ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Dicembre

2014

Rapporto tecnico N.55

Italian Case Study: socio-economic impact analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version

Valentino Angeletti, Luca Guidi, Daniela Pestonesi, Marco Biancardi, Marco Alessi, Graziano Abrate, Clementina Bruno, Fabrizio Erbetta, Giovanni Fraquelli, Azahara Lorite-Espejo

Consiglio Nazionale delle Ricerche
CERIS Istituto di Ricerche sull'Impresa e Lo Sviluppo

RAPPORTO TECNICO CNR-CERIS

Anno 9, N° 55; Dicembre 2014

Direttore Responsabile

Secondo Rolfo

Direzione e Redazione

CNR-Ceris
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
www.ceris.cnr.it

Sede di Roma

Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano

Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione

Enrico Viarisio
e.viarisio@ceris.cnr.it

ESSENCE

***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment*

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

The Essence project is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.
Networked computers reside at the heart of critical infrastructures, these are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, and expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber security of control and communication systems is now very strong worldwide. To that aim, several frameworks have been developed or are under development at present, both in the form of guidelines and proper standards, but it is difficult to evaluate costs and benefits of their adoption, although experimentation so far has shown that they may be huge.
In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts;
2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;
4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

The results of the study will be published in a series of technical reports, hosted in the “Ceris Technical reports series”. The published titles are:

1. Considerations on the implementation of SCADA standards on critical infrastructures of power grids.
2. Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria.
3. Terms of reference for the trials.
4. Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case study.
5. Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures.
6. Italian Case Study: socio-economic impact analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version.

Partners of the project are:

CNR-Ceris *(Coordinator) (Italy);* Università del Piemonte Orientale Amedeo Avogadro *(Italy);*
Deloitte Advisory S.l. *(Spain);* Antonio Diu Masferrer Nueva Empresa SLNE *(Spain);*
Enel Ingegneria e Ricerca S.p.A. *(Italy);* Abb S.p.A. – Power systhems division *(Italy);*
IEN - Institute of power engineering *(Poland);* PSE – Operator SA *(Poland).*

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Italian Case Study: socio-economic impact analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version

Valentino Angeletti, Luca Guidi, Daniela Pestonesi [*]
Marco Biancardi, Marco Alessi [**]
Graziano Abrate, Clementina Bruno, Fabrizio Erbetta, Giovanni Fraquelli, Azahara Lorite-Espejo[***]

*Corresponding author: Clementina Bruno
Dipartimento di Studi per l'Economia e l'Impresa
Università del Piemonte Orientale
28100 NOVARA – ITALY
Mail: clementina.bruno@eco.unipmn.it

ABSTRACT**:** The Italian Case study is a comprehensive report in which a possible attack scenario to a thermoelectric power plant is described in the Italian electric grid context and an assessment of social-economic impact is evaluated. A cost-benefit analysis of the adoption of comprehensive CIP standards is estimated. This is a reduced version of a full report in order to have a public deliverable purged from sensitive and confidential information.

Keywords: Cybercrime; Cost-benefit analysis; cost of blackouts

JEL code: D12, D61, L94, Q43

* Enel Ingegneria e Ricerca, Via Andrea Pisano 120, 56122 Pisa, www.enel.com.
** ABB SpA, Via Albareto 25, 16153 Genova, www.abb.it.
*** Università del Piemonte Orientale Dipartimento di Studi per l'Economia e l'Impresa, Via Perrone 18, 28100 Novara, www.unipmn.it.

SUMMARY

1. ITALIAN ELECTRIC SYSTEM

1.1 Introduction

The electric system can be divided into three major subsystems related to three different phases: **generation, transmission** and **distribution of electricity**.

Electricity does not exist as a natural resource and it is therefore necessary to generate it. Generating energy means transforming into "electricity" the power obtained from primary sources. This transformation occurs in power plants.

High Voltage electricity transmission (380 kV - 220 kV - 150 kV) means transferring the power produced in the plants to consumer areas. In order for this to occur, lines and transformation plants are necessary, that is the elements that form the Transmission Grid. In Italy a total of over 63.500 kilometres of lines are owned and managed by Terna, a state owned company.

The last phase of the electricity generation process is represented by distribution, that is the delivery of medium and low voltage electricity to final users.

1.2 Italian electric infrastructure

The process of liberalisation and regulation of the electrical energy market was begun with Directive 96/92/EC, which was subsequently repealed by Directive 2003/54/EC, in force from July 1st 2004.

The European law was applied in Italy with Legislative Decree n° 79 dated March 16th 1999, ("L. Decree n° 79/99", the so-called "*Decreto Bersani*"), subsequently amended by Law n° 290 dated October 27th 2003, which sets forth urgent instructions for the security of the national electricity system and for electric recovery.

More specifically, the above said law delegated to a Prime Ministerial Decree (DPCM May 11th 2004) the definition of criteria, methods and conditions for unifying the ownership and management of the national electricity transmission grid and for the management of integrated undertakings, while respecting the public interest in connection with the security and reliability of the national electricity system and the commercial autonomy of the current owners.

This Code was drafted in compliance with the electricity industry laws and regulations in force at the moment of its application, as well as in compliance with the "*Concession to Gestore della Rete di Trasmissione Nazionale S.p.A. of transmission and dispatching of electrical energy in the national territory*" granted with the Decree from the Minister of Productive Activities on April 20th 2005, published in the Official Gazette n° 98 on April 29th 2005.

1.2.1 Generation

Power plants are owned by Generation Companies: following the Italian market liberalization there are a lot of big and small companies: ENEL Produzione, Edison, EoN, firms owned by municipalities and others.

In Italy there are, in total, some thousands of generation plants with about 122.000 MWe of gross installed capacity at the end of year 2011:

- about 3.500 thermo with about 80.000 MWe of gross installed capacity;
- almost 3.000 hydro with 22.000 MWe of gross efficient power;
- wind generators for about 7.000 MWe;
- photovoltaic for about 12.800 MWe.

The available capacity at the peak was, in 2011, about 63.500 MW; the difference compared with the total installed capacity is due to the out-of-service for maintenance inability of some typology of plants to supply all the nominal power, etc.. In that year the peak demand was recorded on July 13th at 12 am with a value of 56.474 MW.

Limiting the interest to the large power units, connected to the transmission network, we have about **130 units with power greater than 200 MWe and only 28 units with power greater than 500 MWe**. Each power plant is constituted by one or, most frequently, by more units (with the same or with different power). Each unit is directly connected to the transmission network and is considered an autonomous entity from the point of view of network control and market participation.

1.2.2 Transmission

High Voltage electricity transmission (380 kV - 220 kV - 150 kV) is Terna's task. Terna operates the National Transmission Grid and the electricity flows for Italy under security conditions through dispatching: keeping the electricity supply and demand in balance, 365 days a year, 24 hours a day.

The Electricity Transmission Grid is a set of power lines (over 63.500 kilometres of lines) and stations (431 transforming and switching stations throughout the country) that form the meshed structure for transferring electricity from the sites where it is produced (power plants) to the sites where it is distributed (users and distribution grids). The national transmission grid is formed by three separate meshed systems which are interconnected, each one having a different voltage (132/150, 220 and 380 kV).

The 380 kV system, interconnected with the European electricity system, constitutes the primary transport network which conveys the electrical energy produced by most of the power generation plants to the most important junction points for transformation to lower voltage levels.

The 220 kV system is fed by a non-insignificant percentage of power plants, and, in part, carries out the distribution of high voltage.

The 150-132-120 kV system has the role of high voltage distribution, feeding the HV/MV primary stations or directly providing electricity to high voltage utilities.

A line is the system that connects two junctions of the grid. It is formed by the power conductors that transfer electricity, by guard wires that protect the conductors against voltage surges having atmospheric origins and by the pylons supporting conductors and guard wires. Lines can be single or double circuit if they are built with one or two groups of conductors, respectively.

A primary substation is a plant where the interconnection among the different voltage levels between lines and energy transformation occurs. Through the transformer, two power junctions are connected to different voltages where the corresponding electricity lines converge. The station contains all the equipment necessary for closing and sectioning the converging lines in order to manage energy flows.

1.2.3 Distribution

Electricity distribution is the final stage in the delivery of electricity to end users. A distribution system's network carries electricity from the transmission system and delivers it to consumers. Typically, the network would include medium-voltage (1kV to 72.5kV) power lines, substations and pole-mounted transformers, low-voltage (less than 1kV) distribution wiring and meters.

The modern distribution system begins as the primary circuit leaves the primary substation (the boundary between the transmission network operated by a TSO and the distribution network operated by a DSO) and ends as the secondary service enters the customer's meter socket.

Distribution circuits serve many customers. The voltage used is appropriate for the shorter distance depending on utility standard practice, distance, and load to be served. Distribution circuits are fed from a transformer located in an electrical substation, where the voltage is reduced from the high values used for power transmission.

In Italy by law, for each municipality there is only one distribution company that operates the distribution network. In some big towns the distribution is managed by small companies, often participated by multinational groups: “ACEA Distribuzione” in Rome, “A2A Reti Elettriche” in Milan and Brescia, “AEM Torino” in Turin. However, the major Distribution System Operator (DSO) in Italy is still Enel Distribuzione with the following assets:

Medium Voltage (MV)

- 1.983 primary substation (HV/MV) with a transforming power of 87.532 MVA
- 477 satellite centres and MV sections
- 333.194 km of MV lines

Low Voltage (LV)

- 345.388 secondary substation (MV/LV) with a transforming power of 65.688 MVA
- 62.453 other secondary substation (MV/LV) with a transforming power of 1.197 MVA
- 725.735 km of LV lines
- About 30 million of smart meters

1.3 Electric system operation

1.3.1 Dispatching

Electricity is not a storable commodity. Hence it is necessary to produce the requested quantity and distribute it through the system in such a way as to ensure that electricity supply and demand are always evenly balanced, thus guaranteeing continuity and safety in supply of the service. Management of the flows of electricity is known as dispatching.

The real time management of the Italian electric system, interconnected with the European system, is performed through a hi-tech control system, which refers to the Terna National Control Centre, that monitors 293 lines, among which 9 interconnections with foreign countries, 3 submarine cables and 281 national 380kV lines.

The control system acquires, minute by minute, all the data relating to the state of the electric system and, in accordance with the requirements of the moment, implements the appropriate corrective measures. The essential duties of the National Control Centre are performed:

- **In the planning phase**, with the drawing up of the operation plans developed on the basis of the forecasts for electricity and power demand at national level and of the availability of the production units. The short-term weekly and daily forecasts, developed on the basis of medium-term forecasts, allow determination of the production levels, configuration of grid functioning and power reserve.
- **In the real time control phase**, analysing the state of the electric system, the National Control Centre intervenes in the generation of active and reactive power and on the electric grid; at the same time it works to achieve optimization of the service, recovery in the event of outage, control of any emergencies and coordination of works-related manoeuvres.
- **In the operation analysis phase**, in addition to processing the statistics relating to all the operating data, it analyses the functioning of the production and transmission system, so as to gather useful indications for optimisation of system operation.

1.3.2 Grid Code

The "***Code for transmission, dispatching, developing and security of the grid"*** (Grid Code) is applied in relations between Terna and grid users starting November 1st, 2005. This document was drawn up in compliance with the provisions stated in Prime Minister Decree dated May 11th, 2004 regarding unification between ownership and management of the grid. It governs the procedures regarding the activities of connection, management, planning, development and maintenance of the national transmission grid, as well as dispatching and measurement of electrical energy.

