La Qualità del Servizio delle Reti Elettriche sotto attacchi informatici ai loro sistemi di Telecontrollo (SCADA)

E. Ciancamerla, M. Minichino
ENEA
The research activity has been funded by different EU projects, the last one is EU FP7 CockpitCI project: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures.

CockpitCI tool:
- predicts, detects, analyzes and reacts to cyber attacks on SCADA system which controls a Medium Voltage electrical grid.

ENEA:
- is responsible of models to predict QoS of an electrical grid under cyber attack on its SCADA system, which intend to support CockpitCI tool.
- provides a core contribute for CockpitCI tool validation.
• **Introduction**
  – SCADA system
  – Cyber security in SCADA
  – SCADA vs cyber attacks

• **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 modelling approach and Hybrid Test Bed**

• **Conclusions and future work**
• **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**

**Introduction**
Cosa controlla lo SCADA?

Interruttore di manovra sezionatore in sottostazione AV/MV (centro ENEL di Aquila)
Cosa controlla lo SCADA?

Trasformatore AV/MV (i.e. TAPS di regolazione tensione)
(centro ENEL di Aquila)
Cybersecurity in SCADA

FACT: Evolution from proprietary and closed architectures to open, standards-based solutions for ICS-based infrastructure

CONSEQUENCE: Cyber-attacks can come from any part of the infrastructure:

1. FIELD Network as SCADA systems
2. OPERATION Network as Telco system or monitoring/management system
3. IT Network as enterprise devices and services

and can target any part of it
SCADA versus cyber attacks

• Once a vulnerability has been exploited specific adverse actions can performed

  – **Worm propagation**: it spread throughout network connection and its effect is disconnect the communication between Control Server SCADA and its field components (PLC/RTU)

  – **Denial of Service (DoS)**: the attacker send a lot of service requests in a short time to the server and so slow down the server resources

  – **Man In The Middle (MITM)**: Changes to instructions, commands; the attacker intercepts the traffic between two SCADA devices (e.g. HMI and Control Server SCADA or Control Server SCADA and PLC), which believed to exchange information with the legitimate interlocutor, but indeed the attacker may sniff the information and/or send false messages (e.g. sniffing SCADA login/password, view or modifying command or data monitoring)
Reference scenario

- limits the extension of the real word
- provides a concrete context of operation focused on interdependencies
- consists in identification of
  - service
  - sequences of adverse events including cyber attacks that may impair QoS, in terms of continuity, readiness, time response
  - interconnected networks supporting the service
  - interconnections among networks and systems
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
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
Modelling assumptions on SCADA and corporate network

### Assumptions on corporate network

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Backbone (DWDM)</th>
<th>TeX (STM-16)</th>
<th>LeX (STM-4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>10 Gbps</td>
<td>2.5 Gbps</td>
<td>600 Mbps</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>TCP+UDP</td>
<td>TCP</td>
<td>TCP</td>
</tr>
<tr>
<td>Traffic Bit-Rate</td>
<td>12 GB (TCP) + 8 GB (UDP)</td>
<td>12 GB</td>
<td>12 GB</td>
</tr>
<tr>
<td>Type of Agents</td>
<td>CBR for UDP</td>
<td>FTP for TCP</td>
<td></td>
</tr>
<tr>
<td>Number of Agents</td>
<td>100 for UDP</td>
<td>100 for TCP</td>
<td></td>
</tr>
</tbody>
</table>

### Assumptions on SCADA communication links

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Ethernet</th>
<th>RS-485</th>
<th>RS-232</th>
<th>VHF-radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>100 Mbps</td>
<td>19.2 Kbps</td>
<td>19.2 Kbps</td>
<td>4.8 Kbps</td>
</tr>
<tr>
<td>Source/Destination Node</td>
<td>SCADA - MCP_T – PoP</td>
<td>MCP_T-FIU</td>
<td>RF modem - Telco Nodes</td>
<td>RF modem - RTU</td>
</tr>
<tr>
<td>Traffic type</td>
<td>DLC (TCP)+ TCP</td>
<td>DLC (TCP)</td>
<td>DLC (TCP)</td>
<td>DLC (TCP)</td>
</tr>
<tr>
<td>Traffic bit-rate</td>
<td>256 bytes /30 sec</td>
<td>256 bytes /30 sec</td>
<td>256 bytes/30 sec</td>
<td>256 bytes /30 sec</td>
</tr>
</tbody>
</table>
### Cyber attack use cases

