AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE,
L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

Modeling the loss of controllability and observability of electrical grids under SCADA cyber attacks

E. Ciancamerla, B. Fresilli, M. Minichino, S. Palmieri, T. Patriarca
ENEA

SCADA Cybersecurity Workshop
Luxembourg, 10th March 2014

Summary

- **Introduction**
  - SCADA system
  - SCADA vs cyber attacks
- **SCADA cyber security**
- **Reference scenario**
  - Fault Isolation and System Restoration (FISR) service
  - Electrical grid, SCADA and corporate network
  - a single heterogeneous network (power grid, corporate network, SCADA)
- **Cyber attacks & models**
  - Worm
  - DoS
  - MITM
- **Impact of Cyber Attacks on SCADA and electrical grid QoS**
  - numerical indicators
  - simulation results
- **Limits of models: towards test bed and models integration**

- **SCADA (Supervision Control and Data Acquisition)**
  - nervous system of Electrical grids
  - communication links dependent on (public/private) Telco networks
  - mutual propagation of disturbances and adverse events between Power grids and Telco networks

- **loss/degradation of SCADA services impacts on QoS to power grid customers**

SCADA vs Cyber attacks

- The complexity and the de-isolation of SCADA systems leaves many cyber vulnerabilities as well as vectors for attacks;
- Cyber vulnerabilities involve computers, communications (Telco and SCADA networks) and intelligent sensors/actuators distributed over the power grid;
- Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously;

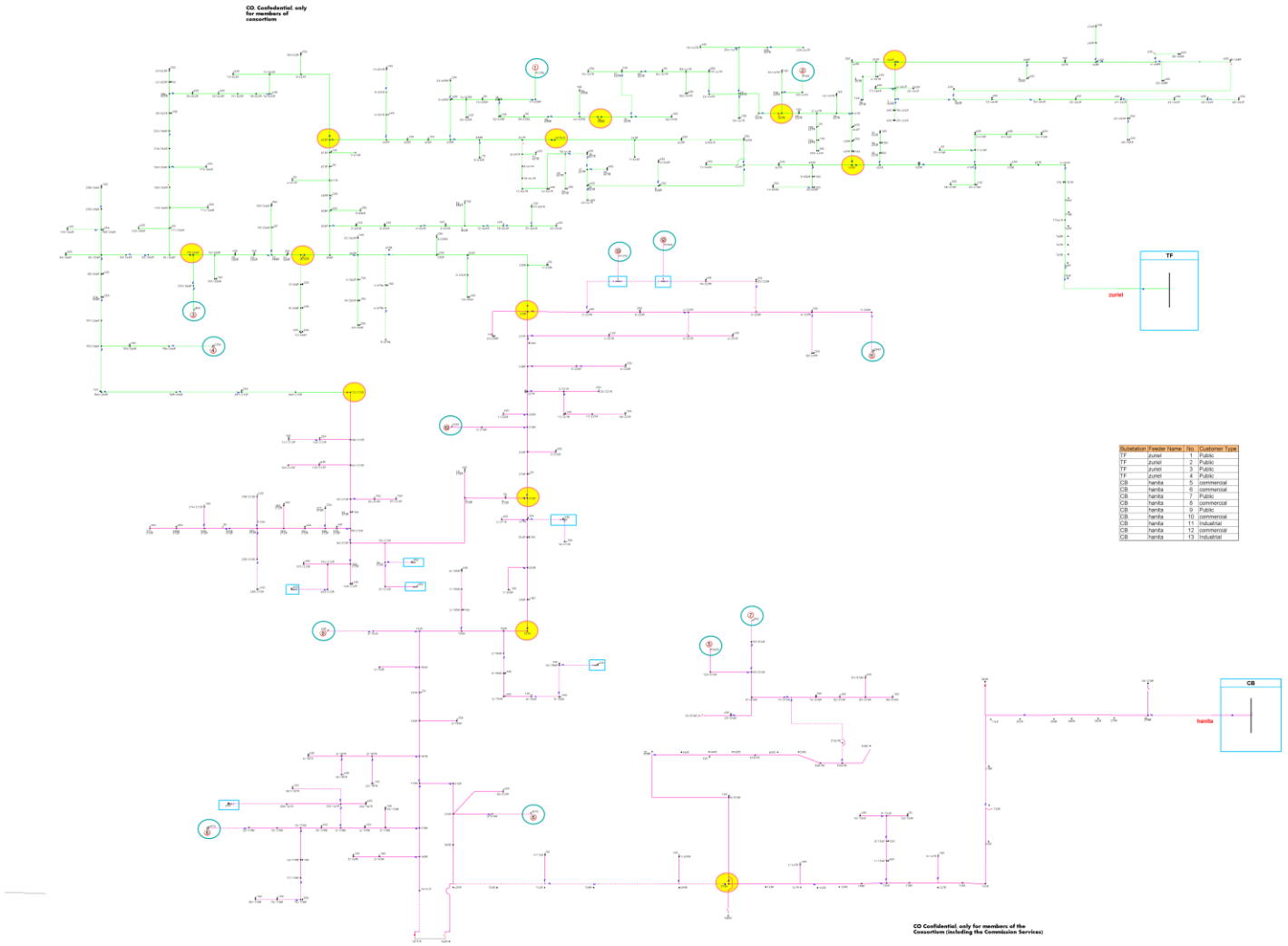
- Once a vulnerability has been exploited specific adverse actions can performed
  - Addition of software infected with malware
  - DoS (Denial of Service)
  - Man-In-The-Middle (MITM): Changes to instructions, commands

