APPENDIX 2:
SUMMARY OF THE MAIN RESULTS OF **THE ESSENCE PROJECT**

Appendix to **Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators**

Project Title:	Europe and Eurasia Cybersecurity Partnership
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Cooperative Agreement #:	AID – OAA-A-16-00049
Recipient:	National Association of Regulatory Utility Commissioners (NARUC)
Date of Publication:	May 2020

Author: CNR-IRCrES, The National Research Council of Italy, Research Institute on Sustainable Economic Growth[1]

[1] The present document has been prepared by Elena Ragazzi (project leader), Ugo Finardi, and Alberto Stefanini.

1 The ESSENCE experience: who, what, where, and why

ESSENCE – *Emerging Security Standards to the EU power network controls and other Critical Equipment* has been a research project funded by the European Union under the CIPS EU program aiming at evaluating costs and benefits of applying emerging security standards to the European power grid controls systems, based on two case studies.

When ESSENCE began, much work on the definition and the technical assessment of standards against malicious attacks had already been done (Masera & Stefanini, 2008), (Finardi, Ragazzi, & Stefanini, 2013). Nevertheless, in Europe, no clear position had emerged while some standards failed to be completed for years. Many operators adopted different types of protections – above all the Transmission System Operators (TSOs) - but without converging on a common fixed framework. Substantially, the lack of concrete experience on what generalized standard compliance would imply was an obstacle against regulation. This intuition was the reason that pushed the promoter CNR-CERIS (former denomination of CNR-IRCrES, Italy) to launch the ESSENCE project. Apart from the coordinator, partners of the project were 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 systems division (Italy), IEN - Institute of power engineering (Poland), and PSE – Operator SA (Poland).

Throughout 2012-2014, the ESSENCE project performed a study in order to evaluate these costs and benefits on a rational base, including:

- the development of a common understanding of industrial needs and requirements regarding the security of control systems and the related standardization efforts;
- identification of the main power system vulnerabilities induced by control systems and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
- evaluation of the main emergent frameworks for ensuring industrial control systems security, so as to establish the costs of their adoption on an objective basis.

The project conclusions were largely based on the outcome of two case studies, concerning a broad portion of the Italian power generation capability and the Polish transmission system. Both confirmed that cyberattacks able to properly exploit current vulnerabilities of the two systems could turn into large and extended blackouts. Relevant results were also obtained regarding the issue of the cost of countermeasures. In fact, based on current and prospected security standards, the project identified the key organizational and technical countermeasures needed to increase the security level of the involved infrastructures so as to neutralize possible attacks.

Based on their outcome, costs and benefits for their adoption were extrapolated to the whole of the respective countries. The project followed a mix of compliance based approach and of risk assessment approach. To counter the cyber threat, which is common to all critical infrastructures, several standard frameworks were being proposed at that time (see Table 1). Before ESSENCE, it was difficult to evaluate the costs and the benefits of their adoption, although early experimentation showed they were considerable. Thus, there was a need for establishing the economic and organizational impact of their implementation in Europe.

Table 1- Key reference standards for ESSENCE

Standard	Reference sector	Involved stakeholders	Compliance
ISO 27000	IT in general IT networks	End users and product manufacturers	May be required in specific market segments
NIST 800-53	Security and privacy controls for federal information systems and organizations	U.S. federal agencies Service/product providers to the above	Compulsory and binding for U.S. federal agencies
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security	U.S. federal agencies Service/product providers to the above	Special publication, dealing with online ICS control security. It is a guide, without binding status.
IEC 62351	Developed by WG15 of IEC TC57.[2] Aimed at handling the security of TC 57 series of protocol, including IEC 60870-5 series, IEC 60870-6 series, IEC 61850 series, IEC 61970 series & IEC 61968 series.	Power system device manufacturers and end-users	Wherever applied, it brings power systems SCADA peripherals compliant w.r.t authentication of data transfer, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection
ISA/IEC-62443	Industrial communication networks - network and system security	End users/product or service providers	Completed in 2018
NERC CIP 001-010	North American power system	NERC affiliates (electrical utilities and grid operators)	Mandatory for NERC affiliates

[2] The IEC Technical Committee 57 is one of the technical committees of the International Electrotechnical Commission (IEC). TC 57 is responsible for development of standards for information exchange for power systems and other related systems including Energy Management Systems, SCADA, distribution automation, and teleprotection.