This is fundamental in a competitive electricity market, where many competitors must have access to the grid, which is a natural monopoly, on non-discriminatory basis. Otherwise the access to the grid could be sued as source of market power, perturb the competitiveness of the market and reduce its welfare performance.

This is also why, following the Bersani Decree cited above and the introduction of competition, an unbundling process occurred and the ownership of the grid was transferred from the previous owner (mainly Enel, but not only) who was active in other competitive phases, to a public owned, non-competitive firm [1].

[1] This was partially replicated later on also for the local distribution network, which had to be conferred to separate firms, so as to ensure better external accountability. The distribution activities are run under a concession regime by these companies, who are charged of the management of the distribution grids and of metering and billing activities, and are not allowed to carry out commercial activity (electricity sales). See the integrated text on the accountancy and pubblicity duties for firms active in electricity and gas industries ("Testo integrato delle disposizioni dell'autorità per l'energia elettrica il gas e il sistema idrico in merito agli obblighi di separazione contabile (unbundling contabile) per le imprese operanti nei settori dell'energia elettrica e del gas e relativi obblighi di comunicazione - tiuc, deliberazione 18 gennaio 2007, n. 11/07 http://www.autorita.energia.it/allegati/docs/14/231-14all.pdf)

More specifically, the Grid Code[2] sets forth transparent, non-discriminatory regulations for:

a. access to the grid and its technical regulation;
b. development, management, and maintenance of the grid;
c. the performance of dispatching services;
d. supply of services of measurement and settlement of financial charges connected to the aforementioned services; and
e. security of the national electricity system.

As governed by the Concession, the operator of the grid, in carrying out his own activities, performs for users the services briefly described below.

a) Transmission service.
The service of transport and transformation of electrical energy along the national transmission grid, from the production plants and lines interconnected to foreign countries to the local distribution grids. This service includes the activities of connection, development, use and maintenance of the grid.

b) Dispatching service.
The service aimed at maintaining the balance between the input and withdrawal of electrical energy, with necessary reserve margins. The service consists in activities aimed at issuing instructions for the coordinated use and operation of production plants, the transmission grid and ancillary services.

c) Metering service.
The activity aimed at obtaining the measurements of electrical energy in the points of energy input, withdrawal and the interconnection points, and the recording of energy flows of the various users.

d) Metering aggregation service.
The activity aimed at collecting the measurements reported by the distribution companies as well as the measurements of electrical energy regarding the points of energy input located within the Operator's Grid.

In addition to the abovementioned services, the Operator shall collect statistical data regarding the production and consumption of the national electricity industry, process such data and make it available by publishing specific documentation.

1.3.3 Electricity Market

The "Italian energy stock exchange", as the electricity market is commonly defined, allows electricity producers, consumers and wholesalers to enter hourly electricity purchase and sale contracts. Transactions occur on a web platform which the operators connect to through the internet, with safe access procedures and through digital certificates, to finalize online electricity purchase and sale contracts.

[2] D.P.C.M. 11 maggio 2004 in materia di unificazione tra proprietà e gestione della rete e sulla base delle direttive dell'Autorità per l'energia elettrica e il gas di cui alla delibera n. 250/04. http://www.terna.it/default/Home/SISTEMA_ELETTRICO/codice_rete.aspx

The electricity market, namely the place where transactions involving electricity are conducted, was set up in Italy as a result of Legislative Decree n° 79/99 ("*Decreto Bersani*") as part of the implementation of the EU directive on the creation of an internal energy market (Directive 96/92/EC repealed by Directive 2003/54/EC).

The electricity market is divided into:

1. Day-Ahead Market - MGP
2. Intra-Day Market - MI
3. Dispatching Services Market - MSD

In the MGP and MI - also referred to as Energy Markets - producers, wholesalers and end customers, as well as Acquirente Unico (AU) and Gestore dei Servizi Energetici (GSE) buy and sell wholesale quantities of electricity for the next day. These markets, which are managed by Gestore dei Mercati Energetici (GME), define system marginal prices at which the energy is traded.

In the MSD, Terna procures the resources it needs to manage and control the system (solving intra-national congestions, creating energy reserves, real-time balancing).

2. Structure of Industrial Control Systems in a Generation Power Plant

The following schematic represents the industrial network architecture that was typically employed till 5-10 years ago to interconnect the devices of the Industrial Control System chosen for the Italian case study and on which the cost of applying the standard should be evaluated for cyber security purposes.

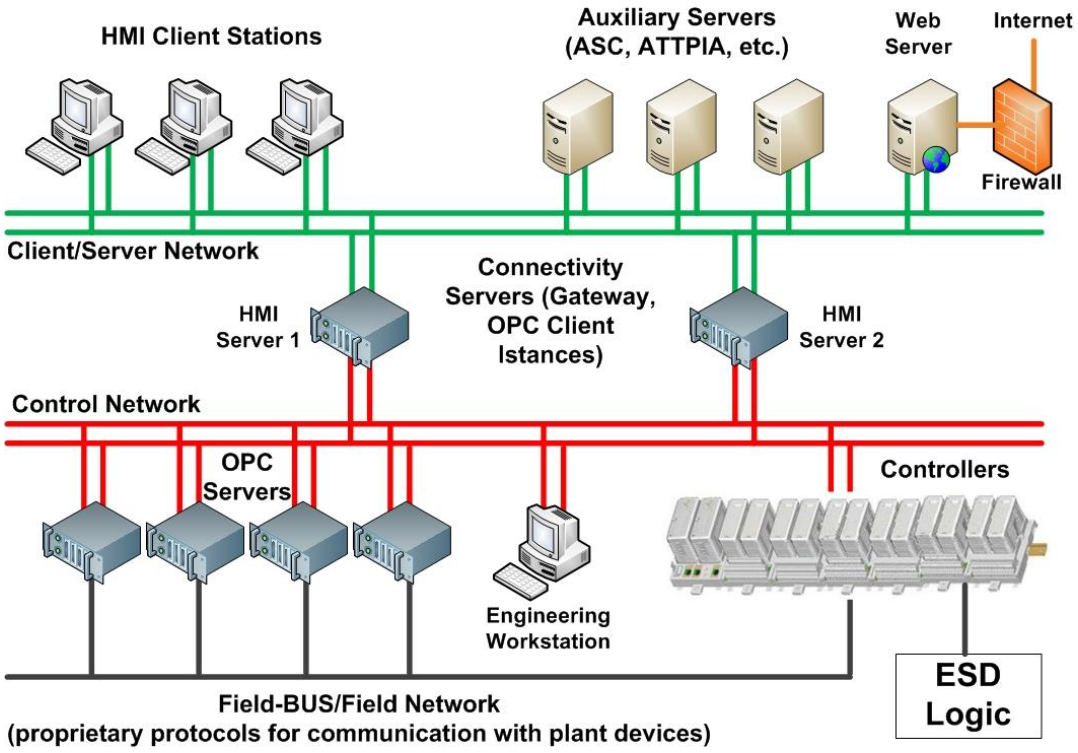

Figure 1: typical network architecture in ics

Network is composed of two subsections:

- Upper section is the Client/Server network that connects all HMI Client Stations of the SCADA and all auxiliary servers .
- Lower subsection is the Control Network which connects controllers, OPC Servers (Front End Servers) and Engineering Work Stations.

A redundant server (on which the SCADA software is installed) works together as gateway to interconnect Client/Server and Control networks and may also work as HMI Client Stations.

Front End Servers on control network communicate with the devices on field using proprietary protocols and make the collected data available, in general, on OPC standard protocol. Collected data from field travel from OPC server to HMI Client Station passing through the redundant servers on which OPC Client instances are properly configured.

Data exchange between the connectivity servers and the HMI Client stations on the upper subsection of the ICS network is performed internally at the SCADA software using an Ethernet based protocol.

The industrial network presented above implements the following redundancy protocols:

- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP: recovery time of 1-20 seconds) for the Client/Server Network.
- the IEC 62439 Medium Redundancy Protocol (MRP: recovery time max 500ms) that has been chosen for the Control Network.

3. ATTACK SCENARIOS

Industrial processes controlled and monitored through Supervisory Control And Data Acquisition (SCADA) computer systems are affected by vulnerabilities that can be exploited; this has been proven by Stuxnet, a Windows-specific computer worm discovered in June 2010, able to spy and reprogram ICT systems of critical industrial infrastructure. For this reason in the Italian case study two scenarios will be taken in considerations:

1. Attack performed infecting the computers of a control system with a generic malware able eventually to replicate itself on the network and to affect the control operation.
2. Attack performed in order to saturate the network traffic and affecting the entire functionality of the control system (DOS attack). This is achieved by corrupting somehow the functionality of a network apparatus (switch, hub, etc.).

3.1 Infection methodologies

Malicious code, not detected by the antivirus software, is executed on the connection of a mass storage device (USB pen-drive or optical disc drive).

3.2 Attack effects on the industrial control system network

Both attack typologies considered for the case study would generate dramatic consequences on the network performance but with different dynamics and with different duration of the recovery procedures to be applied in order to bring back the industrial system to the healthy condition.

After the attack, regardless the methodology applied to perform it, the system would become unable to handle the communication and to distribute the process information on the network. PLCs and RTUs would not be able to monitor in real time fundamental process parameters or to produce consistent outputs. The general effect is therefore the impossibility to guarantee the correct execution of essential process stages (like the water and steam cycles in a Combined Cycle Gas Turbine power plant).

Such a situation, if recognized to be critical, must bring to an emergency stop procedure of the production in order to avoid damages to the plant facilities. The emergency procedure can be started by the operator who decides according the circumstances to push the emergency stop push-button (also known as the "red mushroom").

But power plant design includes safety mechanisms to automatically intervene in case of remarkable drifts from the safe process operation: the system in charge of implementing such mechanisms is known as the Emergency Shut Down system or simply ESD system. So when the plant status becomes critical the probability of a shut-down (operator or automatically started) becomes very high.

3.3 Intervention methodologies after the attack and recovery time spans

The intervention methodologies after the attack and the time required to solve the originated effects depend on the attack scenario that brought the system to shut-down.

In case of malware attack the time necessary to cure the infection can be longer than the attack performed directly on a network apparatus like a switch, because the attack would be probably coming from several nodes of the network, making much more difficult the detection of the computers involved in the attack dynamic.

In the other considered scenario (D-DOS or broadcast storm originated from one or more switch/routers), the attack would affect only few network devices, so that they can be immediately isolated and tested in order to recognize any abnormal behaviour.

Till now it has been considered that a cyber-attack (regardless the specific scenario) would generate a collapse of the industrial network making the process not controllable through the SCADA, bringing to the extreme consequence of a plant emergency shut-down.

The power generation plant that was stopped under emergency condition cannot be restarted immediately because there are operations necessary to warm up the process before going back to the operation speed. So, apart from the time required to recognize the attack and to choose and apply the intervention methodologies, there will be an additional time to warm up the process whose duration depends on the time that passed from the emergency shut-down and the time when the network becomes fully functional again. Table 1 gives an idea of the intervention span time.

Table 1: intervention span time

Attack Scenario	Estimated network recovery time (hours)	Plant warm up time (hours)	Total recovery time (hours)
Malware	12-48	1-6	12-56
DDOS	6-8	1-2	6-10

So, from a temporal point of view the total recovery time necessary to make the system healthy again involves a component related to the attack effects on the communication and the warm-up time before restarting the power production.

