



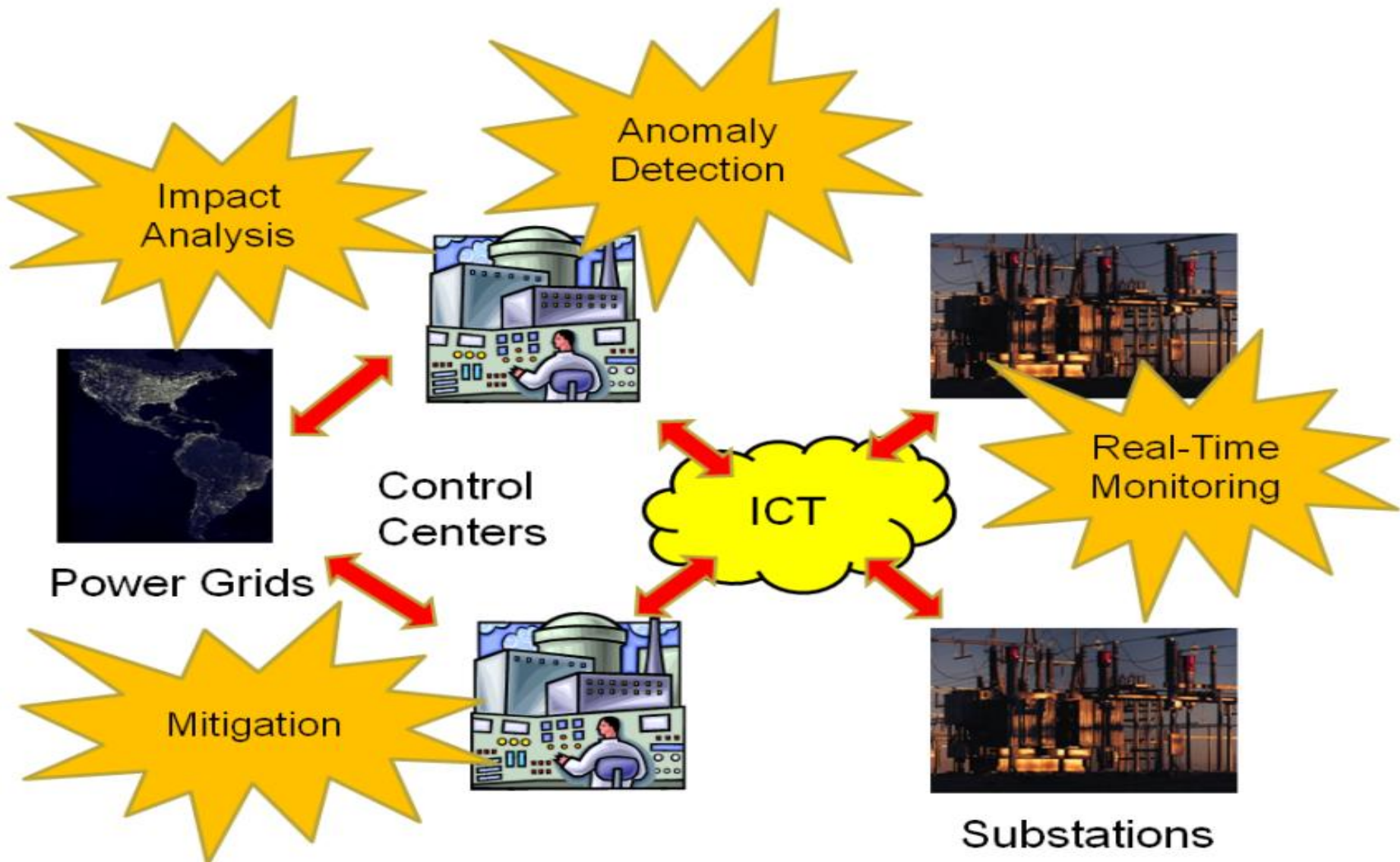
University College Dublin

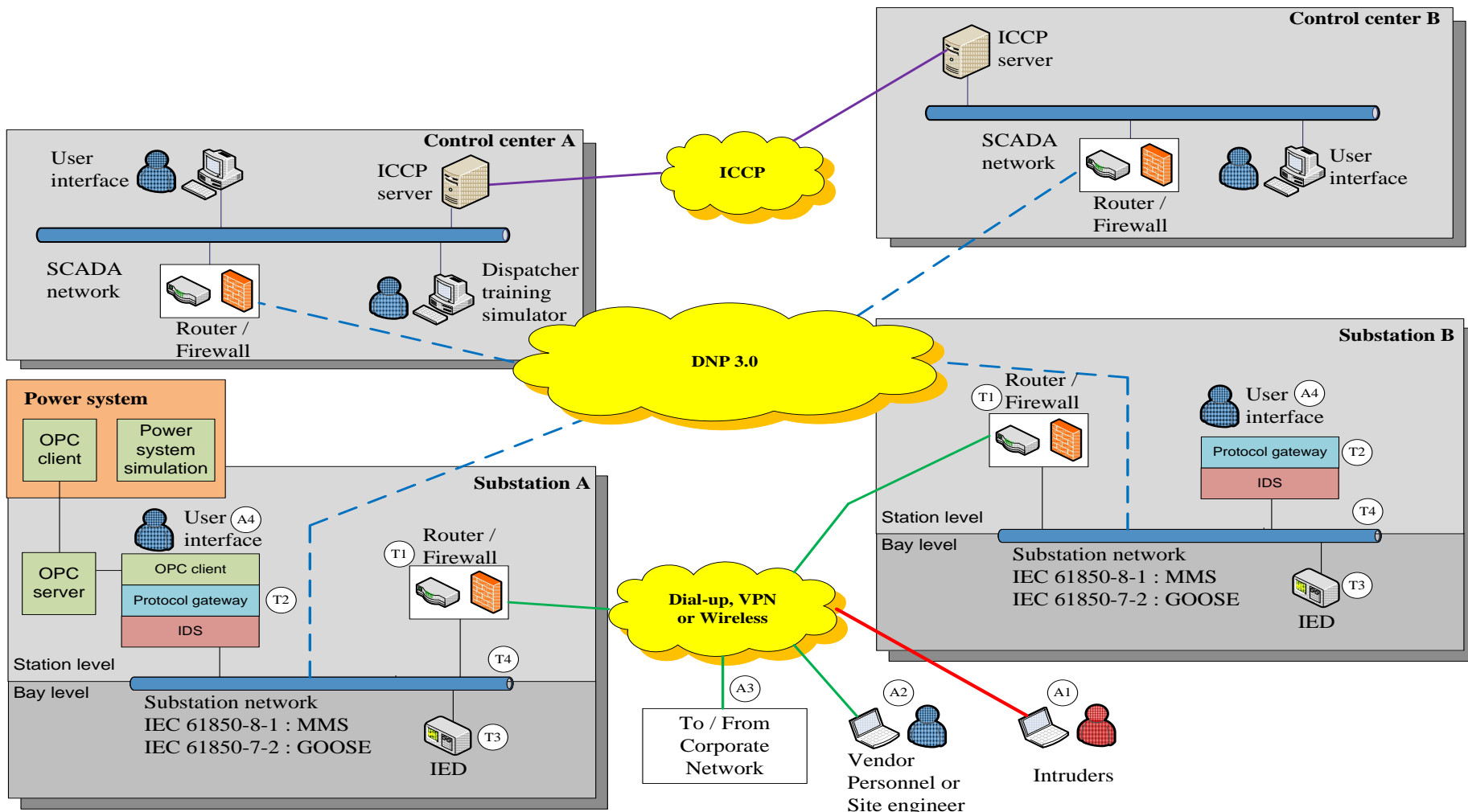
# Cyber Security of SCADA Systems

Alexandru Stefanov  
Chen-Ching Liu

Sponsored by Science Foundation Ireland

- ❖ ICTs on power grids evolved to open, networked environment based on TCP/IP and Ethernet.
- ❖ Firewalls unable to detect insider attacks and connection from trusted side.
- ❖ Most communication protocols do not implement security tech. Data contents can be modified to disturb operability and controllability of the system.
- ❖ Remote access is enabled for Ethernet based networks to allow site engineers, operators and vendor personnel to access remotely.
- ❖ SCADA/EMS and protection/control systems in substations become less isolated, to take advantage of new measurements and control actions.
- ❖ Machines can be infected with viruses, worms, Trojan horses, etc.
- ❖ Stuxnet, Aurora, Night Dragon