2 Description of the Italian case study

The Italian case study (Angeletti, et al. 2014) dealt with the electric power system of an area of Italy connected to the rest of the grid via one single power line. In the region, six main plants operate. Moreover, there were several minor photovoltaic and wind distributed generation facilities with a total gross power of 2500 MWe. The full scenario of the case included several concurrent events:

- the high voltage line connecting the area was supposed to be under maintenance;
- by consequence, the area is isolated from the HV power grid but keeps on self-supplying;
- a cyber attack is performed on the power generation plant with the highest capacity, plant C, causing the plant shut-down;
- the outage of other plants occurs because of the rough frequency transient on the grid,[3] thus causing a blackout on the whole 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

It is more difficult is to estimate the costs for technical interventions (HW/SW) on power plant hosts and networks in generation, due to the difficulty to establish which power units and plants are to be hardened. A fair assumption is to consider only the dispatchable units, i.e. the thermal and hydroelectric plants with power, over a specific threshold. This way, all non-dispatchable renewable plants (i.e. wind and photovoltaic) were excluded, as well as the minor power plants because they are not able to cause relevant problems on the transmission grid with a sudden shutdown.[4]

In this case study, the adoption of countermeasures depends upon several prerequisites such asthe architecture's requirements definition that must ensure the implementation of the main important and well-known security mechanisms.

First of all, 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

[3] i.e., a considerable reduction of the frequency with subsequent detachment from the grid of Plant B. The simultaneous unavailability of two large generating plants on the Sicilian power grid isolated from the continent implies a total blackout on the entire area.

[4] In Italy (2013), there were 130 units with power greater than 200 MWe; some of them were obsolete and with very low or zero hours of production (in particular oil fired units). ENEL owned 14 large combined cycle units (350-380 MWe) and 12 large coal fired units (320 and 660 MWe) in addition to four remote control centers for hydroelectric production and one remote control center 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. Of course, some of these assumptions (namely the exclusion of renewable plants) may no longer hold in 2019, because their impact on whole power generation was dramatically altered in the period 2013-2019.

(Angeletti, et al. 2014, 57). The main countermeasures to be adopted may be summarized as follows (Angeletti, et al. 2014, 59-63):

- deploying anti-(D)DoS devices and services;
- traffic filtering;
- using timely patch management;
- deploying anti-virus software;
- performing system hardening;
- system and 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.

In this way, the project was able to estimate a range of global costs related to the implementation of the listed countermeasures in the Italian generation system (see table 3).

Table 3: 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

The case study also makes a distinction between governance costs and HW/SW costs:

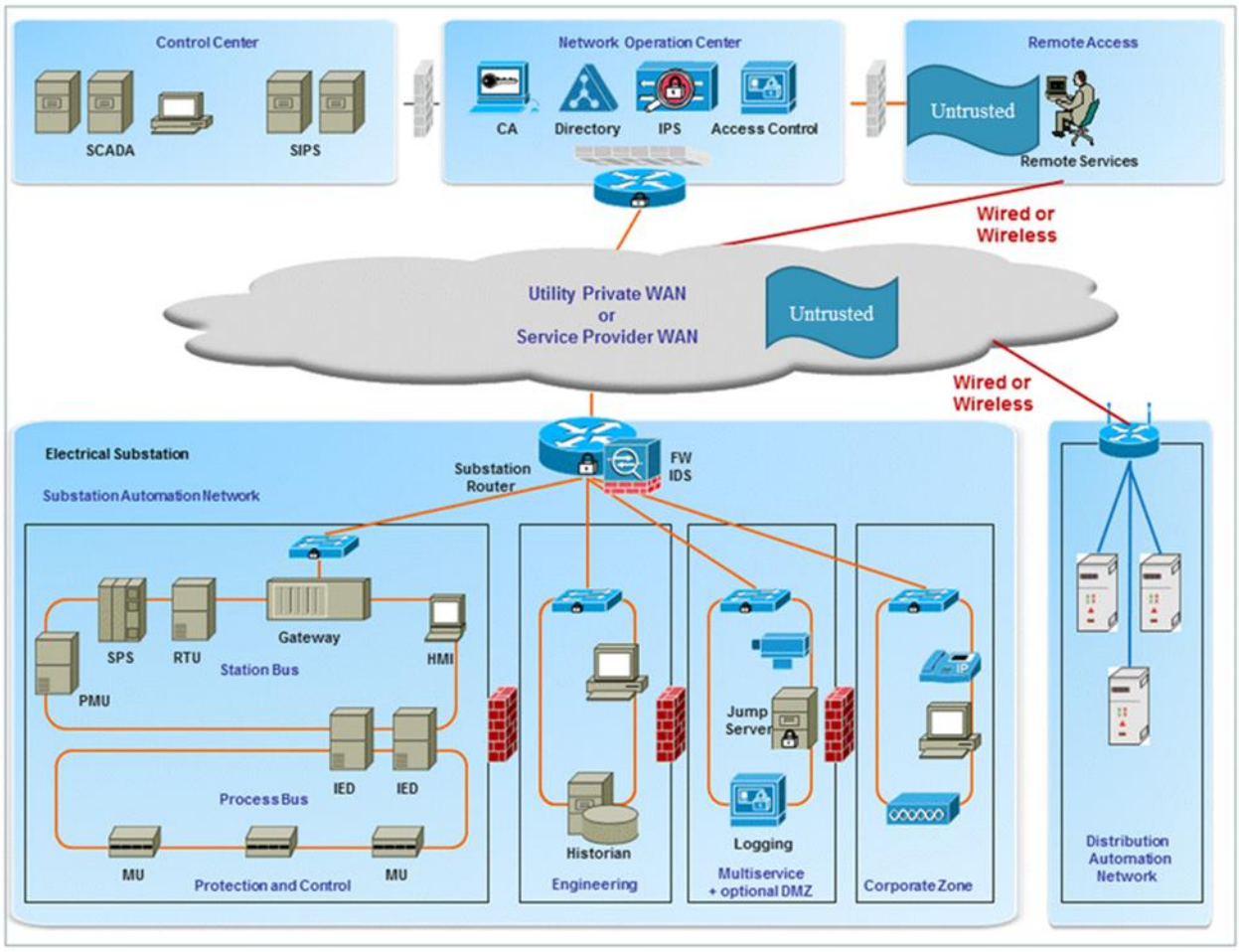
- **Governance costs** are related to the design, operation, and maintenance of corporate policy and procedures for the logical security of all the company divisions and are seen as a global value for the operating company (i.e. it impacts all the business areas for all the countries). More analytically, they are classified as such:
    - **Security program**: this area includes all security requirements concerning SCADA and industrial control system security vision, objectives, goals, strategies, directions, and security plans.
    - **Organization of security**: this area includes all security requirements concerning internal and external (third parties) roles, responsibilities, and 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 the 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.