4. ITALIAN CASE STUDY

4.1 General framework

In order to identify the proper case study, the following considerations have been made: European TSOs identify the most critical node capacity of about 3.000 MWe (near French nuclear power plants) and protect themselves from a loss of power equals to the one of the most critical nodes (N-1 network security criterion).

In order to consider an event on the Italian territory as critical, the event should occur together with other conditions (because there is not in Italy a node managing power close to 3.000 MW).

In case the attack generates a condition that is not immediately recovered due to network congestion or to economic constraints (cross-border contracts), load shedding takes place in order to balance the power lost, according to a priority list. If the situation has not been restored within a reasonable time (about 1.5h) blackout turnovers take place (groups of users who joined to the PESSE program).

After examining these conditions, for the Italian case study it has been decided to include in the scenario some concurrent events:

- a critical high voltage line connecting a wide geographical area to the other part of the National Transmission Grid (NTG) is put under maintenance;
- the wide geographical area (where also industrial facilities operate) is isolated from the rest of the NTG because of the line under maintenance but keeps on self-supplying thanks to the generation plants on the local sub-grid;
- an informatics attack is performed on the power generation plant with the highest capacity operating in the isolated area causing the plant shut-down;
- outage of other plants occurs because of the rough frequency transient on the grid causing the blackout of the entire area.

This scenario fulfils two important requirements, such as the severity of the event and the easy way to assess the consequences being therefore compliant with the scope of the project.

4.2 Scenario for the cyber-attack on a Power Plant in Italy

As stated before, we consider that the attack is performed in conjunction with the maintenance of a critical transmission line (because any hacker usually acts when the system is already under weak conditions). Even if disconnected from the grid, the area keeps supplying itself thanks to a subnet of generation plants (whose capability is summed up in Table 2) still able to afford industries facilities and final users' demand in the isolated area.

Table 2: main plants in the case study area

Plant	**Type/fuel**	**Gross power (MW)**
Power Plant A	Thermoelectric	1280 MW
Power Plant B	Thermoelectric	774 MW
Power Plant C	Thermoelectric	1340 MW
Power Plant D	Hydroelectric	500 MW
Power Plant E	Gas Turbine	180 MW
Power Plant F	Thermoelectric	470 MW

Moreover, there are photovoltaic and wind distributed generators with a total gross power of 2500 MWe.

In case of cyber-attack able to shut down the generators of the power plant providing the greatest energy capability (in this case Plant C), the transition on the grid causes a considerable reduction of the frequency and the detachment from the grid of other systems (e.g. Plant B). The simultaneous unavailability of two large generating plants on the grid, isolated from the rest of NTG, must surely imply a total blackout on the entire area.

The re-start up plan begins soon after the blackout, in order to restore voltage and frequency of the transmission grid. In the time range between 1 and 3 hours other plants (including renewable sources) can be recovered leading to get back other power.

It's plausible to consider at least 6 hours to fully recover from the blackout and to come back to the steady situation in case of blackout of the area hosting the facilities listed in the table above.

4.3 Timeline

In the Table 3 the main events between 10:00 and 16:00 of the selected day (i.e. the day chosen for the simulation for which the load profile is precisely known) after the attack are listed.

Table 3: timeline of events between 10:00 and 16:00

Time (hh:mm)	Event	Situation on the electric grid
10:00	Cyber-attack to Power Plant C with sudden shutdown	3.000 MWe as instantaneous load
Few seconds after 10:00	Frequency fall with detachment of Power Plant A, Power Plant B and other plants from the grid.	Total blackout with power falling to 0
10:05	Re-start plan begins: black start Power Plant D, Power Plant E.	No power. Voltage and frequency of the grid towards the nominal values.
10:15	Energisation of first electric bus bars in primary substations closer to the major cities of the area).	No power. Voltage and frequency at nominal values. Increase in power at a rate of 2 MW/min (30 MWe/15 minutes). Priority given to residential use in great towns.
11:15	Some functionalities on the grid and some power plants are recovered, facilitating the speed of power increase	120 MW recovered on the grid. From now on, increase in power at a rate of 4 MW/min (60 MWe/15 minutes).
13:15	TERNA recovers the functionalities of the line connecting the area to the rest of NTG. Synchronization with the grid of the NTG and other power plants (also renewable) in the area begin to produce.	600 MW recovered on the grid. From now on, increase in power at a rate of about 13,3 MW/min (200 MWe/15 minutes).
16:00	The situation is completely restored with the load profile equal to the unperturbed situation	2920 MW as average value on the grid in the period 16:00 – 16:15

4.4 Evaluation of the impact on the load profile

In order to evaluate the socio-economic impact of the blackout, it is necessary to set the day on which the attack occurs and to define hour by hour the load profile of the area in the unperturbed case and in the case of blackout.

Once the day and the hourly load profile has been set, it must be established the load profile for each major category of users: agriculture, industry, commercial (services/tertiary), residential. Moreover, for an accurate assessment of the effects of a power failure for a given period, consumption for different subcategories of industry and commercial/services will also be evaluated.

For the sake of simplicity of calculation, assessments of production and consumption of energy will be carried out for discrete intervals of a quarter of an hour.

4.4.1 Daily load profile without attack

Once fixed the reference day, the hourly load profile for the entire Italy is provided by Terna in the statistical data series. The hourly load profile for the interested area is extrapolated using a factor proportional to the annual consumptions rate. This hourly profile is then processed to get a more detailed profile, quarter-hour based. This greater detail is required to achieve an accurate reconstruction of the process of recovery subsequent the blackout. The process of "smoothing", that produces 96 values of the day, preserves the total energy consumed in the day: 61,994 MWh.

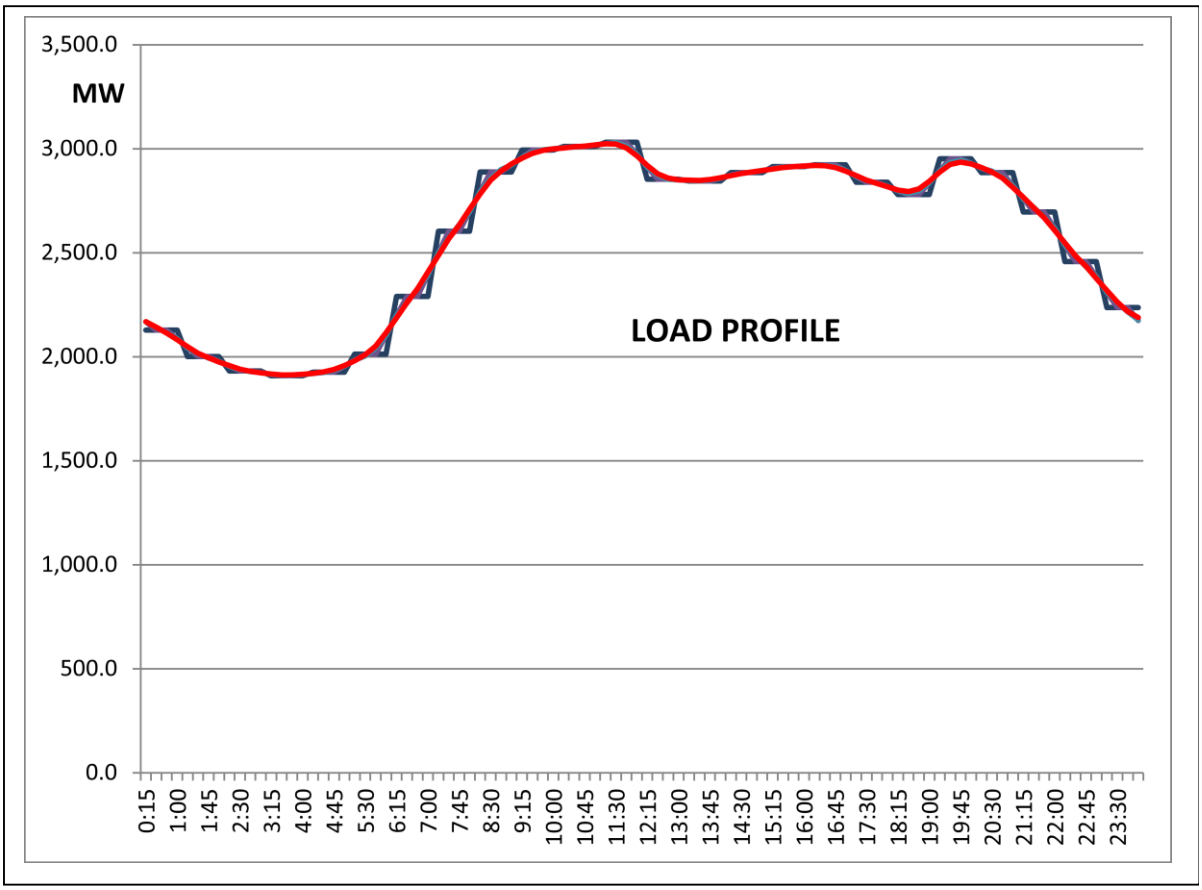

Figure 2: load profile for the day n which the hypothetical attack is simulated

Figure 2 shows the load profile where is visible also the transition from the hourly profile to the more detailed one. The daytime load remains persistently over 2,500 MW and even above 2,800 MW in the period considered for the effects of the attack (from 10 to 16). More complex is the assessment of the consumption profile for the different categories of users. There are four main categories: agriculture, industry, services (tertiary) and domestic/residential. For an accurate assessment of socio-economic impact, however, it seems necessary a further division into sub-categories. Terna provides a significant detail for industry and services/tertiary; agriculture and residential users on the other hand do not have subcategories.

Table 4: categories and subcategories of final electric users

AGRICULTURE
INDUSTRY
- **Basic Manufacturing**
  - Iron and Steel
  - Non-Ferrous Metals
  - Chemistry
  - Building Materials
  - Paper Industry
- **Non Basic Manufacturing**
  - Food
  - Textiles, Clothing and Footwear
  - Mechanics
  - Means of Transportation
  - Plastic and Rubber Processing
  - Wood and Furniture
  - Other Manufacturing
- **Construction**
- **Energy and Water**
  - Fuels Extraction
  - Refining and Coking
  - Electricity and Gas
  - Water Supply

SERVICE INDUSTRY (TERTIARY)
- **Saleable Services**
  - Transport
  - Communications
  - Trade
  - Hotels, Restaurants and Bars
  - Credit and Insurance
  - Other saleable Services
- **Not Saleable Services**
  - Public Administration
  - Public Lighting
  - Other not saleable services

RESIDENTIAL

By analysing the values of the profiles, some categories appear to be quite relevant for electricity consumption. Table 5 below shows the top 10 categories, out of 24, which represent more than 82% of the total daily consumption.

