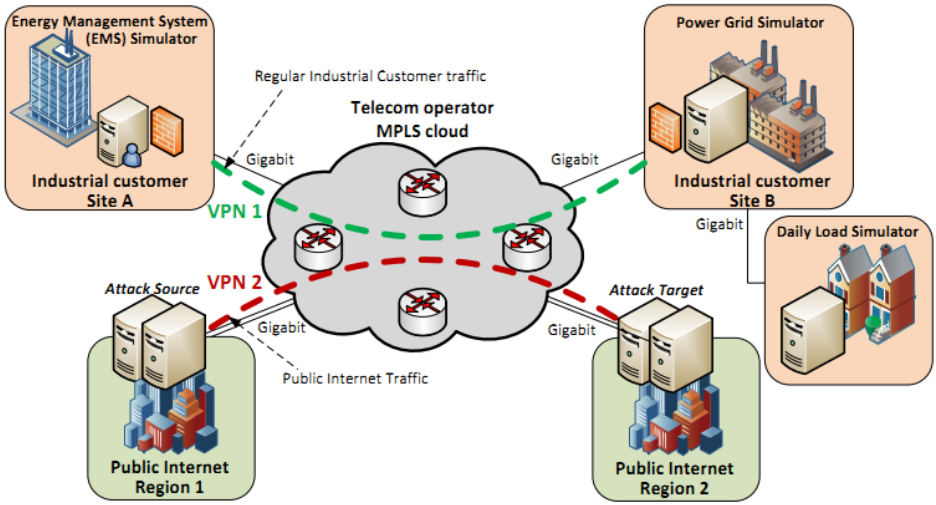
- Provides the "glue" between the two layers

Experimental scenario – DDoS attack

- A telco operator provides
  - internet access to the public and
  - a dedicated connectivity solution to an energy operator linking the Energy Management System (EMS) deployed on site A to the power plant on site B.
- The telco operator uses a shared infrastructure for both services, using a non optimized MPLS setup.
- An internet inbound-outbound DDoS attack will transit through the MPLS cloud.
- The attack increases the latency of between Site A and Site B beyond acceptable parameters, blinds the operator and the EMS →blackout.
- Not even intended!!!

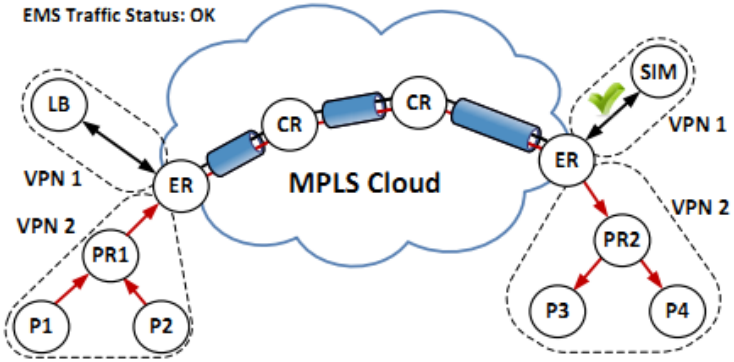
Experimental setup – DDoS attack

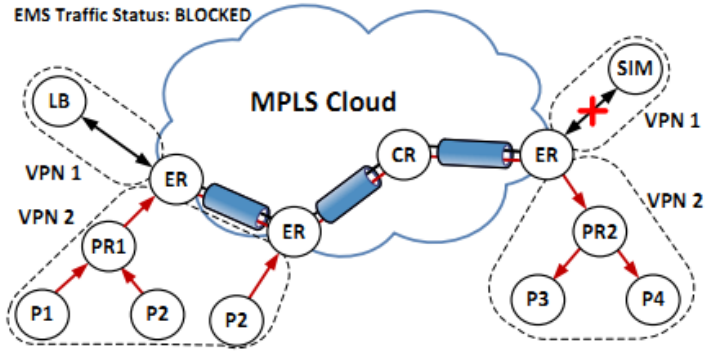
- real-time simulation of an electrical grid, the IEEE 39-bus grid, under typical daily load
- simulation of an Energy Management System (EMS) that used the MPLS network to remotely ensure the voltage stability of the Power Grid
- Emulation of the MPLS network using 4 Cisco 6503 routers
- Public internet emulation: 14 PCs

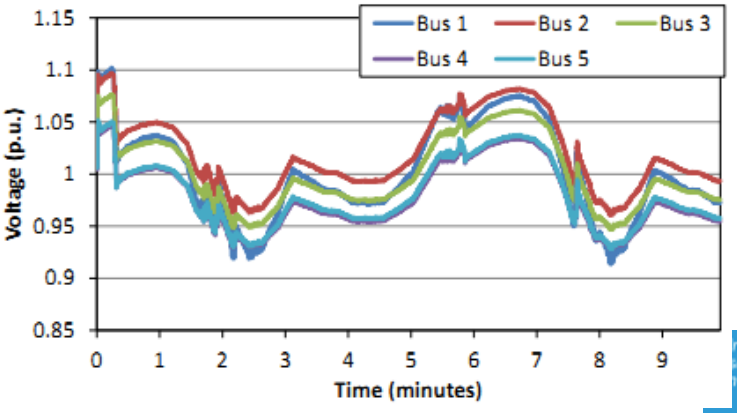


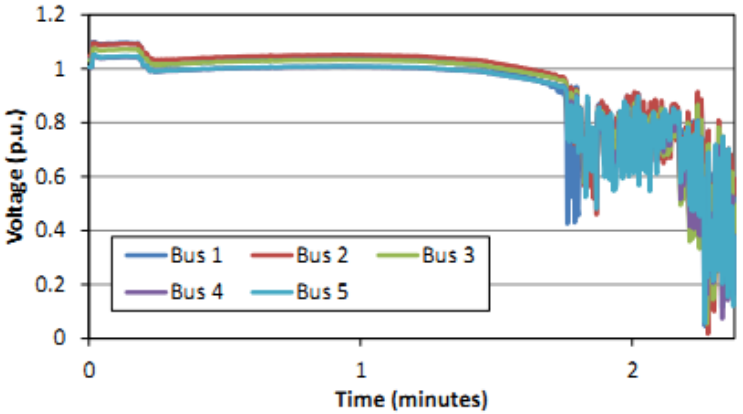
DDoS Attack Impact

- Dual and triple DDoS source with one external router and one/two edge routers









Conclusion

Experimental assessment of **cyber-physical infrastructures security**

- e.g. study the consequences of cyber attacks on the Power Grid

Approach:

- **Simulation for physical components**
- **Emulation with real components for cyber layers**

Advantages:

- Repeatability, flexibility, multi-user platform.
- Using emulation yields more accurate results than simulation.
- Goes beyond IP-only systems for exercising or cybersecurity studies.
- Malware and real cyber components can be used in a safe way
- Cost-efficient approach

European Commission

Thank you !!

" By **failing** to prepare, you're preparing to **fail**"

- Benjamin Franklin

Joint Research Centre