- **HW/SW costs** are 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 are a value associated with each production unit.[5] They are classified as such (p. 39):
    - **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 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 cybersecurity into systems from the earliest development stages. It also involves the maintenance of those cybersecurity policies and procedures as the system changes throughout its lifecycle.
    - **Human resources security:** in turn classified as prior to employment, training, and awareness, and after employment or upon reassignment.
    - **Physical and environmental security:** the standard provides a comprehensive outline of security controls that 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 minor or major disruption.
    - **Incident management:** the standard provides regulations on how to detect and react to security incidents, as well as a 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.

Network security requirements concern security aspects of communication management on the ICS environment (e.g,. network secure architecture, perimeter security, secure communication protocols) and operation management on the ICS environment (e.g,. configuration and change management, backup and recovery, monitoring). Network security addresses the concept of network segregation and layered protection in relation to the principles of defense-in-depth. Sensitive security perimeters must be clearly identified and protected with measures being more restrictive as one moves going from the outer layer to the inner layer.

[5] The report actually dwindles in terminology, calling them **hardening costs** at p. 38.

Figure 1: a high-level architecture showing zones from a remote access point of view (CIGRE TB 762)



Source: IEC 61850

Network architectures. One fundamental group of countermeasures concerns network architectures. The defense-in-depth architecture strategy must include the use of firewalls, the creation of demilitarized zones (DMZ), and intrusion detection capabilities along with effective security policies, training programs, and incident response mechanisms. An architecture is made by:

- a **control zone,** for low-risk ICS, containing a process control network segment, a proprietary regulatory control network segment, and a proprietary field device network segment. Common filtering strategies are provided.
- a **demilitarized zone,**[6] for high-risk ICS, in order to eliminate or greatly reduce all direct communication between the control zone and the business zone. The security level for the DMZ is higher than the business zone, but less than the control zone. Some of the main benefits of DMZ zones are as follows:
    - minimize the number of people directly accessing control zone devices;
    - provide greater security for important IACS devices;

- compensate for patching delays;
- provide improved security for the control zone by moving management devices to a higher security level.

- a **safety system zone:** some ICS may employ a set of safety interlocks that are relay-based or microprocessor-based. A microprocessor-based logic solver SIS may require a slightly different set of security practices from that employed in the control zone. The target security level for this zone should be determined and appropriate actions should be taken to ensure appropriate countermeasures;
- some **isolated ICS:** the risk associated with those ICS may be too great to allow any opportunity for compromise by an external agent. A facility may choose to disconnect all conduits between the control zone and any other zone. This is a very valid network segmentation strategy for consideration.