Table 5: Daily consumption of the main subcategories

Main Category	Subcategory	MWh	%
RESIDENTIAL		15.967	25,8%
Industry	**Refinery and Energy**	9.961	16,1%
Industry	**Chemistry**	6.023	9,7%
Services	**Trade**	4.704	7,6%
Services	**Other Saleable Services**	4.588	7,4%
Industry	**Water Supply**	2.502	4,0%
Services	**Hotel, restaur. and pub**	2.252	3,6%
Industry	**Building Materials**	1.767	2,9%
Services	**Public Administration**	1.698	2,7%
Industry	**Electric electronics mechan.**	1.681	2,7%
TOTAL		**51.144**	**82,5%**

Figure 3 shows the profile divided, for better readability, only in the four main categories

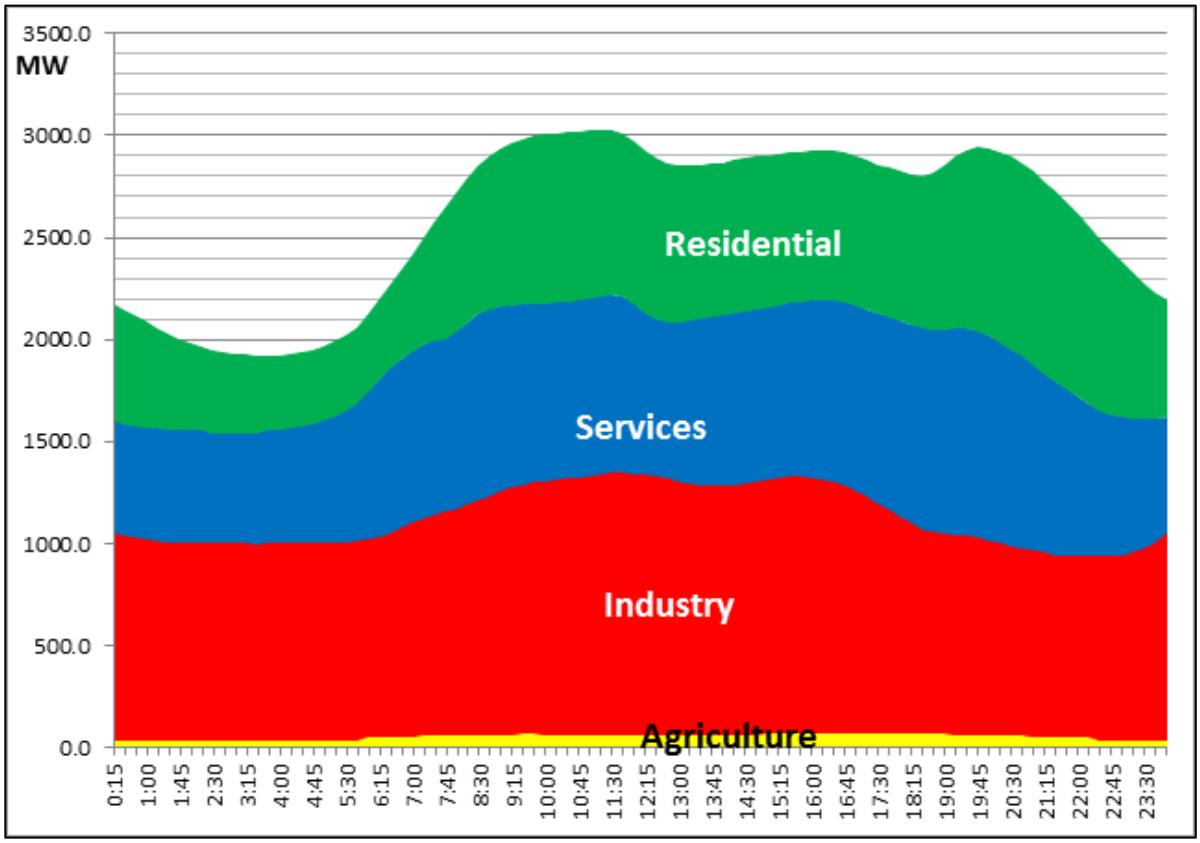

Figure3: hourly load profile without the attack

4.4.2 Daily load profile with attack

In Figure 4 it is reported the evolution of the hourly load profile, total and for the various categories, resulting from the attack. Once the overall trend in the 6 hours of blackouts is defined, that it is defined the profile for the 24 quarters of an hour from 10 to 16 as shown in Fig 4.2, it is necessary to allocate the consumption (or average power in each quarter of an hour) in the subcategories of industry and services. In the absence of specific directions, the best solution is to divide the consumed energy in proportion of all subcategories.

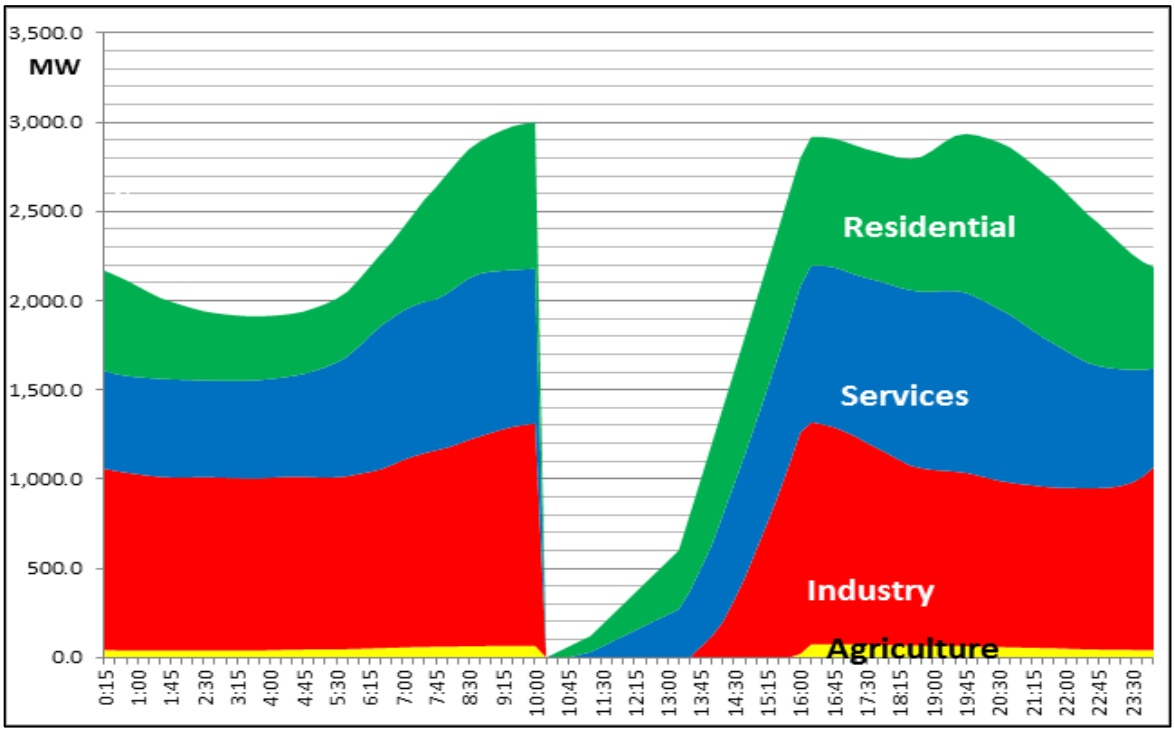

Figure 4: Hourly load profile with the attack

Finally, the effects of blackouts can be summarized in Table 6, which shows the energy (MWh) consumed in the period 10:00 – 16:00 for the different categories of users without and with blackout.

Table 6: Energy consumption (MWh) without and with black-out by user categories in the period 10:00 – 16:00

Category	**Unperturbed situation MWh**	**With black-out MWh**	**Energy not delivered MWh**	**% not delivered in the period**
Agriculture	406,3	23,5	382,8	94,2%
Industries	7852,7	1743,7	6108,9	77,8%
Services	5229,3	2343,4	2885,9	55,2%
Residential	4780,9	2424,2	2356,6	49,3%
TOTAL	18269,1	6534,9	11734,2	64,2%

5. EVALUATION OF SOCIO-ECONOMIC IMPACT

5.1 Evaluating the cost of blackouts

Blackout cost evaluation is a complex issue. The main difficulty relies to the fact that, although markets for electricity exists, markets for interruptions do not, therefore it is not possible to rely on market prices to estimate the economic value of electric supply continuity.

Nevertheless, in the economic literature several methods have been developed to infer the cost of electricity interruptions. De Nooij et al. (2007) [3]provide a taxonomy.

- *Stated preferences methods*, based on surveys. Interviewed people are asked to state a value for blackouts, either in terms of amount they would pay to avoid or reduce the interruption (willingness to pay - WTP) or in terms of amount they would like to receive as a compensation for an increase in interruptions (willingness to accept – WTA). They can also be asked to choose among given combinations of interruption characteristics and monetary values. This method is useful since it relies on preference directly elicited from the interviewees. The main drawback is related to the fact that this approach can be prone to different types of bias of cognitive source; in particular the way question are asked plays a major role (see for instance Beenstock et al., 1998[4]; Carlsson and Martinsson[5], 2008)
- *Production function approach*, which estimates the damages from interruptions in terms of lost production (non-households) or lost leisure time (households). The damage is proportionally related to the energy lost, since the underlying assumption is that no productive activity is possible in absence of electricity (in the same vein, leisure time cannot be enjoyed in case of electricity interruptions). The main advantage is that the application is straightforward once macro-economic data on production and energy consumption are publicly available. The main drawbacks rely on the fact that the result is an approximation of the total damage (some authors identify this category as *proxy methods*), as it ignores factors such as restarting times, damages to equipment or non-complete energy dependence. Nevertheless, the literature agrees in recognizing that these approaches provide a good estimate of the order of magnitude of the global damage. More advanced applications, requiring a broader set of information, rely on input-output matrices to consider the interdependence across different sectors or on methods assigning a positive cost for load disconnected in addition to the cost for energy non-supplied. For recent examples of application of this approach, see De Nooij et al. (2007); Leahy and Tol (2011)[6]; Linares and Rey (2013)[7].

[3] De Nooij, M., Koopmans, C., Bijvoet, C. (2007). The value of supply security. The cost of power interruptions: economic input for damage reduction and investment in networks. *Energy Economics,* 29, pp.277-295.

[4] Beenstock, M., Goldin, E., Haitovsky, Y. (1998). Response bias in a conjoint analysis of power outages. *Energy Economics,* 20, pp. 135-156.

[5] Carlsson, F., Martinsson, P. (2008). Does it Matter When a Power Outage Occurs? A Choice Experiment Study on the Willingness to Pay to avoid Power Outages . *Energy Economics, 30,* pp.1232-1245.

[6] Leahy, E., Tol, R.S.J. (2011). An estimate of the value of lost load in Ireland. *Energy policy,* 39, pp.1514-1520

[7] Linares, P., Rey, L. (2013). The cost of electricity interruptions in Spain. Are we sending the right signals? *Energy Policy,* 61, pp.751-760.

- *Revealed preference methods*, based on market behaviour. This methods infer the value of supply security by observing some particular choices of electricity users, such as the purchase of backup facilities or the use of interruptible contract (Caves et al., 1992)[8]. This approach has the appealing feature of relying on real market choices. On the other hand, these choice options are available for few users categories (mainly large users), while no information would be provided with respect to the other segments.
- *Case studies*. The common feature of this set of approaches is the presence of a real blackout. The consequence of the blackout can be listed and monetized, or a survey can be carried out immediately after the event (Serra and Fierro, 1997[9]). The main desirable property of this method is that it allows to evaluate the consequences of a real event. However, the possibility of generalizing or extending the evaluation to other events is very limited.

Finally, the different approaches are not mutually exclusive: Reichl et al. (2013)[10] employ the stated preference approach for households and a production function approach enriched with information collected through firms' survey for the productive sectors. After a careful evaluation of the *pros and cons* of the available methods, we have chosen to employ a mixed strategy based on the former two methodologies because they can be more easily generalised and then adapted to hypothetical blackout scenarios involving all the users' types. We will rely on stated preference (surveys) for households, since we believe that this method better captures the main source of damage for families, which is likely to be of psychological rather than of material origin. On the other hand, the very low response rate registered by the previous studies relying on firms surveys led us to prefer a production function approach based on local macro-level data of production (value added) and electricity consumption, which can be retrieved from public statistics.

