Qualità di servizio di una rete elettrica sotto attacchi informatici al suo sistema di controllo, supervisione e acquisizione dati

L'articolo descrive modelli per rappresentare un sistema di Controllo, Supervisione e Acquisizione dati (SCADA, Supervisory Control And Data Acquisition) di una rete elettrica e la sua rete aziendale sotto diversi attacchi informatici: malware propagation, Denial of Service (DoS) e Man In The Middle (MITM). Abbiamo utilizzato NetLogo per identificare la propagazione del malware, in relazione alle politiche di sicurezza per il sistema SCADA e la rete aziendale, adottate dall'operatore della rete elettrica. Inoltre, le conseguenze di tali attacchi sulla Qualità del servizio (QoS) del sistema SCADA e della rete elettrica sono state calcolate mediante il simulatore di rete NS2.

Quality of Service of an electrical grid under cyber attacks to its supervisory control and data acquisition system

This paper describes models to represent a Supervisory Control And Data Acquisition (SCADA) system of an electrical grid and its corporate network, under malware propagation, Denial of Service (DoS) and Man In The Middle (MITM) attacks. We use NetLogo to identify possible malware propagation in relation to SCADA & corporate security policies adopted by the electrical utility. The consequences of such attacks on SCADA's Quality of Service (QoS) and, in turn, on the QoS of the electrical grid have been computed by NS2 network simulator.

DOI: 10.12910/EAI2014-93

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

Introduction

SCADA encompasses systems that monitor and control the industrial infrastructure, such as electrical grids. Since SCADA systems directly control physical systems, availability and reliability come in the first place, whereas in ICT (Information and Communication Technology) networks a significant stress is laid on confidentiality of information. Born as isolated systems, SCADA's carry the burden of a legacy of trust in the network, 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 [1]. Contrary to ICT network devices, SCADA systems are designed to run for years on end [2] without any reboot. This complicates the application of software patches and even makes post-attack forensics problematic since the system cannot be taken down and analyzed at wish [1]. In this work, we consider an actual reference scenario identified within the MICIE EU project (http://www.micie.eu) first and then extended within the ongoing CockpitCI (http://www.cockpitci.eu) EU project. We represent SCADA and corporate network under malware propagation, Denial of

Contact person: Michele Minichino
michele.minichino@enea.it

Service and Man In The Middle attacks. We use NetLogo (http://ccl.northwestern.edu/netlogo/) to model and analyse malware propagation in relation to the adopted SCADA & corporate network security policies, and NS2 (http://www.isi.edu/nsnam/ns/) to compute the consequences of the attacks on SCADA performances and, in turn, on power grid functionalities.

Reference scenario

The reference scenario limits the extension of the real world to be included into the models and provides a concrete context of operation. It is composed by an actual SCADA, a 22 kV MV grid and a portion of the corporate network. Topologies, main functionalities, devices, links among devices, communication protocols - with special attention on TCP/IP based protocols [3] - interdependencies, cyber security issues, such as cyber threats, vulnerabilities, pre-existent cyber security policies & technical solutions and attack cases, are described within the reference scenario (http://www.cockpitci.eu). Figure 1 shows a simplified schema of the Medium Voltage (MV) electrical grid controlled by SCADA. It consists of a portion of a MV grid at 22 kV, energized by two HV/MV substations. Each substation feeds different types of loads/customers, throughout