When designing the network architecture for an ICS deployment, it is recommended to separate the ICS network from the corporate network because the nature of network traffic on these two networks is different. Internet access, FTP, e-mail, and remote access will typically be permitted on the corporate network but should not be allowed on the ICS network. If ICS network traffic is carried on the corporate network, it could be intercepted or be subjected to a Denial of Service (DoS) attack. If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a DMZ.

The most secure, manageable, and scalable control network and corporate network segregation architectures are typically based on a system with at least three zones, incorporating one or more DMZs. Networks should be segmented through the use of some sort of barrier device that has the ability to control what passes through the device. On Ethernet-based networks running TCP/IP, the most common barrier devices in use are firewalls, routers, and layer three switches. While a security zone may be created by placing a barrier device into the network, thereby creating a new network segment, a security zone may encompass multiple network segments. It is important not to confuse the functional levels of the reference model with security levels associated with security zones.

Coming to the costs of countermeasures, some expenses, 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.

Table 4 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 (k€/year).

Table 4: 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 organizational aspects of the security program. Four people at T0 and one 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. Six people at T0 and one for the following years	600	100	100
	One technical skilled team in order to control the external parties. Six people at T0 and one for the following years	600	100	100
Security policy, standards, and procedures	Team of ICS-IT skilled people Three people at T0 and two for the following years	300	200	200
Risk Management	Consultancy contract with a security company (90 k€/year) + team of experts. Four people half-time at T0 + two people 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€ (lump sum) to cover a medium-large company, and two internal people for the management of the infrastructure involved full time.	790	290	290
TOTAL		**2,980**	**980**	**980**

The table below 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 six servers and six clients.[7]

[7] Also in this table are the reported 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 5.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 five years. With these assumptions, neglecting inflation, the following basic values in million € were found.

Table 6: 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

It is important to note here that ENEL is the largest electric utility in Italy, and the second largest in Europe. Some reference data about the capacity and production of power plants include 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 as those evaluated for ENEL in the world, with capacity and production being the same. These assumptions are conservative, because the governance costs should be shared between all the business activities of the utilities (generation, distribution, and sale).

Now it is possible to have a rough estimation of the cost that ENEL could bear to secure their own power plants in Italy.[8] The Italian generation capacity is less than one half of the global generation capacity of ENEL in the world, so it is reasonable to charge to the Italian production just half of the governance costs.

Table 7: 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

In summary:

- Governance costs are not the most important contribution to the total cost (compare **Error! Reference source not found.** and **Error! Reference source not found.**), varying from 9% to 20% also considering only the HW/SW of generation security.
- Compared with annual revenues and investments of ENEL to have an order of magnitude of the impact of security costs on the company business, 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 small in comparison to the annual investment in Italian generation plants.[9] In the case of ENEL (the values of table 8.4 to be considered are the "Delta cost"), security costs are about 1/70 of the annual investment.
- If we want to compare the cost of security with the potential damage of blackouts, we have to evaluate these costs in relation to an entire country, which is Italy in this case.

In conclusion, it is reasonable to assume a reference total cost in the range of 10 – 20 M€/year.

[8] The case referred to: 26 main thermoelectric production units, four remote control centers for hydroelectric production, and one remote control center for geothermal production. Governance costs are charged entirely to the Italian production.

[9] 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€

3 The Polish case study

In the case of the Polish case study, the choice of the appropriate countermeasures was preceded by the analysis of the operation of the transmission system, which is properly built and designed for dealing with component failures. The transmission system is designed to maintain continuity of supply according to the N-1 criterion.[10] As a result, only the coincidence of several failures is able to significantly disturb its operation as a whole (Bartosewicz-Burczy, Bruno, Garcia, & Wlodarczyk, 2014, p. 65-69).[11] Key importance should be attributed to countermeasures that may limit the spread of cyber incidents and minimize its impact on the duration of disruption. The study focused on power disturbances affecting the capital city of Warsaw. Namely, two conditions were considered where failure of a single substation component may cause serious disturbance:

- situations where the overlap between work planned at many power plants results in their exclusion, thus the whole system is kept operational by a set of power plants with very little available power.[12] In these conditions, the failure at a single station directly connected with the power plant results in a loss of supplied power which cannot be quickly compensated by the rest of the system, because the existing transmission lines are not able to transmit enough power to all the remaining substations. Thus, system unity is jeopardized and falls into a set of asynchronous islands where continuity of supply is granted and areas are wholly excluded from power.
- A second case concerned the sudden shutdown of an international exchange station on the Polish-German border, when a large amount of energy was in transit from north to south Germany. In addition to its impact on the Polish system, this situation may threaten stability of the German transmission system and impact on the entire system connected to the ENTSO-E.