FISR service performed by SCADA operator

- In electrical grids, failures may cause the de-energisation even of large part of power customers and need to be located, isolated and repaired quickly and safely.
  - Failure location consists in the progressive re-energisation of electrical sections of the grid, by closure/aperture of circuit breakers, starting from the most upstream section of the grid to the most downstream section of the breaker originally tripped.
  - The process ends when the feeder protection at substation is activated and the faulty section is located and isolated.
  - Finally, on the repair of the faulty section, the grid is restored to its original configuration.
- FISR: Fault Isolation and System Restoration - procedure is based on grid monitoring, sensing of loss of power, circuit breakers operations, performed throughout Remote Terminal Units (RTUs).

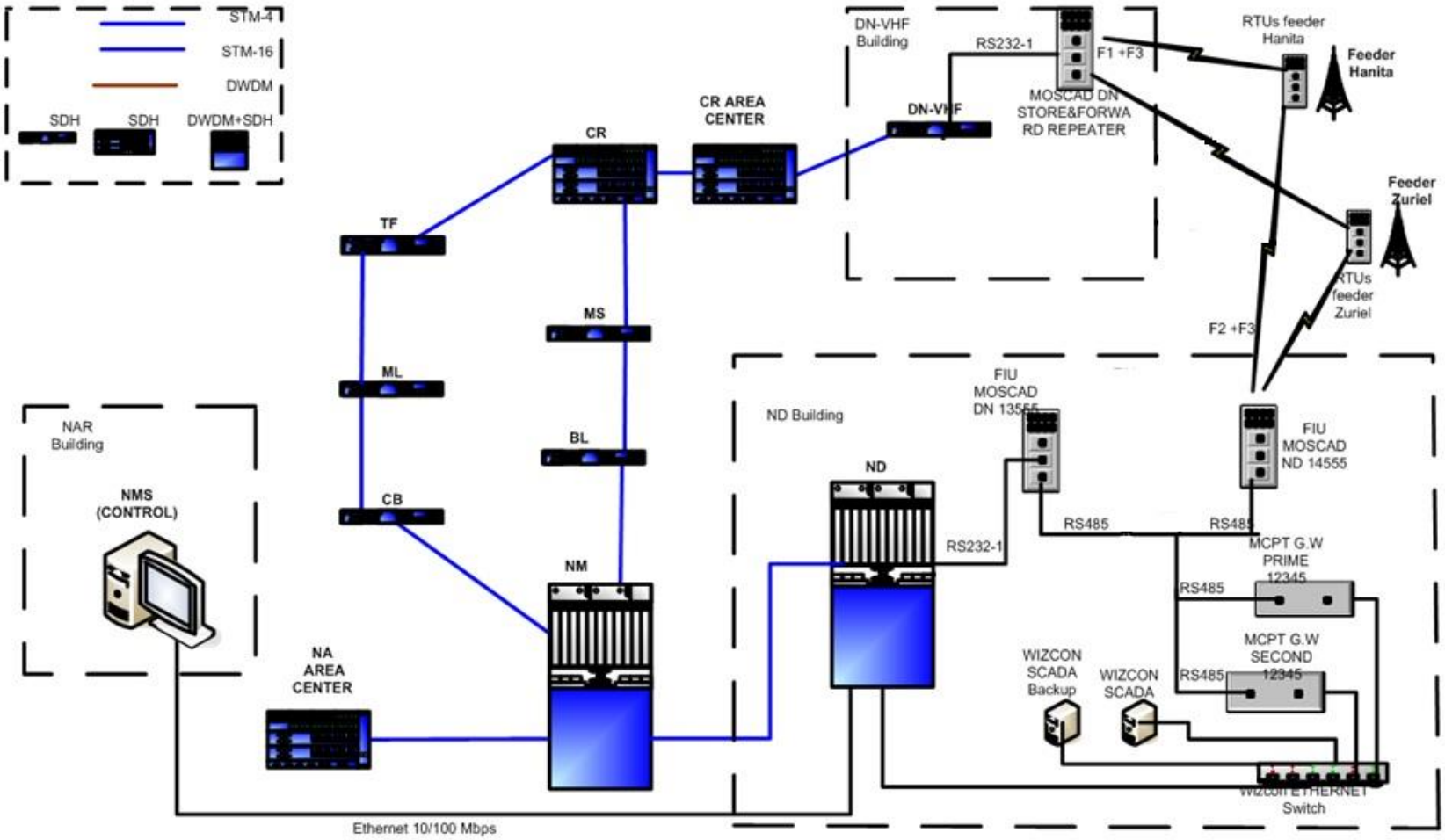
FISR degradation affects the quality of electricity supplied to grid customers