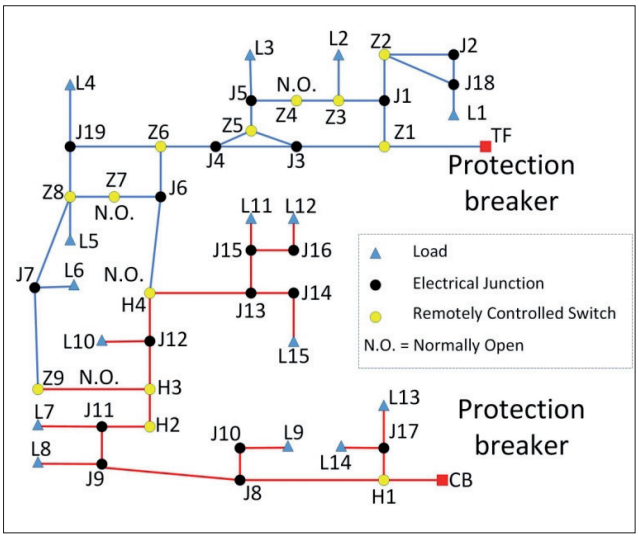

FIGURE 1 MV power grid

electrical sections, connected to one another by Normally Close Circuit breakers. The substations include Protection breakers. Under normal operative conditions, customers are energized by either one substation (TF) or the other one (CB), by means of two sub grids, separated from one another by two, Normally Open, Tie switches. Tie switches and Circuit breakers are remotely controlled by SCADA via its Remote Terminal Units (RTU). SCADA monitors the grid status, acts on Circuit breakers to connect or isolate the grid electrical sections, and on the Tie switches position to feed a subgrid by the alternate substation, in case of power grid reconfiguration on permanent electrical failure in the subgrid.

Figure 2 shows the SCADA system and a portion of corporate network of Israel Electric Corporation. From the SCADA Control Centre (SCC), the operator remotely controls in real-time the electrical grid in Figure 1, by means of RTUs. Particularly, the following devices belong to the SCADA system:

- MCPT G.W gateway, which converts a proprietary Data Link Communication (DLC) protocol for Radio channels to the TCP/IP protocol. For DLC and TCP/IP protocols, each transmission is automatically accompanied by an ACK message, ensuring the transmission integrity.
- Field Interface Unit (FIU MOSCAD), dedicated to RTU interrogation and routing of data messages to/from SCC. It comprises a Radio Frequency (RF) Modem Interface (RF Modem ND), that includes two VHF radio units (F2, F3) connecting the RTUs to SCC throughout either the F2 or F3 channel.
- Store & Forward (S&F) Repeater MOSCAD DN, which communicates upwards with the SCC (via the RF Modem and FIU) and downwards with the RTUs using the two RF channels (F1 and F3).
- RTUs; there are 13 RTU sites, 9 of them fed by TF substation and 4 by CB substation (Fig. 1).

The SCADA system is fully redundant. The main communication path between SCC and the RTUs traverses the main Gateway (MCPT G.W PRIME) and the main FIU (MOSCAD ND). In case of failure on the main path, data are rerouted on the backup path that traverses the backup Gateway (MCPT G.W SECOND), the backup FIU (MOSCAD DN), the corporate network from Point of Presence (PoP) ND to Local eXchange DN-VHF), MOSCAD DN S&F Repeater and then reaches the RTUs.

In case the primary RF channel is not available for any reason, the system switches to the alternate RF channel.
The portion of corporate network in the reference scenario is also shown in Figure 2. It is composed by three hierarchical layers:

- *A Backbone layer,* where PoP devices are connected to each other in a meshed topology (NA, NM and ND devices in Fig. 2). The PoP is a multiservice optical platform that integrates several technologies, including Synchronous Digital Hierarchy, Synchronous Optical Network (SDH/SONET) and Dense Wavelength Division Multiplexing (DWDM),
- A *Local eXchange layer* (LeX) represents the point of access at lower bandwidth of corporate network. In Figure 2, the following LeX devices: CB, ML, TF, MS, BL, DN-VHF.
- *A Transit eXchange layer* (TeX), between the two other layers, that grants scalable traffic in multi-ring topology. A TeX device is based on the SDH/SONET technology, which aggregates data flows at different bit rates and retransmits them over long distances.

Within the reference scenario, the SCADA operator executes a procedure, named FISR (Fault Isolation and System Restoration), to locate, isolate and quickly and safely reconfigure the electrical grid on permanent electrical failures. Permanent failures may cause the de-energisation even of a large part of electricity customers. We discuss how cyber threats, vulnerabilities and attacks might result in loss of view and loss of control of the electrical grid from the SCADA Control Centre and then, as a consequence, in a de-energisation of grid customers.