Countermeasures were selected in order to:

- delaying attack propagation through organizational measures (diversification of service providers), exploiting the heterogeneous structure of the substation devices, and upgrading ICT systems (by removing vulnerabilities, hardening, separation, introducing firewalls);
- maximizing the probability of attack detection during the reconnaissance phase, implemented through construction of intersystem communication nodes and inter-control points, implementation of honey pot traps, and construction of systems for automatic analysis and correlation of events;
- minimizing the duration of every single failure.

The above reported facts result in a security strategy that reduces the number of potentially harmful cyber attackers to a very limited group of experts, whose knowledge, budget, and time may allow them to break any security in a manner undetected by the monitoring systems.[13] The ICT systems for power facilities

[10] i.e., the rule according to which the elements remaining in operation within a Transmission System Operator's control area after occurrence of a contingency are capable of accommodating the new operational situation without violating operational security limits.

[11] Independent from their cause, whether due to a physical cause, such as flood or earthquake, to an operational mishap or to the malfunction of equipment, either inherent or induced by a cyber attack.

[12] These contingencies may happen, for instance in the summer 2013 the Polish national power supply fell below the required minimum.

[13] In practice, the high probability of being detected during an attack should effectively discourage the vast majority of potential attackers to implement cyber-attacks, when other methods such as physical attack would be more effective.

significantly differ from those employed in IT companies. Differences are not due to use of special technology, but to their implementation methods. The use of particular technology for time periods much longer than originally anticipated[14] is the difference that has the greatest impact on security. In those conditions, however, even the most safety conscious providers of equipment and IT systems are not able to anticipate inherent vulnerabilities in their products over such a long time span.

On the other hand, although vulnerability reduction in principle implies rather common countermeasures, equipment replacement is very expensive because:

- automation belongs to one of the most expensive endowments of power stations. Its refurbishment requires high workload of specialized personnel, and a long time is required to dismantle old equipment, install and program the new one, and then test it prior to entry into service;
- installed countermeasures cannot introduce delays in transmission of signals. Therefore, when developing proposals for the recommended standards, it is necessary to take into account not only their costs but also an estimation of the difficulties of their implementation, in view of the need to maintain the required operational quality parameters. The higher their complexity, the less likely the success of their implementation.

Construction or modernization of existing power facilities is even more expensive, as it may involve a full redesign of their logical architecture and new ways to support their safety monitoring (e.g. by embedding dedicated IT security solutions or new measures to protect the physical building). Another reason for complications associated with the implementation of IT security for substations is the demanding needs in terms of certainty of device time response parameters and reliability of communications, resulting in improved continuity of service.[15] Moreover, different from business systems, power system facilities can never break their operation, because this would result in interruptions in providing or receiving energy. Table 8 resumes the features of an energy control system ITC system compared to office IT.

Total implementation costs were calculated for each security countermeasure separately, without taking into account relationships with other countermeasures. Also, in the Polish case study, the costs were calculated in terms of what should be borne if no security standards had been implemented yet (costs starting from 0), and costs that should be borne starting from the current situation in order to manage higher supplementary security (Delta costs). In Poland,the total cost for implementing (initial investment) and maintaining (annual management) the security standards encompasses the listed countermeasures in the case of "Cost starting from 0." That is € 26,016,000 for implementing and 5,016,280 for maintaining. The total cost of implementation of additional countermeasures not yet existing in transmission system is €7,486,000 and the additional annual cost for maintaining the implemented countermeasures is € 2,457,200.

The most recommended way to increase the level of security is the comprehensive implementation of countermeasures in all listed groups.

Table 8. ITC for power system

	Energy Control Systems	**Office IT**
Anti-virus/mobile code	Uncommon/hard to deploy	Common/widely used
Component lifetime	10-30 years	Three to five years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular/scheduled

[14] For example, the operating system Microsoft Windows XP, commonly used for construction of IEDs and other automation devices, must work even for a dozen consecutive years.

[15] Moreover, any significant architectural change should be thoroughly tested, and due to the current lack of appropriate testing facilities, this results in very long deployment times.