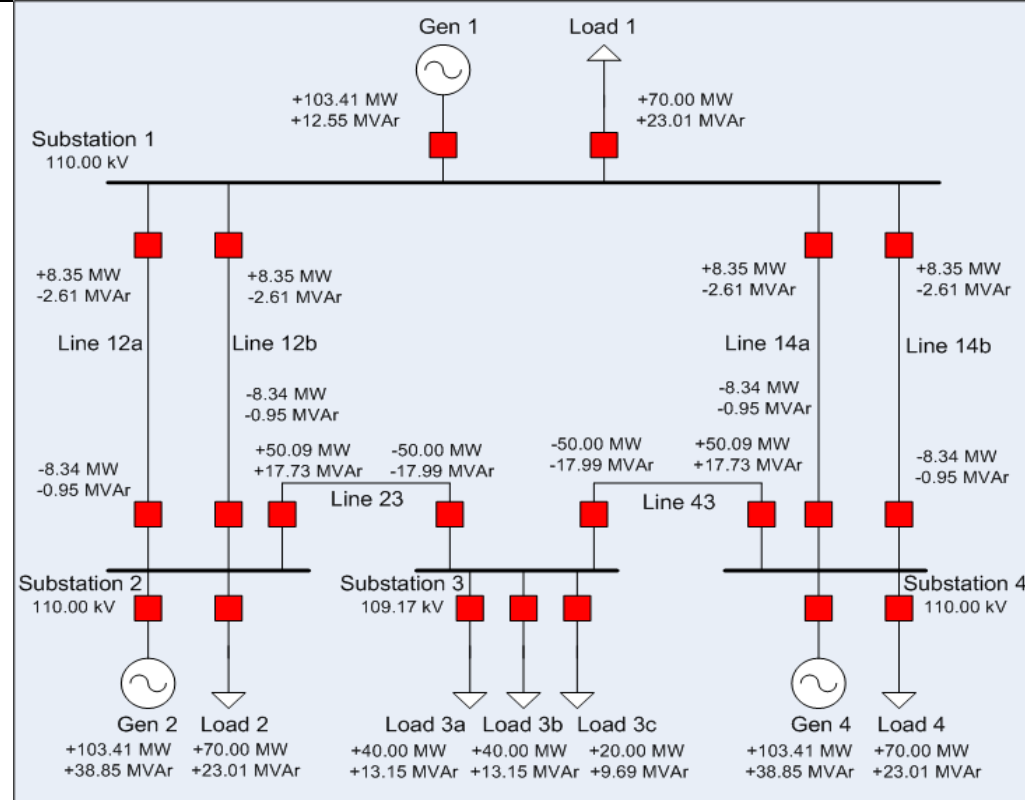
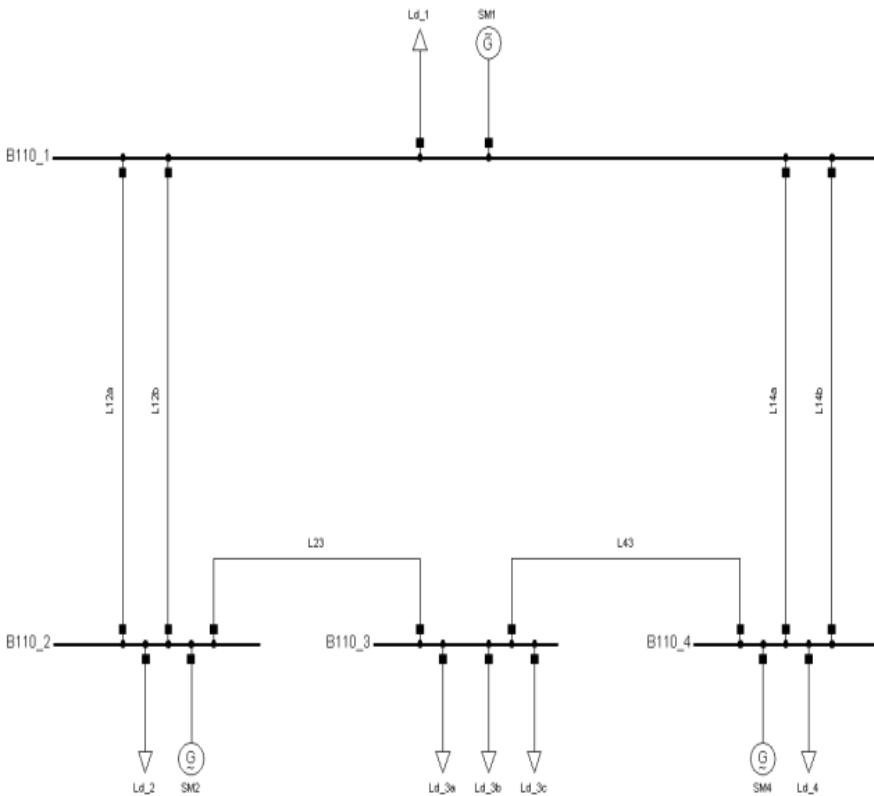