Scada cyber security

Cyber vulnerabilities and attack vectors of SCADA challenge the reliability, resiliency and safety of the electric grid day by day. For such a reason, a cyber security protection of SCADA & corporate network cannot be neglected by electrical grid utilities. Vulnerabilities involve computer, communications (SCADA & corporate

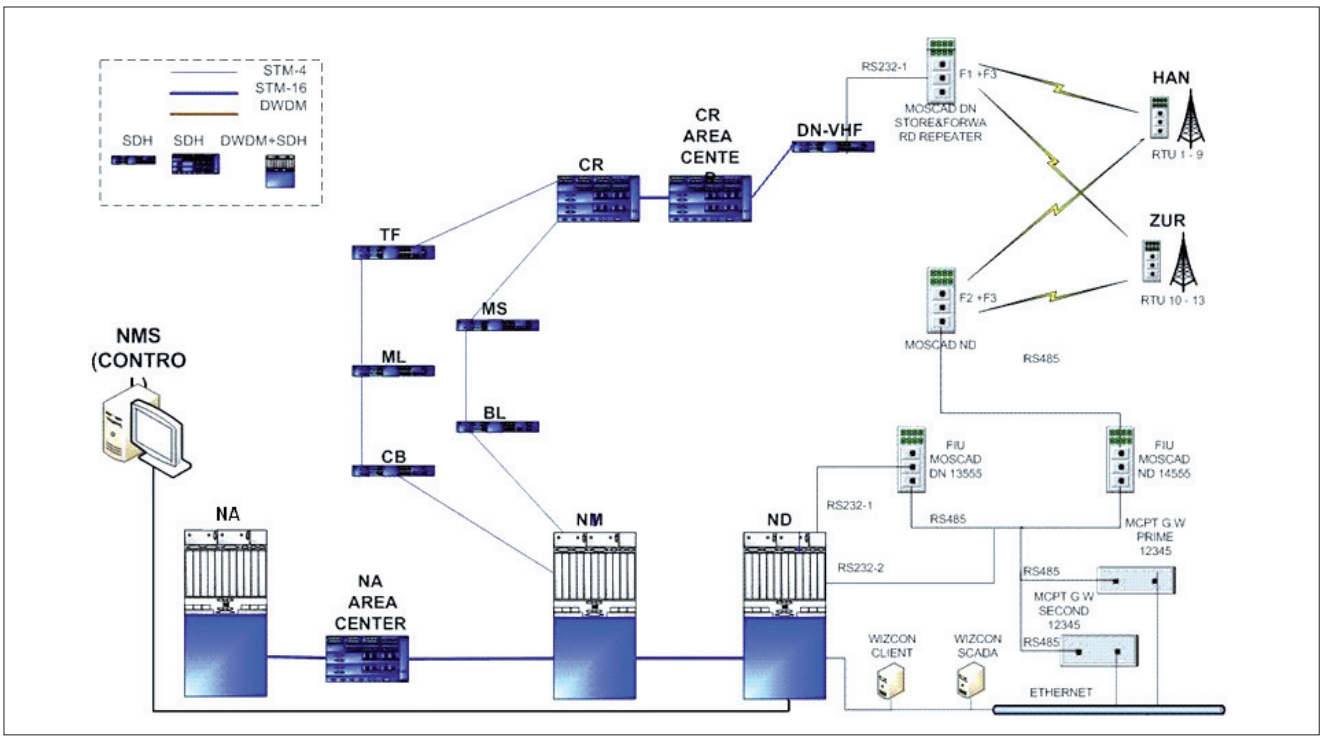

FIGURE 2 The SCADA system and a portion of corporate network

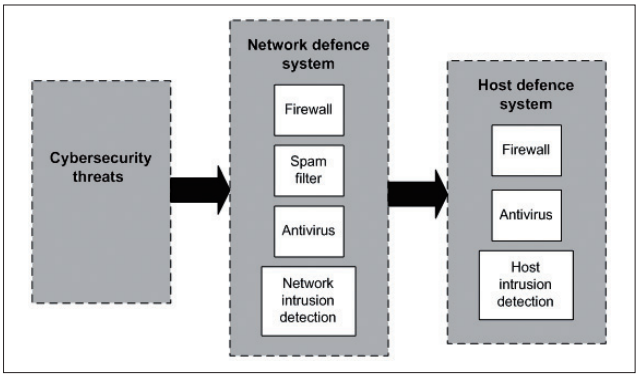

FIGURE 3 A typical cyber security protection system
Source: CockpitCI EU project

networks) and in turn electrical grids. Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously, and can come from many places, including indirectly through corporate network. As a deterrent for attackers, security policies are adopted such as system hardening and intrusion detection systems.
Once a vulnerability has been exploited, specific adverse actions can be performed, such as:

- Denial of Service (DoS) on an individual machine/device, a group of devices or an entire sub-network, inside a SCADA network (DoS attacks are considered the easiest type of attack to launch);
- Software infected with malware with the aim of disrupting the performance of the network and/or the machines/devices on the network;
- Changes to the software or modifications to the configuration settings;
- Spoofing system operators and/or devices on the control network (This is the most difficult action to execute but would provide the adversary with the most capabilities);
- Changes to instructions, commands (same difficulty as above): Protocol manipulation, vulnerability exploitation and MITM attacks are among the most popular ways to manipulate insecure protocols, such as those found in control systems.

Figure 3 illustrates a typical cyber security protection system [4]. The system protects the cyber-infrastructure and combats threats at two levels: 1) at network level: "network based defence systems", and 2) at host level: "host based defence systems". Network based defence systems control the network traffic by network firewall, antivirus, spam filters and network intrusion detection techniques, whereas the host based defence systems control the data flow in a workstation by host firewall, antivirus and host intrusion detection techniques.

Models

We represent SCADA & corporate network under the occurrence of three different kinds of cyber attacks:

1. Malware injected into a specific device of corporate network, which spreads throughout the corporate network and SCADA devices up to disconnect the communication between SCADA Control Centre and its RTUs.
2. DoS attacks, in which a malicious agent exploits the weakness of network protocols to flood a specific SCADA & corporate network device, with the aim of saturating the bandwidth of the carrier among SCADA Control Center and its RTUs.
3. MITM attacks, where an attacker intercepts the traffic between two SCADA/corporate network devices and then injects new commands/information that override the original ones.

Malware propagation

The malware injection model is based on SIR (Susceptible, Infected, Resistant) mathematical formalism, for disease spread over individuals [5]. To represent SCADA and corporate network we have got a SIR net, described by a graph, where each device is a node and there is an arc whenever two nodes can communicate with each other [6]. The virus infection is the malware. A node can move from S, the susceptible group, to I, the infected group, when it comes into contact with an infected node. What qualifies a contact depends on the virus. Each infected node contacts the neighbour nodes in each step of time. Each contact may not result in the transmission of the virus, only a percent of the contacts result in transmission. For each j node (j=1,…, N), we define dj as the number of the neighbours of the node j, of which the fraction α may result infected; so, we assume that the virus spread itself, every time step, on a fraction $\beta j = \alpha \cdot dj$ of the nodes.