Real-time requirement	Critical due to safety	Delays accepted
Security testing/audit	Rarely (operational networks)	Scheduled and mandated
Physical security	Very much varying	High
Security awareness	Increasing	High
Confidentiality (Data)	Low-medium	High
Integrity (Data)	High	Medium
Availability/Reliability	24 x 365 x …	Medium, delays accepted
Non-repudiation	High	Medium

Sources: IEC/TR 62351-10

Table 9. Total cost of the implementation all countermeasures by a TSO (€)

Group of countermeasures	**Substations**		**Information control systems**		**Office systems**	
	Implementing	Maintaining	Implementing	Maintaining	Implementing	Maintaining
Antivirus protection	16,000	40,000	2,000	150	30,000	4,000
Backup infrastructure	200,000	100,000	200,000	20,000	600,000	35,000
Data loss prevention	270,000	350,000	4,000	2,690	11,900	36,000
SCADA protocols validation	3,000,000	300,000	50,000	5000		
Firewalls and IPS Protection	1,500,000	350,000	20,000	12,000	90,000	28,000
Integrity of communication	135,000	40,000	50,000	1,200	100,000	5,000
Physical access control	1,600,000	800,000	4,000	2,000	28,000	7,000
Change of existing system configuration	45,000	60,000	67,200	80,000	183,000	160,000
LAN segmentation	820,000	20,000	8,000	10,000	13,000	10,000
Maintenance work	0	280,000	3,000	80,000	133,900	200,000
Procedures	12,000	3,000	15,000	5,000	60,000	5,000
Redundancy	0	0	3,000,000	300,000	5,400,000	1,100,000
Remote and external access-centralized system	0	20,000	20,000	7,000	55,000	18,000
Communication confidentiality (substation and centralized system)	100,000	40,000	20,000	7,000	55,000	18,000
Security events monitoring, managing and reporting	100,000	30,000	120,000	28,000	280,000	20,000
Physical, environment	7,080,000	300,000	40,000	7,000	201,000	9,240
Vulnerability management	240,000	50,000	10,000	1,000	24,000	10,000
TOTAL	**15,118,000**	**2,783,000**	**3,633,200**	**568,040**	**7,264,800**	**1,665,240**

4 A Summary of the ESSENCE main results

ESSENCE conclusions (Ragazzi and Stefanini 2019) were largely based on the outcome of the two above described[16] case studies. Both cases identified some situations in which Industrial Control Systems (ICS) bear important vulnerabilities.[17] In the case-studies' scenarios, attackers exploited these vulnerabilities and led to the sudden shutdown of some power generation plants or of some substations of the transmission grid, which in turn caused a region-wide blackout lasting six hours and involving millions of users:

- In the Polish case study, hypothetical serious disturbance on three substations resulted in the cascading loss of power supply in the entire city of Warsaw.
- In the Italian case study, the cyber-attack was carried out through well forged malware diffusion within the process control network act to damage the OS, or through DDoS, and targeted a power generation plant (400 MW) during the maintenance period of the cable connecting the area to the rest of the national grid during the day hours of peak request.

In both cases, the costs were computed with reference to two situations: the first one was "cost starting from 0," which means without any kind of already existing mitigation countermeasures; the second one was "Delta cost" assuming that a set of "trivial" countermeasures is just implemented by the company.

The ESSENCE analysis estimated the cost that a country should deal with in the adoption of security standards in the transmission and generation of electricity.

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

The costs for a large multinational company or a national TSO is much higher than the direct cost the company or the TSO bears in the event of a blackout, but much less than the damage to production and residential end-users. In both cases, two situations were considered: costs that should be borne if no security

---

[16] Although the two case-studies differed for many features, such as the type of activity, the relevant attack scenarios, and even the countermeasures to be implemented, they bore some common characteristics and were approached with a methodology which included the following common activities:

- Identification of the most likely attack scenarios able to seriously hamper the infrastructure operation;
- Detailed listing of the countermeasures able to block the attacks or to mitigate their consequences and comparison between the different standards;
- Detailed study of the consequences of a successful attack (duration of black-out and recovery path, extension of the region involved, type and profile of consumers not supplied in the various phases of the recovery, and amount of electricity not sold);

The cost assessment was based on two comparisons:

- Regulated scenario (compulsory standard implementation) versus non-regulated scenario (actual countermeasures implemented on a voluntary basis)
- Regulated scenario versus no protection at all (unrealistic situation useful only as benchmark).

[17] These power system weaknesses were clearly confirmed by some past blackouts due to natural phenomena and technical failures (e.g. Italy 2003, USA and Canada 2003, Germany and other Europe countries 2006, India 2012). More recently, their vulnerability was confirmed by the repeated cyber-attacks over 2015-2016 on the Ukrainian power system (Cherepanov & Lipovski, 2017), (Symantec Security, 2016). The hugest was on Dec. 23, 2015, when three regional Ukrainian electricity distribution companies – Kyivoblenergo, Prykarpattyaoblenergo and Chernivtsioblenergo – suffered power outages due to a cyber-attack (Fire Eye, 2016). These events may cause very high direct and indirect damage, both to the productive sector (agriculture, industry, services) and to residential users.

standards had been implemented yet (cost starting from 0) and costs that should be borne starting from the current situation in order to manage higher supplementary security (Delta cost).