**Attack type:**
- Denial of Service (DoS),
- Man in The Middle (MITM)
- Malware spreading

**Attack sources:**
- SCADA devices
- Corporate network devices
- Internet

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Attack initiated from</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>SCADA device</strong></td>
</tr>
<tr>
<td>Malware spreading</td>
<td></td>
</tr>
<tr>
<td>DoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>MITM</td>
<td>Case 7 - between BUS and GW Prime</td>
</tr>
<tr>
<td></td>
<td>Case 8 - between MOSCAD1 and RTU1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Consequences on electrical grid:**
- loss/false observability & controllability of the electrical grid
- degradation of reliability indicators of the electrical grid
Malware (malicious software) is software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems;

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

- Malware and its spreading throughout corporate network and SCADA is represented by SIR epidemic models
SIR epidemic models

- Classic SIR epidemic models consider all the individuals with the same tendency to become infected: Susceptible individuals

- Our models consider each node, which represent an ICT device, with its own different tendency to become infected: *Susceptible* device

- To remove an infection from an *Infected* device, it's necessary an antivirus scan with a certain probability of success in finding and removing the malware

- On the antivirus success, an infected device becomes a *Resistent* device

- We have used NetLogo, a programmable modeling environment for simulating natural and social phenomena, for our SIR models
A SIR model by NetLogo

SCADA & corporate network

Green: susceptible
Red: infected
Grey: resistant
A SIR model by NetLogo

Green: susceptible
Red: infected
Grey: resistant
A SIR model by NetLogo

SCADA & corporate network

Green: susceptible  
Red: infected  
Grey: resistant
A SIR model by NetLogo

SCADA & corporate network

Green: susceptible
Red: infected
Grey: resistant
SCADA & corporate network

Green: susceptible
Red: infected
Grey: resistant
A SIR model by NetLogo

SCADA & corporate network

Green: susceptible
Red: infected
Grey: resistant
A SIR model by NetLogo

SCADA & corporate network

Green: susceptible
Red: infected
Grey: resistant
Impact of cyber attacks on SCADA: numerical indicators by NS2

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 electricity 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 the electrical grid

- Load
- Electrical Junction
- Remotely Controlled Switch
- N.O. = Normally Open

Protection breaker

Diagram of electrical grid with nodes and connections.
FISR response time on malware spreading, MITM and DoS attacks computed by NS2

Percentage of grid customers which remain isolated

<table>
<thead>
<tr>
<th>Failure Section</th>
<th>Initial</th>
<th>Intermediate</th>
<th>Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time [sec]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case 1</td>
<td>18,4</td>
<td>34,8</td>
<td>29,1</td>
</tr>
<tr>
<td>Case 2</td>
<td>18,6</td>
<td>35,2</td>
<td>29,4</td>
</tr>
<tr>
<td>Case 3</td>
<td>&gt; simul. Time</td>
<td>&gt; simul. Time</td>
<td>&gt; simul. Time</td>
</tr>
<tr>
<td>Affected Customers [%]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Before FISR</td>
<td>46,6</td>
<td>26,6</td>
<td>26,6</td>
</tr>
<tr>
<td>After FISR</td>
<td>0</td>
<td>0</td>
<td>6,6</td>
</tr>
</tbody>
</table>
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.
• to conduct cyber attacks on a portion of an actual SCADA and to analyze their consequences on actual/simulated SCADA devices and on the simulated electrical grid

• The aim of the hybrid test bed is threefold:
  i) to reproduce the electrical grid, its SCADA and the corporate network, within the scope of FISR procedure;

  ii) to conduct actual Malware spreading, Denial of Service (DoS) and Man in the Middle (MITM);

  iii) to compute numerical indicators of attack consequences on SCADA and on the Electrical grid.
The hybrid test bed is constituted by the coexistence of actual, virtualized or modeled systems and devices.