5.2 Damage for non-households

As stated in the previous subsection, we have decided to rely on a "production function" approach to evaluate the damage for non-residential users. This approach presents the important advantage of being of straightforward application, once the necessary macro-economic information are available. The approach in its simplest formulation estimates the damage for each sector relying on a constant measure of Value Of Lost Load (VOLL) computed for each sector as a ratio

$$VOLL_i = \frac{VA_i}{EC_i}$$

Where $VOLL_i$ is the value of lost load for sector i, VA_i is the annual value added and EC_i is the annual energy consumption, both referred to the same sector. This simple method implies a linear relationship between lost production (expressed in terms of value added) and energy non supplied. It constitutes a proxy

[8] Caves, D.W., Herriges, J.A., Windle, R.J, (1992). The cost of electric power interruption in the industrial sector: estimates derived from interruptible service programs. *Land Economics*, 68, 1, pp.49-61.

[9] Serra, P., Fierro, G. (1997). Outage cost in Chilean Industry. *Energy Economics*, 19, pp. 417-434.

[10] Reichl, J., Schmidthaler, M., Schneider, F. (2013). The value of supply security: the cost of power outages to Austrian households, firms and the public sector. *Energy Economics*, 36, pp.256-261.

of the actual damage that would occur in case of interruption since it relies on several assumption and simplifications (see De Nooij et al. 2007 and Billinton et al. 2001[11]).

1) It ignores potential costs related to damaged equipment, which are more likely in some sectors than in others, and which are probably not directly linked to the quantity of energy non delivered.
2) It assumes that the damage correspond to the lost value added, i.e. the value of production net of the external purchases. Indeed, it is in general reasonable to assume that when production is stopped, firms do not employ (i.e. save) material and services (including energy). Nevertheless, in some processes also some external input can be lost. For instance, this is the case of perishable raw materials, or energy in productions where temperature must be kept high or low and an interruption implies re-heating or re-cooling operations.
3) It ignores re-starting times, which can be very relevant in some industries.
4) It does not consider that some kinds of activities can be carried on even in absence of electricity. Their weight largely depends on the type of production.

The drawbacks described in points 1) to 3) would imply an underestimation of the total damage, while the issue in 4) would lead to an overestimation; these effects are likely to compensate each other. Globally, as pointed out in De Nooij et al. (2007), and Billinton et al. (2001), the model can be considered a valid method to provide a reliable evaluation of the order of magnitude of the total damage, for general policy evaluations, the main aim of this study, although it could not be sufficiently reliable for accurate sector-specific considerations. The total damage can be computed by multiplying the VOLL of each sector by the total energy non delivered to the same sector, and subsequently by summing the products.

The data on sector value added are published by ISTAT[12]. The national aggregates are available up to the year 2012, but we prefer to rely on territorial data, published up to 2008. Therefore, the value added amounts have been adjusted for inflation to the first quarter of the year 2014 using the production price index for industrial goods. The data on annual electricity consumption are published by Terna, and disaggregated by sector and geographical areas. Since the sector classifications employed by ISTAT and Terna do not match perfectly, some sector have been aggregated to ensure perfect correlation between value added and consumption. The VOLL for each sector has been computed using the formula stated above.

We would like to point out that the electricity sector has been excluded from this evaluation and will be treated separately in the following sub-section. In fact, although a certain level of auto-consumption exists, we did not consider correct to evaluate the lost production of electricity as function of electricity itself.[13]

---

[11] Billinton, R., Abilgaard, H., Alabbas, A.M., Allan, R.N., Arnborg, S., Bogoi, C., Bozic, Z., Goncalves, L.F.M., Dialynas, E., Holen, E.A.T., Logan, D., Manning, T., Neves De Mesquita, E., Schmitt, O., Shirani, A.R., Simpson, B., Yinbiao, S. (2001). Methods to consider custode interruption costs in power system analysis: task force. CIGRE, Paris, France.

[12] Aggregates of the territorial accounts for activity branch.

[13] To apply this refinement, data on consumption and value added have been isolated. Terna provides separate consumption information for the sector, while value added appears aggregated for electricity, gas and water supply. Therefore we have separated the value for each one of the three sectors in proportion to the number of employees in 2008 (obtained by interpolating the ISTAT data of 2001 and 2011), and accounting for the sector differences in the amount of value added per employee (estimated using the data for the local firms included in AIDA, a dataset provided by Bureau van Dijk).

The average VOLL computed for the entire productive system in the impacted area is 5.92 €/kWh. For comparison purposes, we can for instance see that this value is consistent with the findings of Linares and Rey (2013) for Spain (5.56 €/kWh, excluding residential), but it is lower with respect to the finding of De Nooij et al. (2007) for the Netherlands (7.59 €/kWh)[14]. The following table reports the computed levels of VOLL that, multiplied by the amount of energy non-supplied estimated in the previous chapter, generate the blackout damage reported in the last column (total value of 45.7 euro millions).

The partial VOLL measures are in general of the same order of magnitude as in the previous studies, with some exceptions, probably related to the production mix internal to the category. For instance the chemical sector, presents a particularly low VOLL; on the other hand the textile and the construction sectors show higher values.

Table7: "Average" damage evaluation.

SECTOR	**VOLL (€/kWh)**	**Energy non supplied (MWh)**	**Lost VA (€/000)**
AGRICULTURE	6.73	382.77	2575.09
INDUSTRY			
Manufacturing of food product, beverages and tobacco	3.02	389.86	1177.40
Manufacturing of textile and textile products and leather products	10.25	14.38	147.47
Manufacture of coke, refined petroleum products and nuclear fuel, chemical and pharmaceutical	0.35	3248.13	1124.18
Mechanical equipment, electric and optical equipment, transport equipment	2.89	544.34	1573.69
Gas	17.90	21.64	387.43
water	1.61	718.89	1157.41
Construction	59.99	68.35	4100.49
Industry other	1.96	910.71	1788.61
TERTIARY			
Commercial	5.35	787.90	4213.76
Hotels and restaurants	3.33	377.22	1256.27
Financial intermediation	26.03	53.74	1398.84
Services (other)	14.89	1667.00	24827.31
TOTAL DAMAGE			**45727.95**

[14] In current values for the first quarter 2014.

As a refinement, we will try to modify our evaluation to account for the fact that some of the considered industries manage activities which are not strictly dependent on electricity supply (see Linares and Rey,). Construction is an example of such industries. Also for financial services, although strictly dependent on information system mainly electricity-based, we can assume that the main output (i.e. financial rents on investments) is not lost in case of blackout. Finally, most agricultural activities depend only weakly on supply continuity, with probably an exception for breeding. Therefore we have chosen to provide also a "prudential" version of the total damage, computed by setting to zero the VOLL for construction and financial service, while for agriculture we maintain the 7% of the VOLL, representing the share of breeding on the total agricultural activities in the interested area (computed either in terms of number of firms or of number of employees). This value can be interpreted as a "minimal" one, since the damage for sectors with evident low electricity dependence has been set to zero, while additional cost component are still not considered. Therefore, this value can be reasonably be taken as very close to the lower bound of the possible damage. Table 8 reports the results of this prudential computation, highlighting a total damage for non-households sector of about 37.8 euro millions.

Table 8: "Prudential" damage evaluation

SECTOR	**VOLL (€/kWh)**	**Energy non supplied (MWh)**	**Lost VA (€/000)**
AGRICULTURE	0.47	382.77	180.26
INDUSTRY			
Manufacturing of food product, beverages and tobacco	3.02	389.86	1177.40
Manufacturing of textile and textile products and leather products	10.25	14.38	147.47
Manufacture of coke, refined petroleum products and nuclear fuel, chemical and pharmaceutical	0.35	3248.13	1124.18
Mechanical equipment, electric and optical equipment, transport equipment	2.89	544.34	1573.69
gas	17.90	21.64	387.43
water	1.61	718.89	1157.41
Construction	0.00	68.35	0.00
Industry other	1.96	910.71	1788.61
TERTIARY			
Commercial	5.35	787.90	4213.76
Hotels and restaurants	3.33	377.22	1256.27
Financial intermediation	0.00	53.74	0.00
Services (other)	14.89	1667.00	24827.31
TOTAL DAMAGE			**37833.78**

Finally, we propose a third evaluation applying the electricity dependence shares used by Linares and Rey. The shares should reflect the weight of the processes for which electricity is a necessary input. The authors, however, define the employed shares as a "best guess" of the actual part of value added lost in case of blackout, since no empirical support is available at the moment. However, we can see that this third evaluation provides a global damage evaluation of a similar order of magnitude with respect to the previous one (34.6 euro millions).

Table 9: Damage evaluation with energy dependence coefficients

SECTOR	**VOLL (€/kWh)**	**Energy dependence (share)**	**VOLL CORRECTED (€/kWh)**	**Energy non supplied (MWh)**	**Lost VA (€/000)**
AGRICULTURE	6.73	0.40	2.69	382.77	1030.04
INDUSTRY					
Manufacturing of food product, beverages and tobacco	3.02	0.90	2.72	389.86	1059.66
Manufacturing of textile and textile products and leather products	10.25	0.90	9.23	14.38	132.72
Manufacture of coke, refined petroleum products and nuclear fuel, chemical and pharmaceutical	0.35	0.90	0.31	3248.13	1011.76
Mechanical equipment, electric and optical equipment, transport equipment	2.89	0.90	2.60	544.34	1416.32
gas	17.90	0.90	16.11	21.64	348.69
water	1.61	0.90	1.45	718.89	1041.67
Construction	59.99	0.40	24.00	68.35	1640.20
Industry other	1.96	0.90	1.77	910.71	1609.75
TERTIARY					
Commercial	5.35	0.80	4.28	787.90	3371.00
Hotels and restaurants	3.33	0.80	2.66	377.22	1005.01
Financial intermediation	26.03	0.80	20.82	53.74	1119.07
Services (other)	14.89	0.80	11.91	1667.00	19861.84
TOTAL DAMAGE					**34647.74**

5.3 Damage for the electricity sector.

The cost of a blackout for the electricity sector will be evaluated in terms of value of the energy non-supplied to final customers.

For generators, the lost revenues can be expressed in terms of energy not sold evaluated at the market price of that day.

We will employ for this purpose the actual hourly market prices registered for the day chosen for the hypothetical attack (Source: GME), which will be multiplied by the energy non delivered in each hour of blackout (the amount of energy non-delivered is net out of the auto-consumption of the electricity sector itself).

The following table show the results.

Table 10: Damage for the electricity producers

Time	Price (€/MWh)	Energy not sold (MWh)	Lost revenues (€)
10	115	2927	336,655
11	115	2753	316,696
12	115	2387	274,548
13	90	1914	172,297
14	90	1157	104,138
15	90	403	36,268
TOTAL		11,542	**1,240,602**

In order to achieve a damage evaluation homogenous to the one proposed in the previous paragraph, in terms of value added, we net out from the total revenue lost the corresponding cost of gas (the main external input), evaluated in 52.83 €/MWh.[15]

Therefore the total loss in terms of value added can be approximated as:

1,240,602 – (11,542 * 52.83) = € 630,838 VA lost for generators (in current value for 2012).