Another assessment was performed about the involved economic impact. This is relevant in that most human activities (not only in the productive sector but also in households and leisure) depend on electric power supply. Moreover, in most developed countries service reliability has reached very high levels, so that an outage is often considered an exceptional event. For this reason, when it happens (especially if it is unexpected), it creates huge inconveniences.

Although consumers would surely agree that electricity supply security has a relevant value, how high this value is (in monetary terms) makes for a very difficult issue due to specific reasons related to economic methodology. Since direct measurements of the value of service reliability are in general considered as very difficult tasks, a reasonable and broadly accepted approach to evaluate supply security is estimating the damage that would occur in case of failure.

Failures may assume different forms, such as blackouts (loss of power lasting a period of time), brownouts (non-complete drop in voltage), transient faults (loss of power lasting few seconds), etc. ESSENCE focused on the consequence of blackouts in selected areas, since this is the kind of failure considered in the Italian and Polish case studies. Blackouts may generate several different kinds of damage; we made a distinction between economic and non-economic (social) costs. Some damage categories present an evident causal relationship with the interruption, while in other cases this link is weaker.

Among the immediate effects of the cessation of supply, the main drawback for the productive sectors is production losses. However, depending on the production process characteristics, other damage categories are relevant. This is the case of idle or spoiled production factors (labor, materials, capital), damaged equipment, and re-starting costs. For households, food spoilage is one annoying inconvenience. All these sources of damage can be classified as economic since they generate either a monetary ("out-of-pocket") loss, a profit reduction, or both.

Other sources of inconvenience play important roles, though they do not generate monetary losses. These can be classified as social costs of interruptions and involve the loss of leisure time, the inconvenience due to the lack of services, uncomfortable temperature in buildings, mental stress, etc. It is clear that these costs apply to individuals, while firms mainly face purely "economic" damages. Finally, other costs arise as mediate consequences of the interruptions, such as the increase in criminal activity, and their evaluation is even more complex. Developing a methodology including all the possible sources of damage is not practically feasible. Thus, ESSENCE decided to focus on some cost categories only, namely the whole damage suffered by a household during a blackout and the damage in terms of lost production only for companies.

ESSENCE was able to estimate costs in this way: for the Italian case, a total damage for non-households was found to range from 35 to 46 million €, while for the residential segment the blackout cost was between 36 and 64 € million, with a believable value set around 52 € million considering the characteristics of the average consumer in that area. The damage to the electricity sector due to non-sold energy is about two million €. In relation to the Polish trial, a damage for non-households was found to be between 25-35 million €, while for households the range was between 30 and 61 € million. If we consider the characteristics of the average residential consumer, we get a total cost of about 52 million €. For electric operators, the damage is about 0.7 million €. In conclusion, the estimated damage for households is in both cases far higher than for non-households. The damage to the electricity sector (not taking into account the damage to reputation) is a very small fraction of the total estimated damage.

In other words, the ESSENCE project identified the key organizational and technical countermeasures needed to increase the security level of the involved infrastructures so as to neutralize or mitigate possible attacks.

The obtained results quantify the cash flows for the implementation (investment costs) and maintenance (annual operational costs) of the security standards, according to the above described "no protection" and "Delta cost" cases.

In the Italian case study, based on a generation company, a further passage has been necessary: the costs needed to implement the chosen countermeasures in the firm have been used to estimate the costs that it would be necessary to afford to protect the whole country. This explains why the estimate on the cost of implementation for the Italian case is expressed in terms of a range. In fact, it starts from the number of plants exceeding a given size, which is known, but then the protection requirements depend also on the use conditions; not all plants are run in conditions of continuity, and then for some of them protection could not be judged a priority.

In the Polish case study, concerning the national TSO, the whole country protection is included in the simulation. Starting from the simulation, some considerations on scalability have been made, so that it would be possible to quickly assess the cost concerning TSOs of different scales. This kind of analysis is impossible in the case of the generation system, because the cost depends on the features of the system (age, fuel type, scale, share of renewables, geographical diffusion) which differ a lot by country.

The simulation showed that in both case studies, an attack borne in conditions of vulnerability can lead to extended and durable blackouts in selected areas. Since security standards will hamper the huge inconveniences of a blackout, their benefits have been estimated as the economic and social damages that could be avoided implementing the correct countermeasures.