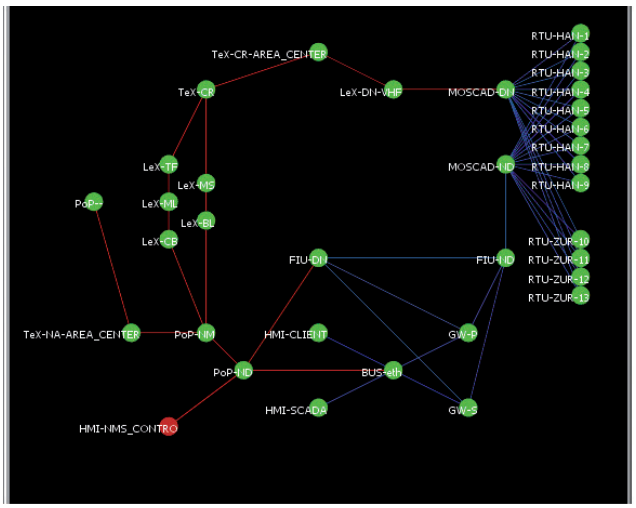

FIGURE 4 The infection starts on an NMS device of corporate network

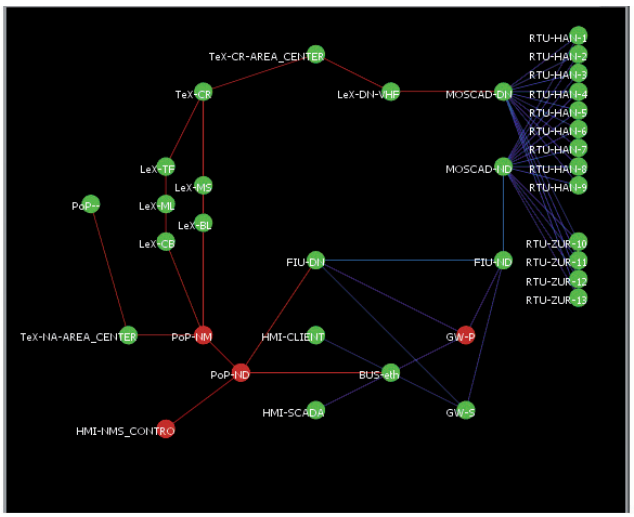

FIGURE 5 The infection spreads on corporate network and SCADA devices

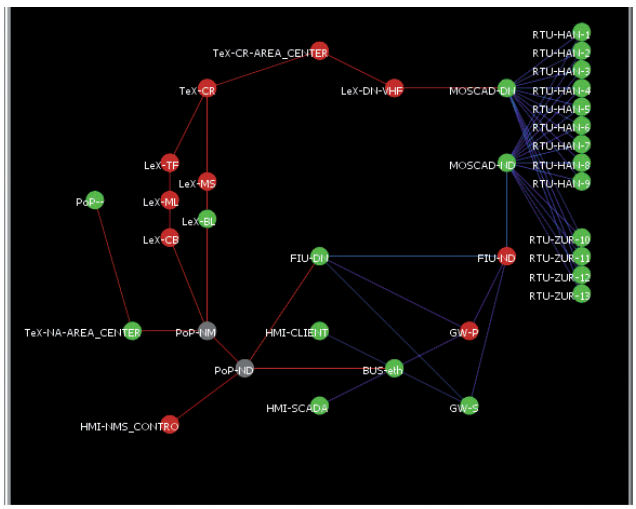

FIGURE 6 SCADA operator loses grid Observability

We justify such an assumption thinking of dealing with a stealth virus. A stealth virus does not infect nodes too much each time, since otherwise it could be more easily detected, for instance, looking at the increased traffic value. Moreover, we assume that each node has a different probability to contract the virus: γj. The virus doesn't disappear after a certain period of time, but just after periodically running the antivirus or after maintenance operations, kj is the rate of the antivirus scan. Depending on the virus, there is the possibility that the antivirus can find it and know how to remove it, ϕj is that probability. At each point of time, we have three groups of nodes and a specific numbers of nodes in a group. We have used NetLogo to create the model, set SIR variables and represent the occurrence of a cyber attack on a corporate network device (Network Management System). NetLogo is an agent-based modelling tool for simulating natural and social phenomena. It is particularly well suited for modelling complex systems developing over time. In our model, malware spreads throughout the corporate network and SCADA devices until it disconnects the communication between the SCADA Control Centre and the RTUs. We assume that the security polices of SCADA and corporate network are dependent upon the criticality of their devices. We use the following variables:

- *Alfa*: it is the spread value and it is a measure of how many neighbours are reached by the virus infection. Its range is (0, 100) %.
- *Antivir-check*: it indicates how many time units are needed to perform an antivirus check (or everything that can help to find a malware). Its range is (1, 365) days.

- *Virus-spread-time*: the virus can spread itself along the network at various rates. We assume that an infected node may infect just a fraction of its neighbours. Its range is (1, 365) days.

Figure 4 shows the screenshot, at the time t = 0 , of the SIR model. The infection starts on the Network Management System device of the corporate network (Fig. 2), named HMI-NMS_CONTRO in Figure 4. Along the infection spreading, each node of SIR model can be in one of the three states: Susceptible (*S*): the node is healthy (in green colour) and it can be infected by a malware; Infected (*I*): the node is infected (in red colour): at some rate it can infect neighbour nodes; Recovered (*R*): the antivirus scan has successfully removed the infection (in gray colour).
The links among corporate network nodes are depicted in red colour while the links among SCADA nodes are depicted in blue colour.
According to the modelling assumptions on the infection spreading, the virus propagates throughout PoP-ND and PoP-NM devices (respectively, at time step=1 and at time step=2) and, in turn, on the GW-P device (at time step =4) of the primary SCADA Control Centre-RTU connection (see Fig. 5). Then the virus spreads on LeX-CB and FIU-ND (time step= 5). The infection of the FIU-ND node causes the primary connection between the SCADA Control Centre and the Remote Terminal Units to get out of service. At such a stage, the SCADA operator still has a full observability and operability of the electrical grid of Figure 1, by means of the secondary communication between the SCADA Control Centre and the RTUs. At time step = 52, the virus also infects the TeX-CR node. At this stage (Fig. 6), the SCADA operator completely loses the observability and operability of the electrical grid of Figure 1. If a permanent electrical failure occurs on the grid, the SCADA operator cannot run the FISR service remotely.