For homogeneity with the other part of the analysis, we would like to express this value adjusted for inflation to the first quarter 2014.

We got a value of **VA lost for generator equal to 636,169[16].**

15 This unitary cost has been obtained by dividing the average wholesale gas price for the period (28 €/Mwh) by an efficiency coefficient of 53% (AEEG, 2013). Therefore, the cost of producing 1 MWh of electricity by means of a thermal plant should generate an average cost of 28/0.53 = 52.83 €/MWh.

16 The consumer price index has been employed.

For the other operators of the electricity chain, it is possible to approximate the total damage using the value of the different component of price (price for residential users in the fourth quarter 2013 is employed), retrieved from CCSE and Autorità per l'Energia Elettrica, il Gas e il Sistema Idrico.

Table 11: Damage for the other electricity operators

	Value of the price component (€/MWh)	**Energy non-supplied (MWh)**	**Total damage (€)**
Dispatching	10,8	11.542	124.654
Supply	7,7	11.542	88.873
Network	27,7	11.542	319.713
System costs	37,1	11.542	428.208
Taxes	25,4	11.542	293.167
TOTAL			**1.254.615**

5.4 Damage for households

For households we have adopted a stated preference method based on customer surveys. The approach relies on a choice experiment, where the choice questions were set in terms of willingness to accept (WTA) blackouts of certain durations, provided that the supplier would have compensated the household with a bill discount. The respondent was simply asked to state whether or not he would have accepted the interruption (with the discount). A total of 28 scenarios (i.e. combination of duration and discount) were constructed, since we have hypothesized:

- 4 duration levels: 1 minute, 2, 4 and 6 hours.
- 7 discount levels: 1, 7, 13, 19, 25, 31, 37 euros.

In order to not impose an excessive effort on respondents, only 7 randomly chosen scenarios were presented to each one of them.

In the literature the most common approaches rely on willingness to pay (WTP) in order to avoid blackouts. In general, WTP and WTA differ relevantly, with the latter exceeding the former by several times. This is due to the so-called "endowment effect", which is the psychological tendency for an average person to ask an higher compensation to give away something he owns with respect to the amount he would pay to purchase the same good or service.

Therefore we expect *a priori* higher results than in studies relying on WTP.

Nevertheless, we have chosen a WTA approach because, after a careful evaluation, we believe it is more respondent to the need of evaluating a single blackout (rather than more general scenarios describing supply security in terms of interruption frequency and other characteristics). A WTP approach would in this case be not completely suitable, since users' opinion (this is especially true for residential users) is that continuity is a necessary characteristics of the service. An interruption could represent a sort of "pathological" disservice,

and it is very likely that many respondent would be willing to pay no additional money to avoid it, or that the WTP expressed would understate the actual value they assign to the interruption.

The interviews have been mainly carried out by means of online questionnaires (integrated with face-to-face interviews to cover customer segments not easily reachable through the internet) starting from March 2014. The same questionnaire has been distributed in Italy and in Poland (with monetary values converted to local currency) in order to have a sample covering residential users of both the countries involved in the case studies developed through ESSENCE.

We have collected a total of about 500 questionnaires in Italy and 120 in Poland, of which about the 80% was complete and could be employed for the estimates.

The details of the methodology used for the estimation is in the full Benefit Analysis report[17].

We have simulated three possible value of damage for Italian households (i.e. by setting *d_pol*=0):

- the maximum damage, occurring for a family not living in the countryside, with head of the household aged more than 24, with high electricity bill.
- The minimum damage, occurring for a family living in the countryside, with head of the household aged 18-24, paying low electricity bill.
- An average case reflecting a "typical family": not living in the countryside, with a head of household aged more than 24 and an energy monthly cost set at the sample median (€ 39.5).

Table 12: Damage for households

Damage	Maximum case	Minimum case	Average case
Damage per household for 15 minutes interruption in €	3.34	1.79	2.86
Damage per household for 6 hours interruption in €	54.57	32.43	43.04
Total damage in € Millions	**63.8**	**36.1**	**52.5**
Average damage per family in €/kwh	27.06	15.30	22.29
Average damage per family in €/h	10.88	6.15	8.97
Average damage per person in €/h	4.25	2.41	3.52

[17] Clementina Bruno, *et al.*, (2014), *Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case studies*. Ceris Technical report. Special Essence series. N. 52http://essence.ceris.cnr.it/images/documenti/RT_52.pdf

The results, described in Table 12, are very far from the findings of similar work relying on a WTP approach. For instance, Reichl et al. find a WTP of 1.79 €/kWh in winter in Austria, while Carlsson and Martinsson find a WTP of 1.31 € for a four-hours blackout in Sweden.

The values are more consistent with studies that evaluate the residential sector using the "production function" approach, in terms of values of lost leisure time, evaluated at the average hourly income. In fact, De Nooij et al. find a residential VOLL of 20.84 €/kWh and an average damage per person of about 3 €/h for Netherlands, while the VOLL estimated by Leahy and Toll (2011) is above 30 €/kWh from 10.00 to 16.00. Finally, the residential VOLL computed by Linares and Rey is lower: 8.79 €/kWh.

Summing up, our findings seem to provide reasonable estimates of the damage suffered by families during an interruption with the characteristics described in the previous chapters.

6. SELECTED STANDARDS

The frequency of cyber-attacks have increased significantly over the last several years and became more sophisticated and their consequences more dire.

Indeed, enterprises today would do well to expand their efforts to mitigate the consequences of inevitable breaches, which likely affect infrastructure systems and compromise key data.

Security for industrial automation and control systems is similar to general information system security but quite different for some aspects.

Automation and control systems put higher requirements on integrity, availability, performance, and immediate access.

Also, the potential impact of an attack on automation and control systems may include not only financial losses and loss of public confidence, but also violation of regulatory requirements, damage to equipment and environment, and endangerment of public and employee safety.

Adoption of standards and identification of countermeasures to be compliant with them is the first step to prevent such breaches or to manage a cyber-security event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs.

Particularly, the security of industrial automation and control systems become increasingly critical and the potential impact of an attack may be more serious than for computer system in general.

Security measures aim at protecting the integrity of availability of system but security improvement must be a continuous activity.

In order to perform the economic evaluation of countermeasures and standards that should be adopted in order to face and protect a plant's automation and control system, three steps will be performed:

1. analysis of different already existing standards; and the identification of those that fit the best with the protection needs of the considered plant;
2. identification of standard and countermeasures that fit the best with the protection needs of the considered plant and then, to be adopted;
3. costs evaluation and, particularly, evaluation on socio-economic impacts thorough the analysis of a blackout impacts on citizens and industry, agricultural and tertiary.

Standards describe uniform engineering or technical criteria, methods, processes, and practices and may actually be a regulatory requirement. The confusing proliferation of standards and guidance for electric power system cybersecurity has understandably made it more difficult for individual utilities to quickly determine what is required of them and has certainly posed a challenge for those who would like to review or provide input to the many parallel efforts. To be thorough, a general description of standards such as NERC, NIST and ISA will be provided[18].

6.1 NIST

NIST provides guidance for establishing secure industrial control systems (ICS). Particularly, it releases guidelines (NIST SP 800-82) for establishing how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements.

Furthermore, NIST SP 800-53 highlights that changes to the security controls include a new emphasis on secure software development in an effort to shift security away from the focus of the past few years, during which it's targeted matters such as configuration management or continuous monitoring.

6.2 ISA/IEC-62443

ISA/IEC-62443, formerly ISA 99. is a set of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

As depicted in Figure 5: Planned and published ISA-62443 work products for IACS Security all ISA-62443 standards and technical reports are organized into four categories called General, Policies and Procedures, System, and Component, hereafter described:

- *General*: it includes common or foundational information such as concepts, models and terminology. Work products that describe security metrics and security life cycles for IACS are also included;
- *Policies and Procedures* address various aspects of creating and maintaining an effective IACS security program;
- *System Integrator* includes work products that describe system design guidance and requirements for the secure integration of control systems. Focus on the zone and conduit design model;
- *Component* includes work products that describe the specific product development and technical requirements of control system products.

[18] For a complete review of actual and forthcoming standards, please see: Ugo Finardi, Elena Ragazzi and Alberto Stefanini (2013). *Considerations on the implementation of SCADA standards on critical infrastructures of power grids*. Ceris Technical Reports, special Essence series, N. 47. http://essence.ceris.cnr.it/images/documenti/RT_47.pdf

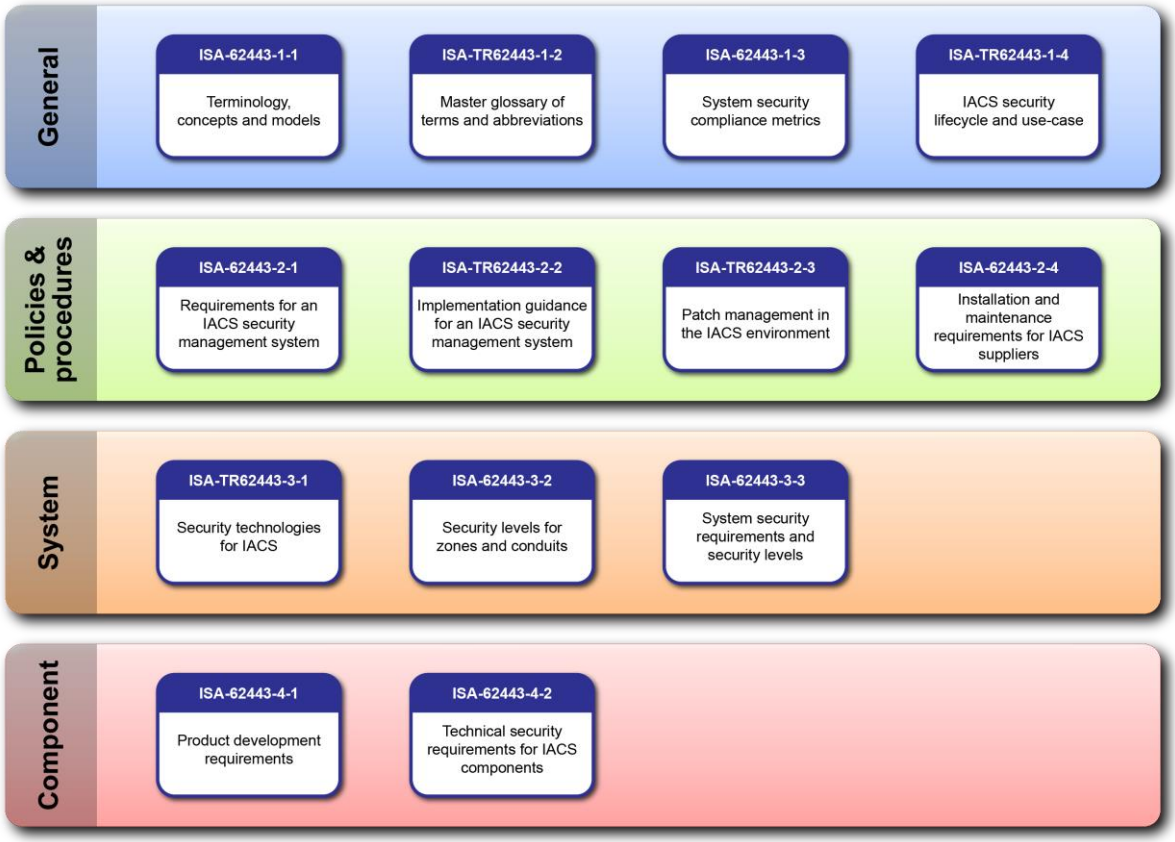

Figure 5: Planned and published ISA-62443 work products for IACS Security

6.3 NERC

NERC (North American Electric Reliability Corporation) mainly works on cyber security standards and guidelines related with secure bulk electric system.