Interconnected networks supporting FISR:
Electrical 22 KV grid portion



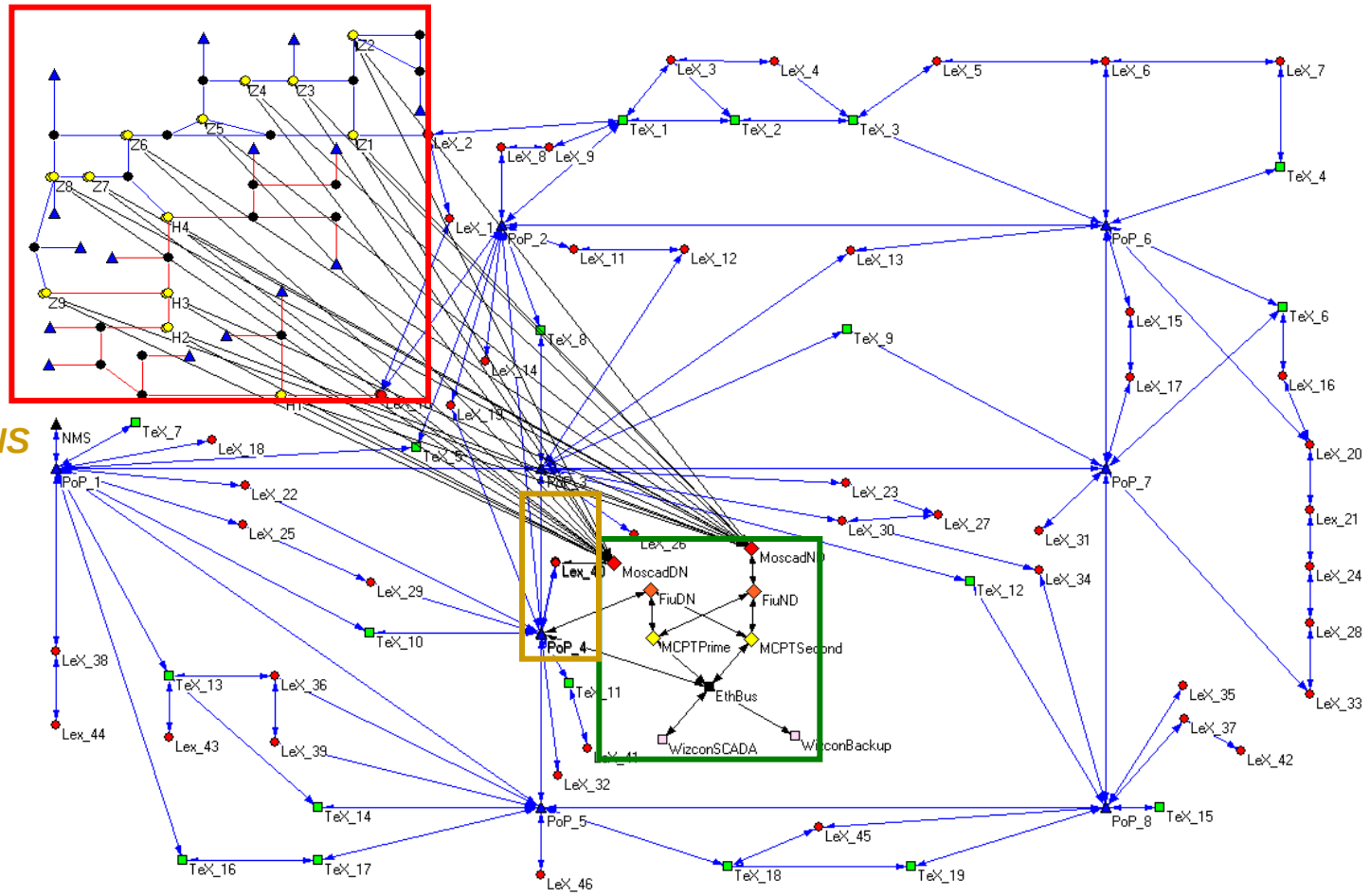
Substation	Feeder Name	No.	Customer Type
TF	zuriet	1	Public
TF	zuriet	2	Public
TF	zuriet	3	Public
TF	zuriet	4	Public
CB	hamita	5	commercial
CB	hamita	6	commercial
CB	hamita	7	Public
CB	hamita	8	commercial
CB	hamita	9	Public
CB	hamita	10	commercial
CB	hamita	11	Industrial
CB	hamita	12	commercial
CB	hamita	13	Industrial

Interconnected networks supporting FISR:
SCADA and Communication network



A single heterogeneous network supporting FISR

Power grid, SCADA system, Telco network



INTERCONNECTIONS

SCADA and Telco

Telco and HV grid

RTUs, SCADA and Telco devices energised by Power grid by means of emergency power supply systems

Grid observability from SCADA limited to FISR service

We need a very simple model of the grid:

- **its topology: Substations, Trunks, Loads, Junctions, RTU Breakers**

RTU Breakers (N.O. & N.C) operation (open/close) from SCADA centre

Flows (ON/OFF) from Substations to loads, according to Junctions and RTU breakers position

Electrical failures implying the automatic opening of the protection devices of the feeding substation

Risk of loss/degradation of FISR service

The degradation/loss of FISR service performed by SCADA operator, is critical because it is strictly correlated to the quality of power supplied to customers.

A timely actuation of FISR service, consequential to a permanent failure of the grid, reduces the outage duration

The time response of *FISR s*ervice,

affects the quality of electricity , in terms of (reliability indexes)

- SAIDI
- SAIFI
- CAIFI

by NS2 open source simulator

Cyber attack models

- Worm propagation
- Denial of Service (DoS)
- Man-In-The-Middle (MITM)

Results:

- before the attack, normal conditions
- during the attack, anomalous conditions
- after the attack, tail of anomalous conditions

Impact of cyber attacks on SCADA and electrical grid

cyber attacks targeted at a source node may spread throughout SCADA and corporate network nodes up to affect (i.e. disconnect) the primary and the redundant communication between SCADA Control Centre and its RTUs

Cyber attacks: Worm

- A malware (MALicious softWARE) that infects a computer and is able to infect other computers without the user intervention