DoS and MITM attacks

DoS and MITM attacks are specified in terms of attack parameters, attack initiation sources, attack targets. Specifically, attack initiation sources fully cover SCADA & corporate devices and even external devices connected by means of the internet. Attack targets have been chosen to cause a maximum number of damaged SCADA devices as a consequence of a successful attack on a single device.
Different indicators of expected consequences of a DoS or MITM attack have been investigated. Any attack may result in the loss of view and of control of the RTUs (and thus of the electrical grid) from SCADA Control Center. In our models we measure the following numeric indicators of SCADA performances on the attack occurrence:

- *LoV*, Loss of View: the SCADA Control Center cannot receive packets from the RTUs;
- *LoC*, Loss of Control: the RTUs cannot receive packets from the SCADA Control Center;
- *DPR*, Dropped Packets Rate: how many packets are missing on the network;
- *TTBP*, Transmission Time Between two Packets;
- *RTT*, packet Round Trip Time: composed by TCP transmission time plus ACK transmission time;
- *Packets routing*.

DoS attacks have been performed with the aim of saturating the bandwidth of the carrier used for the communication between the SCC and its RTUs. The MOSCAD front end of Figure 2 has been chosen as an attack target. The main parameters of the DoS attacks have been specified in terms of packet size, interval between packet transmission, number of packets sent during the attack, the protocol of the flood attack.
The main characteristics of the MITM attacks are as following:

- the attacker intercepts the traffic;
- once the traffic is intercepted, the attacker injects new commands/information that override the original ones. The injection occurs by means of packets between the SCADA Control Center and the victim RTU, with the same format of the normal SCADA packets, but with a higher frequency. The rationale is that a higher frequency of the MITM packets facilitates the overriding of normal SCADA packets;
- the attacker does not modify the payload of normal SCADA packets;
- the attacker connects to SCADA devices or corporate network devices through an Ethernet cable at the same speed of the Ethernet of the reference scenario;
- when the attacker intercepts the VHF communication, (s) he uses a VHF antenna, the propagation time between MOSCAD and MITM and from MITM and RTU is halved.

Again here, the MOSCAD front end of Figure 2 has been chosen as an attack target. Particularly, MOSCAD-DN when the attack comes from the corporate network and SCADA is working on the alternate path; MOSCAD-ND when the attack come from an external devices connected to SCADA system by means of the Internet.

To evaluate the attack consequences on SCADA's performances, we have considered the following numeric indicators of the MITM attack:

- *LoV*, the SCADA Control Center receives false information/data from MITM attacker. The consequent false observability of the Power grid from the SCADA Control Center may induce a tricky behaviour by the SCADA operator.
- *LoC*, the RTU receives false commands from the MITM attacker instead of the SCADA Control Center.
- Change of *Packets routing*.

Also a slight variation of *TTBP* and *RTT* has been expected

To predict the above indicators, we have built and run an NS2 model of SCADA & corporate network under cyber attacks, according to the schema in Figure 2 and the cyber attacks specified above. Table 1 summarizes the main parameters of DoS attacks on the SCADA system and their impact on SCADA performances. Particularly, the first four lines specify the attack parameters: source, destination, start and end time of the attack. The following four lines report the consequences of the attacks, as measured by the NS2 model: Loss of View (*LoV*), Loss of Control (*LoC*), maximum and minimum values of the Round Trip Time (*RTT*) during the attack, missing packets (*DPR*). Also, the simulation time and computation time are reported in the last two lines. Computation time grows from 15 to 21 minutes.

Figure 7 shows, as an example, the "travel times" of SCADA packets to RTU-1, under four phases of a DoS attack coming from LeX-BL.