Particularly, the so-called NERC-CIP standard approach, deals with the implementation of the necessary security practices to meet the compliance requirements.

To be more precise, NERC adopted Cyber Security Standards CIP-002 through 009 specifying the minimum requirements needed to ensure the security of the electronic exchange of information for supporting the bulk power system.

NERC-CIP identifies standards in key areas designed to protect power plants and all other aspects of electric utility operations and assets. The standards include:

- provisions for identifying critical cyber assets;
- developing security management controls;
- training;
- perimeter and physical security;
- incident reporting and response planning, and recovery plans.

Summarizing, NERC-CIP establishes standards in eight key areas designed to protect not only power plants, but all other aspects of electric utility operations and assets as shown in the table below:

Table 13: NERC – CIP standards for electric utility operations and assets

SECTION	STANDARD
section 002	The standard includes provisions for identifying critical cyber assets
section 003	Developing security management controls
section 004	Implementing training
section 005	Identifying and implementing perimeter security
section 006	Implementing a physical security program for the protection of critical cyber assets
section 007	Protecting assets and information within the perimeter
section 008	Incident reporting and response planning
section 009	Recovery plans

7. IMPLEMENTATION OF STANDARDS AND COUNTERMEASURES

The standards and countermeasures hereafter proposed result from a deep analysis performed on the standards above mentioned and synthetically described.

Particularly, the selected standards are based on a gap analysis that has been done verifying if the technical specifications of each standard fit with the security requirements of the considered plant.

7.1 Governance Level

The Governance requirements established in International Standards, Best Practices and Policies on the Industrial Control System Security in the Energy Sector SCADA Systems are grouped in the following areas:

- **Security Program**: this area includes all security requirements concerning SCADA and Industrial control system security vision, objectives, goals, strategies, directions, security plans
- **Organization of security**: this area includes all security requirements concerning internal and external (third parties) roles, responsibilities, organization to guarantee SCADA and Industrial control System security
- **Security policy**: this area includes all security requirements concerning policies, procedures and plans of actions on SCADA and Industrial Control System security
- **Risk Management**: this area includes all security requirements concerning risk management approach and methodology in a manner allowing a SCADA and Industrial Control System security risk management

- **Asset Management**: this area includes all security requirements concerning asset management necessary to achieve and maintain appropriate protection of SCADA and Industrial control systems assets.

7.2 Hardening Level

Hardening can be defined as the process of checking and securing a system, through the adoption of specific techniques to reduce system surface exposed to attacks. There are various methods to do hardening; these may involve, among other measures, the choice of services to be used, updating of software packages, configuration optimization, elimination of unnecessary application users, closing open network ports, setting up intrusion-detection systems, firewalls and intrusion-prevention systems.

Table 14 provides the guidelines to implement the capabilities necessary to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

Table 14: Guidelines to implement the capabilities necessary to increase security

HARDENING
Standard
Malicious software prevention The standard indicates the security controls in order to detect record, report and mitigate the effects of malicious code.
Configuration management Process designed to monitor, track, review and more generally, manage the information that describes systems, including all hardware and software.
Cryptography and key management The standard indicates the security controls to ensure a correct implementation of the public key authentication method.
Backup and Recovery The standard addresses: • The backup and restore practices; • Recovery procedures preparation; • Procedures exercises and contingency plan review.
Network security The standard defines requirements concerning network segmentation and access control.
System acquisition, development and maintenance The standard addresses designing cyber security into systems from the earliest development stages. It also involves the maintenance of those cyber security policies and procedures as the system changes throughout its lifecycle.

Human resources security
Prior to employment The standard is intended to provide security guidance for general purpose IT assets as well as control system environment.
Training and awareness The standard doesn't provide very helpful recommendations other than what should be done in traditional environment.
After employment or upon reassignment The standard is intended to provide security guidance for general purpose IT assets, without focusing on automation systems. It addresses the establishment and operation of an Information Security Management Systems (ISMS) but it doesn't contain peculiar indications for Control Assets.
Physical and environmental security The standard provides a comprehensive outline of security controls which may be selected to suit the specific needs of the environment to get protected.
Business Continuity Management The standard states the importance of sound and rehearsed recovery procedures to restore business operations after either a minor or a major disruption.
Incident Management The standard provides regulations about how to detect and react to security incidents, as well as reporting process that may be selected to suit the specific needs of the environment to get protected.
Compliance and Improvement The standard defines the management responsibilities in monitoring, reviewing and improvement. Particularly, the standard defines the main actions that an organization shall implement to guarantee security compliance and improvement.
Access Control The standard defines security requirements for account administration, authentication and authorization and additionally contains commonly implemented technological applications to enforce the mentioned security principles.

7.3 Network Technical Requirements

In the table 15 selected standard and related requirements and guidelines to be adopted have been presented. They are based on the network technical requirements established in International Standards, Best Practices and Policies on the Industrial Control System Security in the Energy Sector SCADA Systems.

Table15: Network Technical Requirements

Standard **Communications and operations management**
Network Architecture The standard gives detailed guidelines and best practices and a specific section about SCADA segmentation architecture is presented. **Firewall** The standard highlights that in the Industrial and Automation Control System firewalls should not be used as a single means of protection. Software and hardware firewalls should be used in connection with other security measures such as IDS-systems, monitoring systems such as netIQ/MOM, and computer software such as Active Directory and VPN (Virtual Private Network). Configuration of firewalls should start with setting up the firewall configuration to deny all traffic, and then looking at the traffic required and only allowing it explicitly. **Network Security Detection** Within a network there should be tools with capability of recognizing and reporting an attempted violation. These systems are called Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Network-based IDS can monitor network activity to detect any attacks while network-based IPS can also block the traffic, then basing its action on a proactive approach. **Network Specific Services** The standard defines very general security controls for external services used in the authorization boundary. **Cryptography** The main technical countermeasure available against these vulnerabilities is cryptography. **Key management** Key management should be supported by an infrastructure that includes hardware, software, processes and so on. A very important special case ok KMI is Public Key Infrastructure, meant to securely manage digital certificates identities. **Bump-in-the-Wire** BitW devices are placed symmetrically on each side of a network between two devices: they communicate with each other and provide efficient (symmetric) crypto services without any modification of the original devices or network. It is universally agreed that BitW solutions are very effective for ICS field communication involving old “legacy” end devices (RTU/PLC/…) on slow physical links as serial ones.

7.4 Host security requirements

In table 16 selected requirements to be adopted have been presented. They are based on the host security requirements established in International Standards, best practices and policies on the Industrial Control System Security in the Energy Sector SCADA Systems.

Table 16: Host security requirements

Standard
Access control
Account management: the standard specifies the controls for managing information system accounts, including establishment, activating, modifying, reviewing, disabling, and removing accounts. *User access, privileges and password management:* The standard specifies how the organization should deal securely with invalid user access and concurrent sessions. *Operating system and application access control:* The standard deals with the ICS in order to provide the capability to define initial authenticator content, change default authenticators upon ICS installation, change/refresh authenticators periodically and protect authenticators from unauthorized disclosure and modification when stored and transmitted. *Remote, wireless and devices access control:* The standard requires that the remote access capabilities that enable control engineers and vendors to gain remote access to systems should be deployed with security controls to prevent unauthorized individuals from gaining access to the ICS. *Identification and authentication:* The standard indicates the correct procedure to identify and authenticate all users (humans, processes and devices), and allow them access to the ICS. The standard requires that the security process is used to verify the identity of a user, process, or device, through the use of specific credentials (e.g., passwords, tokens, biometrics), as a prerequisite for granting access to resources in an IT system. *Audit and accountability:* The standard requires that in an ICS the security controls should provide policies and procedures for generating audit records, their content, capacity, and retention requirements. *System and physical access monitoring:* The standard shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during factory acceptance testing (FAT), site acceptance testing (SAT) and scheduled maintenance.
Communications and operations management
Configuration management: The standard indicates the controls that are used to verified modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Configuration change and change control: The standard requires, for the ICS, the implementation of a formal change management program. This process should be establish the procedures used to insure that all modifications to an ICS network/host meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans.

Backup, Recovery & Availability: This standard indicate the security controls family to provide policies and procedures to implement a contingency plan by specifying roles and responsibilities, assigning personnel and activities associated with restoring the information system after a disruption or failure.

Patch management: The standard indicates the security to implement a systematic approach to managing and using software patches that can help organizations to improve the overall security of their IT systems in a cost-effective way.

Hardening: This standard provides the lines guide to implement the capabilities necessary to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

Malicious software prevention: The standard provide the line guide to implement the capabilities necessary to malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications.

Cryptography and key management: The standard indicates the security controls to ensure a correct implementation of the process of public key authentication method and integrity.

Software and data protection: The standard indicates the security controls to ensure the confidentiality of information on communication channels and in data repositories to prevent dissemination. Particularly, the standard indicates the security controls to provide policies and procedures for limiting the access to media/data to authorized users**.**

System acquisition, development and maintenance

Capacity management, acquisition and acceptance: The standard indicates the security controls to provide the allocation of sufficient audit record storage in according to commonly recognized recommendations for log management and system configuration.

Data validation, retention and error handling: The standard indicates the security controls to provide policies and procedures for identifying, reporting, and correcting information system flaws. Particularly, the standard indicates the security controls to provide the capability to determine whether a given user took a particular action.

Development. This standard indicates the correct guideline to implement a Development Configuration System for the ICS software applications and a Security Plan to test and evaluate the security components.

Maintenance and testing: This standard indicates the security controls to provide policy and procedure for performing routine and preventative maintenance on the components of an information system.

8. COUNTERMEASURES TO BE ADOPTED

The countermeasures stated are possible starting points to counter each threat and permit initial estimation of the total effort required to repulse each threat.

8.1 Countermeasures for the considered Use Case Scenario

Countermeasures against threats are required to ensure that the plants operate well and in particular, to guarantee the security of supply. Particularly, those include all ICT components, which directly deal with energy for monitoring and control such as SCADA systems. The security of this system is of paramount importance since attacks may directly influence the security of supply.

Countermeasures depend upon several prerequisites such as, first of all, the architecture's requirements definition that must ensure the implementation of the main important and well known security mechanisms.

Communication between the components of an ICS is performed both via wired and wireless links. If these links are impaired, it may no longer be possible to acquire measured data and monitor the processes. This is termed a (distributed) denial of service attack, i.e. an attack that causes a failure regarding functionality or availability, possibly by multiple attacks:

- strict configuration of network access points;
- use of dedicated, cabled links for safety-related functions;
- if applicable, set-up of IDS/IPS to detect attacks and for alarming via alternative channels;
- redundant connection of components, using different protocols or communication routes;

Starting from the IT architecture, common security architecture must be based on the segmentation of the Control System Network:

- partition the system into distinct security zones;
- implement layers of protection to isolate the most critical parts of the system.

Particularly:

- each zone must be inside the next, leading from the least trusted to the most trusted and connections between the zones are only possible through secure interconnections;
- all resources in the same zone must have the same minimum level of trust;
- the inner layers, where communication interaction needs to flow freely between nodes, must have the highest level of trust;
- equipment in a zone must have security level capability. If the capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken;
- any communications between zones must be via a defined conduit (conduits control access to zones, resist Denial of Service (DoS) attacks or the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic).