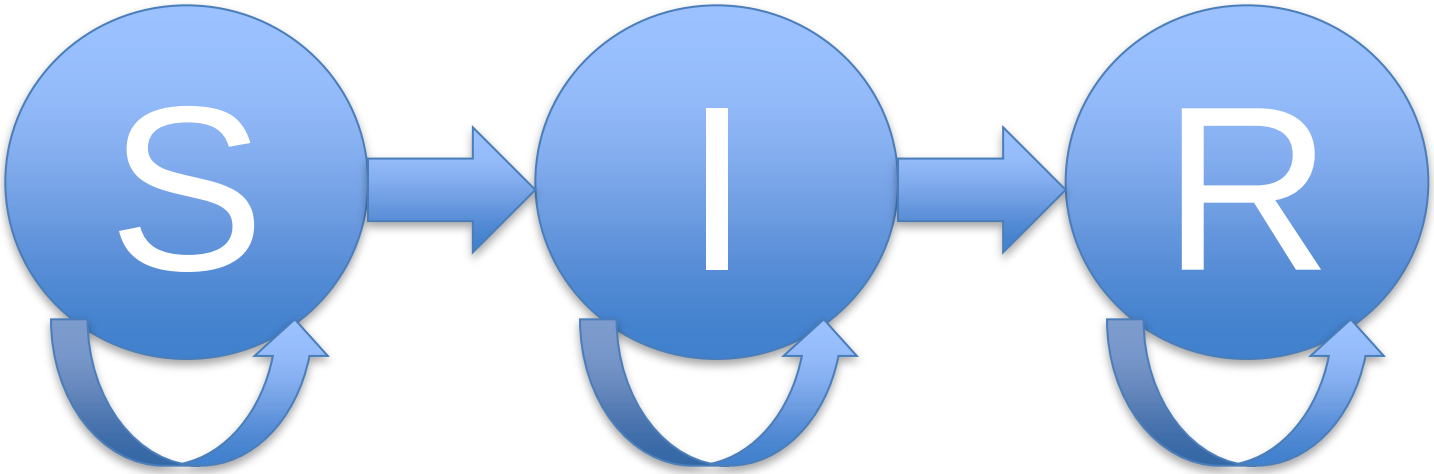
- Once a computer is infected, it is under the control of the attacker, in our model, an infected node goes in DoS

Malware and its spreading throughout corporate network and SCADA by SIR epidemic model

- Malware (**mal**icious soft**ware**) is software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems;

- malware spreads itself from computer to computer similarly to epidemics for biological populations

SIR model



- Node is healtly
- Malware can reach it

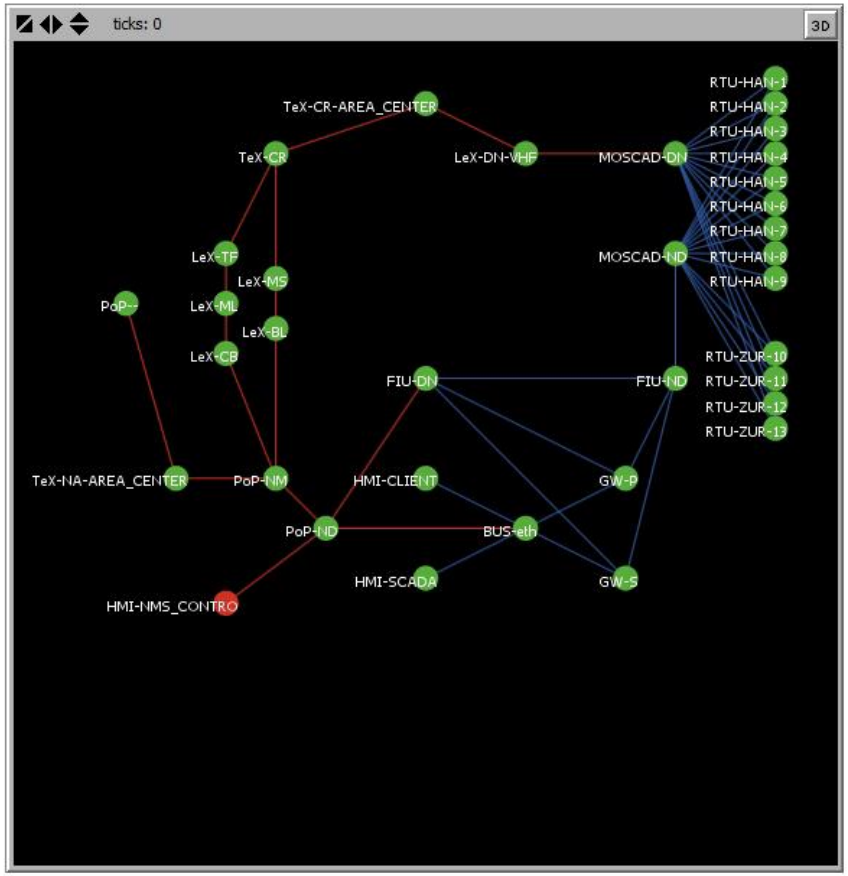
- Node is infected
- Malware controls it