The messages between the SCC and RTU-1 are differentiated by colour: black for commands from the SCC to RTU-1; blue for ACK from RTU-1 to the SCC; red

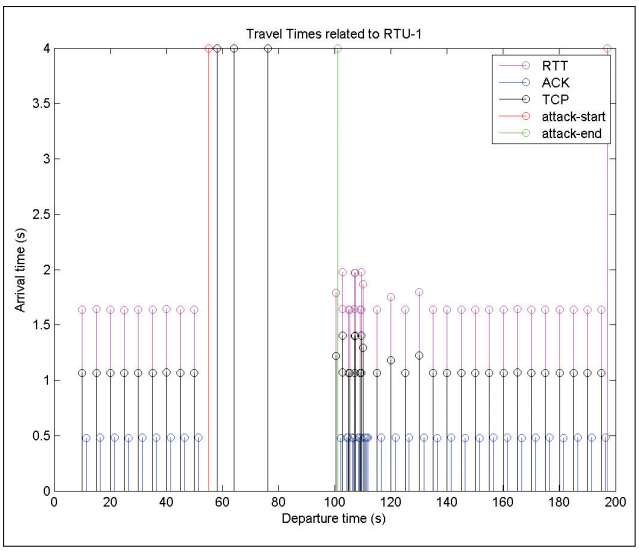

FIGURE 7 Arrival times (TCP, ACK and RTT) of SCADA packets to RTU-1 under a DoS attack

Attack source	PoP	TeX-CR	LeX-BL	Internet
Attack target	MoscadDN	MoscadDN	MoscadDN	MoscadND
Start time [sec]	55	55	55	55
Stop time [sec]	101	101	101	101
LoV	NA	NA	NA	0/17
LoC	57/57	57/57	57/57	59/76
RTT Max/Min [sec]	Inf / inf	Inf / inf	Inf / inf	Inf/ 1792
DPR	57/57	57/57	57/57	59/93
Simulation time [sec]	200	200	200	200
Computation time [min]	21	15	17	15

TABLE 1 Simulated DoS attacks on SCADA system

for the start time of the flood attack (55 s); green for the end time of the flood attack (101 s); magenta for the RTT of the exchanged packets. In Figure 7, the arrival times of packets which take an infinite time to arrive to destination are shown with a saturated arrival time of 4 sec., that is the upper border of the figure. Four attack phases can be distinguished:

1. Before the attack: SCADA packets flow from the SCC to RTU-1 and come back normally. RTT, TCP and ACK travel times are regular.
2. During the attack: the flood starts to increase the occupancy of all the buffers of the devices flooded by the attack, until they are saturated.
3. Soon after the attack: there is a tail. SCADA messages go in de-synchronization. That is due to the fact that the saturated buffer is emptied at a rate that is different from the nominal packet transmission rate; along the tail, packets are transmitted at lower intervals than the nominal ones.
4. Return to nominal conditions: flood problems end and the operative conditions come back to nominal ones.

Table 2 shows the computational time and all the traversed devices in communication between the SCC and RTU-2, along the phases of a MITM attack, which occurs between MOSCAD-ND and RTU-2. For each row of the table, the first bullet shows the route taken by SCADA packets from the SCC (n. 27) to RTU-2 (n. 5); the second bullet shows the opposite route from RTU-2 to the SCC. The MITM node (n. 38) is bold-highlighted and underlined. The relationship between numbers and devices of the SCADA and corporate network is shown in the last two columns, where the MITM node (n.38) is not included. These very simple results show the change of the packet routing, in case of MITM occurrence in the network.

Impact of cyber attacks on the electrical grid and customers

In a situation in which a permanent electrical failure of the power grid occurs and the SCADA operator cannot act remotely or can act with delay as a consequence of any of the above cyber attacks, a large portion of the power grid customers can be de-energized.

Table 3 summarizes the values of FISR response time and the percentage of the affected power grid customers. Three different operative conditions (cases) of SCADA & corporate network have been considered: case 1) nominal conditions of SCADA & corporate network under initial infection spreading; case 2) the outage of the primary path between the SCC and the RTUs; case 3) On outage of the primary path between the SCC and the RTUs, a successful cyber attack (Malware, or DoS, or MITM) causes the back-up connection between the SCC and the RTUs to get out of service; in such a case the operator loses view and control of the grid. Three different locations of the permanent electrical failure on the grid have been assumed: 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 until 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 the failed section and the tie switch are powered by the other substation until the manual repair, that restores the initial configuration of the grid; iii) *failure in a terminal section of the grid* (bounded by the RTU and loads): the loads of the failed section are isolated until the manual repair, that restores the initial configuration of the grid.