SCADA : Supervisory Control and Data Acquisition  
 ICCP : Inter-Control Centre Communications Protocol  
 DNP : Distributed Network Protocol

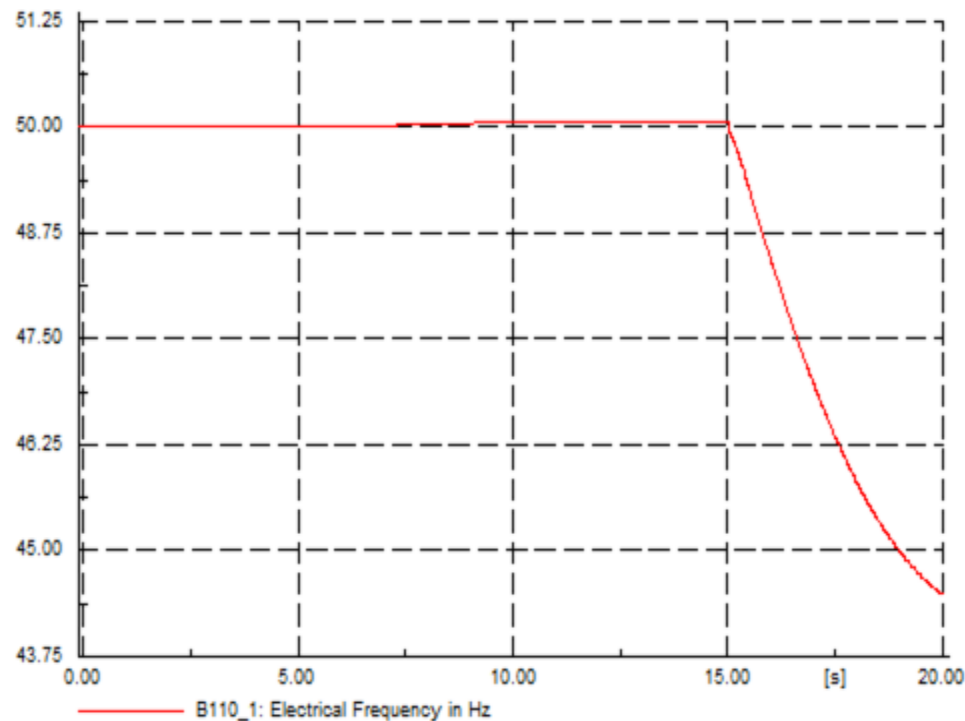
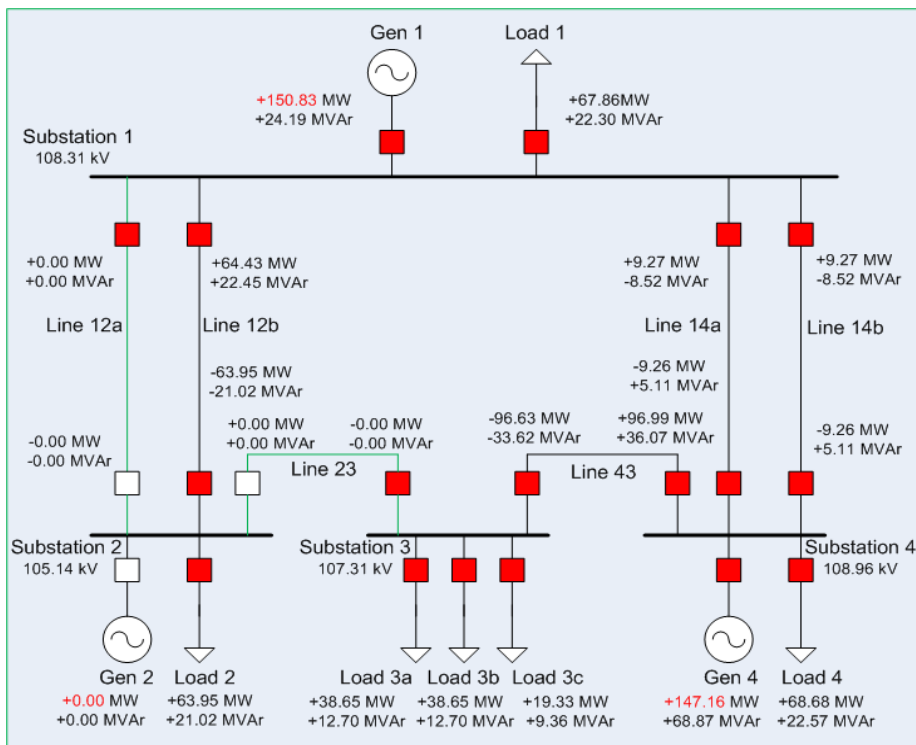
VPN : Virtual Private Network  
 MMS : Manufacturing Message Specification  
 GOOSE : Generic Object Oriented Substation Events