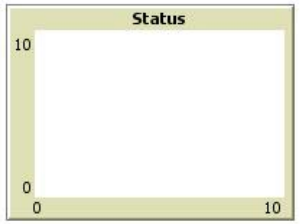
- Node is resistant
- It is immune to malware

Malware spreading algorithms

- Classic SIR epidemic models considers all individuals equals, with the same tendency to become infected
- Our model considers each node, which represent an ICT device, with its own different tendency to become infected
- To remove an infection, it's necessary an antivirus scan with a certain probability of success in finding and removing the malware

NetLogo: SIR implementation





Green: susceptible
Red: infected
Grey: resistant

Impact of Cyber attacks on SCADA: numerical indicators

a) *LoV,* Loss of View - if the SCC can't receive packets from the RTUs.
In case of MITM, SCC receives false information/data from the attacker and the consequent false observability of the electrical grid from SCC may induce a tricky behavior of SCADA operator;

b) *LoC* , Loss of Control - if the RTUs can't receive packets from the SCC.
In case of MITM, the RTU receives false commands from the attacker instead of SCC;

c) DPR, Dropped Packet Rate - a global vision of how many packets are missing;

d) TTBP, Transmission Time Between two Packets;

e) RTT , Packet Round Trip Time - composed by TCP transmission time plus ACK transmission time;

c) Packets routing.
It changes in case of MITM

FISR response time

- **FISR response time is intended as the time between the occurrence of loss of electricity supplied to customers (due to a grid failure) and the restoration of elecricity to customers**

- The time response of FISR service is critical because it is strictly correlated to the quality of power supplied to customers.

  – A timely actuation of FISR service, consequential to a permanent failure of the grid, reduces the outage duration and then contributes to keep indicators of quality of power supplied to customers within prefixed values

  – On the contrary a delayed actuation of FISR service gets worst such indicators

- A delayed actuation of FISR service occurs when data and control messages are exchanged between SCADA Control Center and RTUs outside a preassigned time threshold.

Impact of Cyber Attacks on Electrical Grid

FISR response time on malware spreading, MITM and DoS attacks by NS2

Percentage of grid customers which remain isolated

Failure Section		Initial	Intermediate	Terminal
Response Time [sec]	Case 1	18,4	34,8	29,1
	Case 2	18,6	35,2	29,4
	Case 3	> simul. Time	> simul. Time	> simul. Time
Affected Customers [%]	Before FISR	46,6	26,6	26,6
	After FISR	0	0	6,6

FISR response time and % of affected grid customers

for three different sections of the permanent failure on the power grid:

i) failure in an initial section of the grid (bounded by the feeding substation and its closest RTU): the loads of failed sub-grid are energized by the other substation, up to the manual repair, that restores the initial configuration of the grid;

ii) failure in an intermediate section of the grid (bounded by two RTUs): the loads into this section are isolated, the loads bounded by failed the section and the tie switch are powered by the other substation, up to the manual repair, that restores the initial configuration of the grid;

iii) failure in a terminal section of the grid (bounded by RTU and loads): the loads of failed section are isolated, up to the manual repair, that restores the initial configuration of the grid.

for different operative conditions of SCADA system and corporate network:

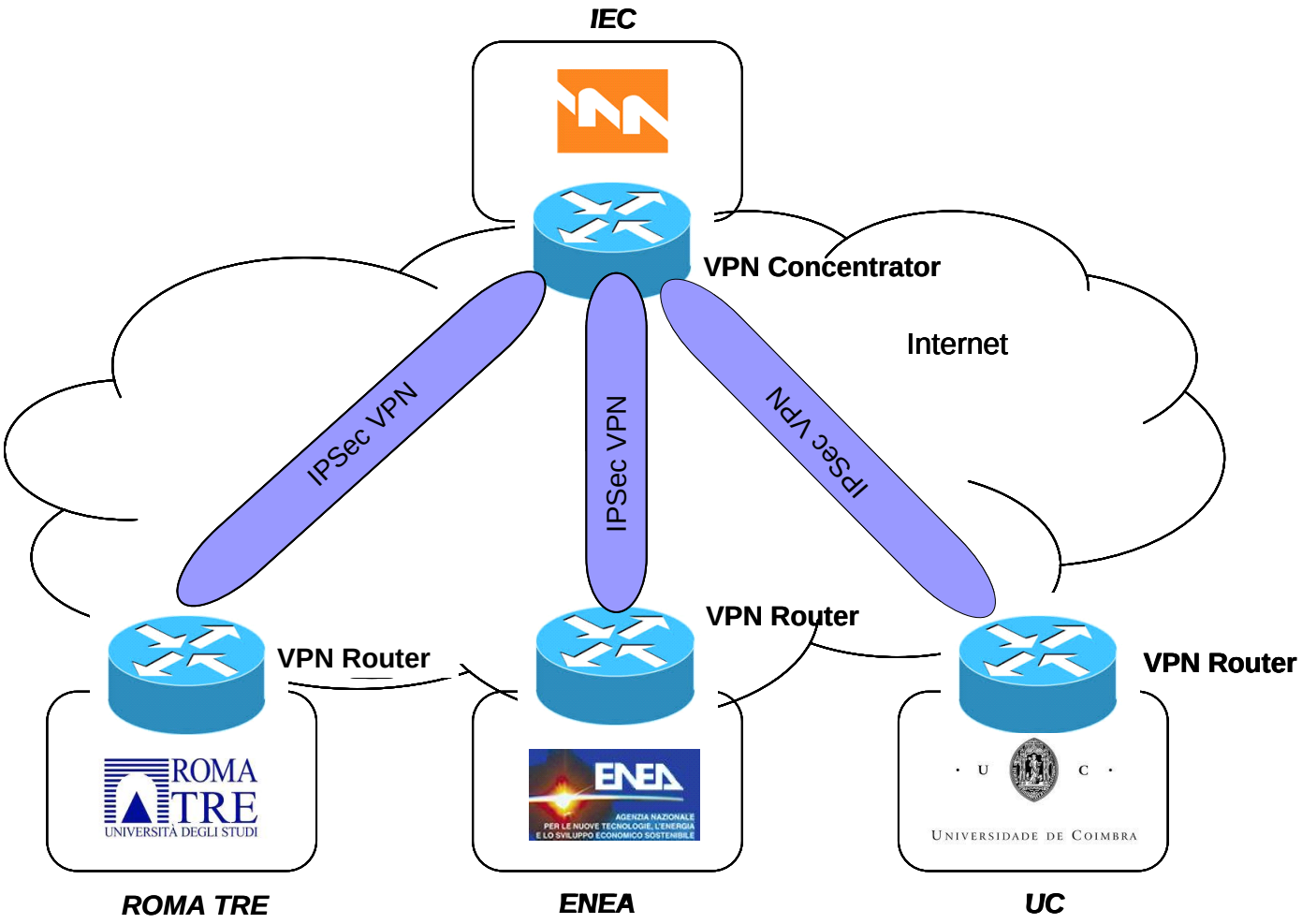
case 1) normal condition of the SCADA system and corporate network under initial infection spreading;

case 2) the infection spreading gets out of service the primary connection between SCADA Control Centre and RTUs;

case 3) on failure of the primary connection between SCC and RTUs, any cyber attack (Malware or DoS OR mitm) gets out of service the back up connection between SCC and RTUs;

- The operator looses the grid observability and controllability as final consequence of the attack.

Limits of models: towards test bed and models integration



Limits of models: towards test bed and models integration