Particularly, in the considered Use Case in depth defence implementation leads to *divide the considered system into security zones*, according to its functionality and criticality and to its physical location. This means to *identify security zones by grouping of logical or physical assets that share common security requirements*.

To establish a certain level of trust in a zone, it is required that all resources in the zone have a certain minimum level of security as determined by the organization's security policies. Then, in order to ensure a high security zone, the trust level must be very high. Measures to achieve this must be the following:

- Keep the trusted network zone relatively small and independent from other network zones. It should form its own domain, and be administered from the inside;
- Physically protect all equipment, i.e. ensure that physical access to computers, network equipment and cables, controllers, I/O systems, power supplies, etc., is limited to authorized persons;
- Harden the system by removing or disabling all unnecessary network connections, services, file shares, etc., and by ensuring that all remaining functions have appropriate security settings;
- When connecting a trusted network zone to outer networks, make sure that all connections are through properly configured secure interconnections only, such as a firewall or a system of firewalls, which is configured for "deny by default", i.e. blocks everything except traffic that is explicitly needed to fulfil operational requirements;
- Allow only authorized users to log on to the system, and enforce strong passwords that are changed regularly;
- Continuously maintain the definitions of authorized users, user groups, and access rights, to properly reflect the current authorities and responsibilities of all individuals at all times. Users should not have more privileges than they need to do their job;
- Do not use the system for e-mail, instant messaging, or Internet browsing. Use separate computers and networks for these functions if they are needed;
- Do not allow installation of any unauthorized software in the system;
- Use a virus scanner configured according to the automation system vendor's recommendations on all system nodes;
- Restrict temporary connection of portable computers, USB memory sticks and other removable data carriers. Computers that can be physically accessed by regular users should have ports for removable data carriers disabled;
- If portable computers need to be connected, e.g. for service or maintenance purposes, they should be carefully scanned for viruses immediately before connection;
- All CDs, DVDs, USB memory sticks and other removable data carriers, and files with software or software updates, should also be checked for viruses before being introduced to the trusted zone;
- Continuously monitor the system for intrusion attempts;
- Keep the system updated with all relevant and vendor recommended security updates, including updates to operating system, automation system software, applications, and security related software;
- Define and maintain plans for incident response, including how to recover from potential disasters;
- Regularly review the organization as well as technical systems and installations with respect to compliance with security policies, procedures, and practices.

The main countermeasures to be adopted can be summarized as follow:

- Deploying anti-(D)DoS devices and services;
- Traffic filtering;
- Utilising timely patch management;
- Deploying anti-virus software;
- Performing system hardening;
- System & network segregation;
- Use of "demilitarized zones" (DMZs);
- data warehousing in order to facilitate the secure transfer of data from the SCADA network to business networks;
- Commissioning penetration testing and vulnerability assessments to third parties could provide an objective analysis of the level of security of a SCADA network.

8.2 Costs of implementation

In order to have an estimation of the total cost for a large multinational company, like ENEL, related to the implementation of the countermeasures listed in the preceding section, we must divide the costs in two items: governance cost and hw/sw cost.

The Governance cost is related to the design, operation and maintenance of corporate policy and procedures for the logical security of all the Company Divisions and is a global value (all the business areas for all the countries).

The hw/sw cost is related to the design, acquisition, operation and maintenance of the technical devices to secure hosts and networks of each power plant and data network and is a value associated to each production unit.

Some of the costs, specifically the ones related to the design, acquisition and implementation of countermeasures, are investment costs (capex) to be borne only once, at the initial time; other costs, specifically those related to the operation and maintenance of the countermeasures, are operational costs (opex) to be borne annually.

Moreover, we have defined all the costs for two situations: the first one is *"cost starting from 0"*, that means without any kind of already existing mitigation countermeasures; the second one is *"Delta cost"* assuming that a set of "trivial" countermeasures is just implemented by the company.

Table 17 shows the costs related to the implementation of a detailed security program in the governance domain, in both cases *"cost starting from 0"* and "*cost starting from a security organization already present"*. In the last case we have only the operational costs in k€/year.

Table 17: Governance costs for a large multinational company

Field	Estimated Resources (€ or man working days)	Cost at T0 (k€)	Cost for the following years (k€/year)	Delta costs (k€/year)
	Cost of man-year = 100 k€	Costs starting from 0		Costs starting from a security organization already present
Security Program	Definition of a high level team within the company that implements yearly all the organisation aspects of the security program. 4 people at T0 and 1 for the following years	400	100	100
Organization of security	One technical skilled team in order to cover all the aspects of the internal organization. 6 persons at T0 and 1 for the following years	600	100	100
	One technical skilled team in order to control the external parties. 6 persons at T0 and 1 for the following years	600	100	100
Security policy, standards and procedures	Team of ICS-IT skilled people 3 persons at T0 and 2 for the following years	300	200	200
Risk Management	Consultancy contract with a security company (90 k€/year) + team of experts 4 persons half-time at T0 + 2 persons half time for the following years	290	190	190
Asset Management	Consultancy contract with a security company: 90 k€/y. Automated technical solution for asset management can be implemented: 500k€ (una-tantum) to cover a medium-large company, and 2 internal people for the management of the infrastructure involved full time.	790	290	290
TOTAL		2,980	980	980

Table 18 reports the cost analysis for the Hardware and Software components related to the Hosts and Networks security of a typical 380 MW production unit with 6 servers and 6 clients.

Also in this table are reported the values for both cases *"cost starting from 0"* and "*cost starting from a security organization already present"*. For the hw/sw costs we have capex and opex in both cases.

Table 18: Hw/sw costs for Hosts and Networks security of a typical 380 MWe power unit

	Cost Starting From 0		Delta Cost	
A) Network Requirements	**HW/SW cost (k€)**	**O&M annual cost (k€/y)**	**HW/SW cost (k€)**	**O&M annual cost (k€/y)**
Single 380 MW Production Unit	**370**	**20**	**280**	**10**

	Cost Starting From 0		Delta Cost	
B) Host Requirements	**HW/SW cost (k€)**	**O&M annual cost (k€/y)**	**HW/SW cost (k€)**	**O&M annual cost (k€/y)**
Single 380 MW Production Unit	**125**	**90**	**120**	**40**

TOTAL for a single 380 MWe Production Unit	**495**	**110**	**400**	**50**

In order to have global and comparable figures of costs to be sustained, by a national or multinational company or by all the Generation Companies in one specific country, we need to process the above said data fixing the perimeter of the intervention and some related assumptions.

First of all it is convenient to evaluate a single value of "Annualized Total Cost" including capex and opex. We assume that the initial investment in Governance could be amortized in 10 years and the initial investment in hw/sw could be amortized in 5 years. With these assumptions we have, neglecting inflation, the following basic values in million €.

Table 19: Annualized Total Costs (M€/year) for Governance and hw/sw for a 380 MWe Unit

	Annualized Total Cost in M€/year	
	Starting from 0	**Delta cost**
Governance Cost for a large multinational company	**1.30**	**1.00**
HW/SW cost for a single 380 MWe Production Unit	**0.21**	**0.13**

Now it is possible to have a rough estimation of the cost that ENEL could bear to secure their own power plants in Italy, assuming 26 main thermoelectric production units, 4 Remote Control Centres for hydroelectric production and 1 Remote Control Centre for geothermal production.

We can firstly assume that the Governance costs are charged entirely to the Italian production. Actually, the Italian generation capacity is less than one half of the global generation capacity of ENEL in the world; and so it is possible to have a second assumption with half of the Governance costs charged to the Italian production. The results of both these assumptions are reported in *Table*.

Table 20: Total Annualized Costs for ENEL in Italy (M€/year) in two hypotheses

	Starting from 0	**Delta cost**
Maximum value (all Governance costs)	**7,8**	**5,0**
Realistic value (Half Governance costs)	**7,1**	**4,5**

The first comment is that the Governance costs is not the most important contribute to the total cost (compare Table 19 and Table 20) varying from 9% to 20% also considering only the hw/sw of generation security. Actually, Governance is an activity for all the business areas of the company (electricity distribution, sale and so on); and so these values are higher than the real ones.

These values can now be compared with revenues and investments of ENEL to have an order of magnitude of the impact of security costs on the company business.

ENEL Total Revenues (2013) = 80,535 M€
ENEL Total Ebitda (2013) = 17,011 M€
ENEL Revenues from Italian Generation (2013) = 22,919 M€
Global Investment in 2013 = 5,000 M€
Investment in Italian Generation in 2013 = 318 M€

We see that the annual costs related to the security of Italian generation (i.e. major Italian generation plants) is negligible if compared with revenues and very smaller than the annual investment in Italian Generation Plants. In case of ENEL the values of table 8.4 to be considered are the "Delta cost"; about 1/70th of the annual investment.

If we want to compare the cost of security with the potential damage of blackouts, as evaluated in Chapter 5, we have to evaluate the cost related to an entire country, in this case Italy.

ENEL is the largest electric utility in Italy, the second one in Europe. Following the Italian market liberalization, there are a lot of big and small generation companies (GenCo's) in Italy. Some reference data about the capacity and production of power plants are the following (values rounded up and related to 2013):

- ENEL capacity in the world = 100.000 MWe
- ENEL capacity in Italy = 40.000 MWe
- Total Italian capacity (excluding wind and photovoltaic) = 100.000 MWe
- Available power at peak = 65.000 MWe
- ENEL gross production in the world = 300 TWh
- Total gross production in Italy = 300 TWh

These values sustain the point that the Governance costs of all the GenCo's related to the Italian generation activities are roughly the same of those evaluated for ENEL in the world, being capacity and production the same. These assumption is anyway conservative, because the Governance costs should be shared between all the business activities of the utilities (generation, distribution and sale).

More difficult is the estimation of costs for technical interventions (hw/sw) on power plants hosts and networks in Italy (or any other country) due to the difficulty to establish the power units and plants to be hardened. A fair assumption is to consider only the dispatchable units (i.e. thermo and hydroelectric plants) with power over a specific threshold. In this way are excluded non dispatchable renewable plants (i.e. wind and photovoltaic) and minor power plants not able to cause, with a sudden shutdown, relevant problems on the transmission grid. In Italy there are 130 units with power greater than 200 MWe; some of them are obsolete and with very low or zero hours of production (in particular oil fired units). ENEL owns 14 large combined cycle units (350-380 MWe) and 12 large coal fired units (320 and 660 MWe) in addition to 4 Remote Control Centres for hydroelectric production and 1 Remote Control Centre for geothermal production; in total 31 major sites to be hardened. Considering the ENEL units with significant power but less than 320 MWe, the Italian units owned by other operators and the units out of service, a reasonable estimation of the number of units to be considered is restricted from the range 31-130 to the range 50-100.

In this way we are able to estimate a range of global cost related to the implementation of the countermeasures listed in section 8.1 in the Italian generation system: see Table 21.

Table 21: Annualized Total Costs (M€/year) for the security of generation in Italy

	Annualized Total Cost in M€/year	
	Starting from 0	**Delta cost**
Annualized Total Cost for generation in Italy	**11,8 – 22,2**	**7,5 – 14,0**

It is reasonable to assume a reference total cost in the range 10 – 20 M€/year. These values can be compared with the cost of a single blackout as evaluated in Chapter 5.