IDS : Intrusion Detection System  
 OPC : OLE for Process Control  
 IED : Intelligent Electronic Device



- ❖ 3 hydro-electric power plants (150 MW each);
- ❖ 6 transmission lines (110 kV);
- ❖ 6 loads.

- ❖ **Intrusion:** An attacker gets access to substation's LAN, using a remote access point and then to LON to control the IEDs.
- ❖ **Cyber attack:** 2 circuit breakers are open and power plant 2 is disconnected.



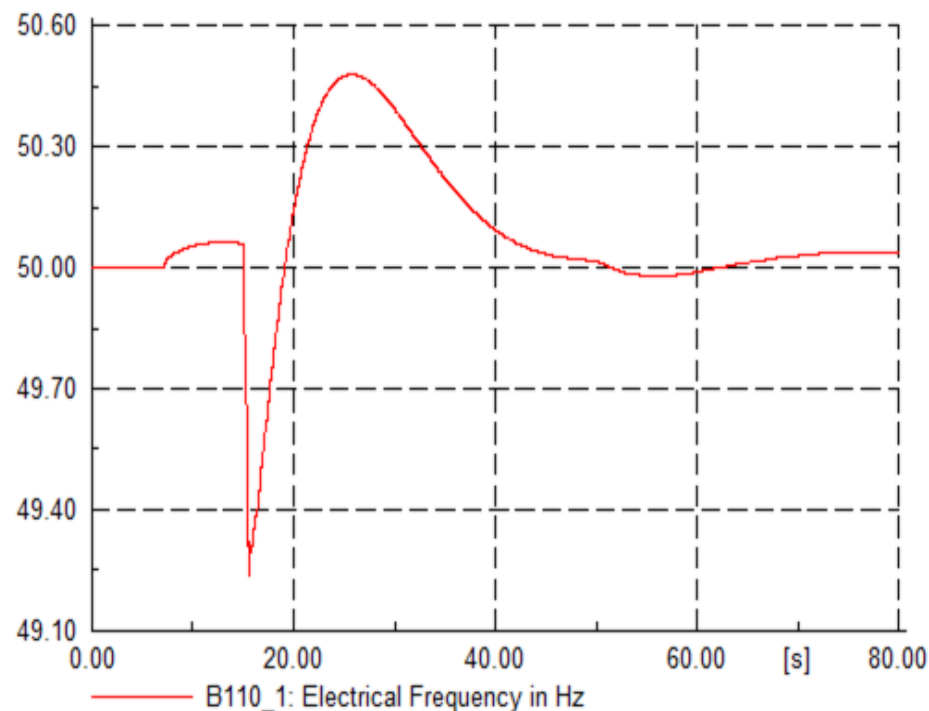
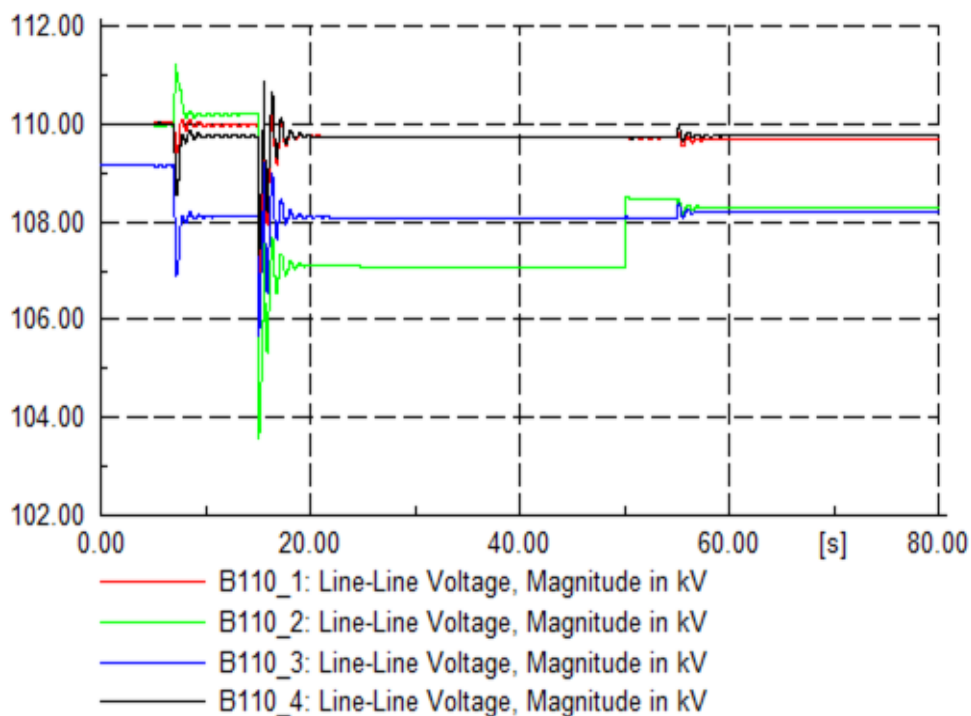
## ❖ IT mitigation strategy:

- Intrusion Detection System (IDS) algorithm finds the anomalies;
- It sends disconnect control commands to the firewall;
- The firewall blocks the intruder's connection.

## ❖ Power System mitigation strategy:

- Monitor the real-time data;
- If there are constraint violations, an **optimization problem** will be defined;
- Compute Optimal Power Flow (OPF);
- Control actions are implemented.

- ❖ Intruder is disconnected by the collaboration between IDS and firewall in the substation network;
- ❖ Compute OPF algorithm (minimize load shedding costs);
- ❖ Loads 1 and 2 should be shed by 100%, 52% respectively.



- ❖ Model the cyber-physical power system;
- ❖ Monitor the interactions between ICT and the power grid;
- ❖ Assess SCADA vulnerabilities;
- ❖ Create cyber intrusions and attacks;
- ❖ Perform simulations using time domain tools;
- ❖ Develop mitigation techniques to stop the attack and restore a normal operating condition.

## **New technology for highly secured SCADA:**

- ❖ Intrusion Detection Systems;
- ❖ Highly-effective firewalls;
- ❖ Vulnerability assessment tools.

Thank you!