- Electrical grid includes Primary Substations, Medium Voltage (MV) feeders, electrical trunks, breakers and loads
  - it is represented by an electrical simulator, with the exception of the breakers, which are actual devices.

- SCADA is constituted by a Control Centre and Remote Terminal Units (RTUs), linked by a communication infrastructure.
  - it is represented by an HMI, which barely implements the FISR procedure. The circuit breakers operations (controlled by SCADA RTUs) are implemented by means of actual Programmable Logical Controller (PLC) devices.
  - PLCs are connected, from one side, to the HMI and, from the other side, to the electrical breakers by actual standard connections.

- An attack system has been customized, starting from an open source tool, where each attack can be specified in terms of characteristics, attack initiation sources, attack targets. The attack system is completed by a detection system based on an open source Network Intrusion Detection System, used to monitor SCADA traffic.
ENEA Hybrid Test Bed Architecture

- **HMI - Human Machine Interface**
- **Programmable Logic Controller** (PLC) with **Sensors** and **Control equipments**
- **LAN provided by IEC**
- **SCADA Control Server**
- **Attacker**
- **NIDS - Network Intrusion Detection System**
- **VPN gateway by Virtual Machine**
An operator via the HMI client periodically download a file of the system log from SCADA Control Server via FTP service. To perform this activity he connects to the FTP server using the credentials in his possession and once he had access to the service proceeds to download the file.

- a MITM attack will allow an attacker to intercept the login credentials and the content of transferred data.
MITM attack by ARP poisoning

- ARP (Address Resolution Protocol) Poisoning (MITM) Attack
- A Man-In-The-Middle (MITM) attack is achieved when an attacker poisons the ARP cache of two devices with the MAC address of their Ethernet NIC (Network Interface Card) (e.g. Client-Server communication). Once the ARP cache has been successfully poisoned, each of the victim devices send all their packets to the attacker when communicating to the other device.
• This puts the attacker in the middle of the communications path between the two victim devices; hence the name Man-In-The-Middle (MITM) attack. It allows an attacker to easily monitor all communication between victim devices.

• The objective of this MITM attack is to take over a session. The intent is to intercept and view the information being passed between the two victim devices.
To perform MITM attack in the switched network LAN, we have used Ettercap, supplied by Kali Linux distribution.

Ettercap is a network manipulation tool used to perform a several kinds of attacks:

- Password sniffing for many network protocols
- Character injection
- Packet filtering and others
- Attacker, using Ettercap, captures traffic between Client and Server
- Ettercap poisons the ARP cache on each device and intercepts Ethernet traffic
- Ettercap extracts the login and password from any active connection
MITM Attack against an FTP Session

- Ettercap shows login and password in clear text in the FTP session
MITM attack: sniffing with Wireshark Tool

- Wireshark is a software tool used to sniff network traffic.
CockpitCI tool validation by IEC Remote Hybrid Test Bed

Cockpit CI HTB#1

Common IT Vlan11
Control Room 1873 Vlan19

IEC ZONE

Vlan13 Field (Common)
Vlan300 Lab IT
Vlan100 Field
Vlan200 Operation management

Cyber Security Energia (41) Roma, 3 Luglio 2014
Conclusions and future work

• We have investigated how different cyber attacks, starting from several places, might degrade the performance of the SCADA and then, lead to outages of the electrical grid.
• Models, indicators and quantitative results of the impact are intended to feed a tool to be developed within FP7 CockpitCI EU project
• We have build a flexible HTB to establish IPSec VPN site to site, to implement the MITM attack, to detect the attack

FUTURE WORK
• Integrate modelling and Test Bed
• Simulate a subset of SCADA system which includes an actual SCADA Control Centre and PLC at ENEA
• Implement attacks (i.e. MITM) between an actual SCADA Control Server and PLC by means of ENEA virtual environment embedded in Israeli Electric Corporation HTB within CockpitCI tool validation