The first row of the table reports the location of the

Computational time:	4 sec	Device	Device number
Traversed devices before the attack	• 27 34 29 1 3 5	FIU-ND	1
	• 5 3 1 29 34 27	MOSCAD-ND	3
Traversed devices during the attack	• 27 34 29 1 3 **38** 5	RTU-HAN-2	5
	• 5 **38** 3 1 29 34 27	WIZCON SCADA	27
Traversed devices after the attack	• 27 34 29 1 3 5	GATEWAY PRIME	29
	• 5 3 1 29 34 27	BUS Ethernet	34

TABLE 2 MITM attack between MOSCAD-ND and RTU-2

Failure section		Initial	Intermediate	Terminal
Response time	case 1	18.4	34.8	29.1
[sec]	case 2	18.6	35.2	29.4
	case 3	> simulation time	> simulation time	> simulation time
affected customers	Before FISR	46.6	26.6	26.6
[%]	after FISR	0	0	6.6

TABLE 3 FISR response time and % of affected customers

permanent failure that requires the activation of FISR. Row 2 reports FISR response time in seconds, distinguished in case 1, case 2 and case 3. In case 3, the SCADA operator completely loses the observability and/or controllability of the power grid. The percentage of the affected customers depends on the section of the grid in which the failure is located. Failures in the initial section of the grid affect a higher percentage of customers. In the case of a failure of the terminal section of the grid, there is a percentage of customers out of power service till the manual repair of the failure of the grid has been completed. The outage duration of the affected customers, in cases 1 and 2, corresponds to the FISR response time plus the manual repair time, when needed. The manual repair time is needed in case of failure in a terminal section of the grid. In case 3, FISR cannot be activated remotely by the SCC and the outage duration corresponds to the manual repair of the permanent failure of the grid.

Conclusions and future work

This work, as far as we know, presents two main novelties with respect to the state of the art: a) the representation of different types of cyber attacks and their propagation on an actual SCADA & corporate network; b) the modelling process of cyber attacks and their impact on technological networks is supported by two heterogeneous tools: NetLogo, focused on malware propagation, and NS2, which computes the impact of cyber attacks on the quality of service of SCADA and its electrical grid. However, the modelling activity presents limits in representing cyber attacks. To overcome such limits we are currently investigating the use of a hybrid test bed [7] to conduct cyber attacks on SCADA and to analyze their consequences on SCADA itself and on the electrical grid. The hybrid test bed is based on the coexistence of actual, virtualized and modelled systems and devices and is intended to: i) reproduce the electrical grid, its SCADA and the corporate network; ii) conduct the three, previously described kinds of cyber attacks on SCADA and the corporate network: Malware spreading, Denial of Service (DoS) and Man in the Middle (MITM); and eventually iii) compute numerical indicators of attack consequences.

Ester Ciancamerla, Michele Minichino, Simone Palmieri, Tatiana Patriarca
ENEA, Technical Unit for Energy and Environmental Modeling - Computing and Technologic Infrastructures Laboratory

Benedetto Fresilli
ENEA, Technical Unit for Nuclear Fission Technologies and Facilities, and Nuclear Material Management – Engineering Simulator Laboratory

references & notes

[1] I. Ahmed, S. Obermeier, M. Naedele, G. Richard, 2012, "Scada systems: Challenges for forensic investigators" in IEEE Computer, 12/2012, 42-49 45(12).
[2] E. Byres, D. Lissimore, N. Kube, 2006, "Who turned out the lights? - security testing for SCADA and control systems", in CanSecWest,, Vancouver, British Columbia, April 2006.
[3] IEC 60870-5-101 Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks.
[4] S. Dua, X. Du, 2011, "Data Mining and Machine Learning in Cybersecurity", Boca Raton CRC Press.
[5] T. Tassier, 2005, "SIR model of epidemic" in Epidemics and Development Policy, Fordham University NY.
[6] E. Ciancamerla, M. Minichino, S. Palmieri, 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).
[7] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, X. Yu, 2009, "Building a SCADA security testbed", in Proceedings of the Third International Conference on Network and System Security, 357–364.