The estimates include the impact on electricity firms, on other firms, and on households. As far as the productive sector, just losses in production (avoided income) are included in the figure, while direct damages to processes are not included (although some qualitative evidence is available) since the values differ very much following the process and the type of firm. As for households, direct cost (for example food spoilage) and social cost is included, but not indirect effects (e.g. increased criminality, failures in providing other essential services). For this reason, the estimate is a lower bound, prudent estimate. Benefits are always expressed as a range, from the more strict to the loosest assumptions that have been adopted. In the case of household, the "expected" value refers to every country's "typical family."

The results arising from the two case studies and by the cost analysis and the benefit analysis run on them are summarized in Table 10.

Referring to the benefit analysis, it can be seen that the largest effects of the black-out are borne by families, followed by non-electricity firms. One could expect a greater difference between the two values. In effect, at present small private users are the first to be re-supplied after a blackout because they are supposed to suffer the most from the lack of electricity. However, even if a lot of attention has been given during the survey to get the consumer involved in the problem of security of supply, nowadays reliability is often taken for granted and so the estimated value of the blackout is still under-evaluated. This perception would probably change a lot after a large blackout is experienced.

Table 10: Summary of cost and benefit estimates in the two case studies (€ MILLION)

ITALIAN CASE STUDY				
BENEFIT		*COST*	*Delta*	*No protection*
Electricity not sold	2	Investment	20-40	28-53
Non-households	35-46	Mantaining	3.5-6	6.5-12.9
Household*	36-52.5-64			
TOTAL	73-112			
POLISH CASE STUDY				
BENEFIT		*COST*	*Delta*	*No protection*
Electricity operators	0.7	Investment	7.5	26
Non-households	25-35	Mantaining	2.5	5
Household*	30-52-61			
TOTAL	55.7-96.7			

*Min-Expected-Max

Electricity utilities suffer from blackouts too, in terms of decreased sales, but the value of their damage is only a small fraction of the total. Actually, in many countries, utilities will pay a fee in case of interruptions in supply. However, they have not been considered, because these compensations (above all when they are bargained) are another way to estimate the effect of a blackout, and so including them in the calculations would have meant to count some effects twice.

Considering the implementation costs, it can be seen that they are relevant both in transmission and in generation, but a relevant share of countermeasures has already been implemented by the two utilities participating in the project. The implementation of countermeasures will not only imply huge investments but also increased maintenance costs.

Comparing benefits to costs, it can be seen that even considering the most restrictive estimates of benefits and the highest estimates of costs, one single event would be enough to completely recover the total cost of implementing security standards both in generation and in transmission. Although it is impossible to precisely estimate the probability of such an event (see the paragraph below), it is widely acknowledged that this probability would strongly increase after the first time in which countermeasures are unable to block or mitigate an attack and their consequences are echoed by the media. This would, in fact, prove the feasibility of the attack and, above all, the visibility, which is most important for cyber-terrorists and can unchain an imitation effect leading to an escalation of attacks.

In summary, the ESSENCE analysis shows that from a mere economic viewpoint, electric companies should not increase their security levels, as the annual costs of those countermeasures are much greater than their direct cost of a single blackout. However, the total cost of an event for the society as a whole is by far greater than the annual cost of the said countermeasures. Therefore, it is of interest for the community to take actions to raise security levels and ultimately reduce global risk.

5 Issues on the classification of countermeasures: comparison among ESSENCE taxonomies and reasoned lists

The concept of cybersecurity was first introduced by the BS7799, a standard originally published by BSI Group (British Standards Institution) in 1995. BS7799 was prepared by the UK Department of Trade and Industry and consisted of several parts. The first one, dealing with the best practices for Information Security Management, was adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management" in 2000, and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007. The second part was first published in 1999 with the title "Information Security Management Systems - Specification with guidance for use," and focused on on the implementation of an information security management system. Furthermore, the 2002 version introduced the Plan-Do-Check-Act approach, aligning it with the ISO 9000 quality standards, and was adopted by ISO as ISO/IEC 27001 in November 2005.

Later standards introduced to cope with cybersecurity in critical infrastructures and control and communication systems, such as the NERC CIP, IEC 62443, the NIST Cybersecurity framework, etc. keep basically consistent with the definitions laid down by the BS 7799: any one of those standards tends to define cybersecurity in its own operational terms, i.e. as a set of guidelines that - once applied - guarantee a certain level of protection to the considered target system.[18]

An important reflection deriving from the ESSENCE experience has been the understanding that no unambiguous cost categorization exists, and no universal recognition of a single cost category assessment exists. In fact, the organization of costs, and the cost categories deriving from this organization, substantially depend on the type of operator (TSO, DSO, power generation) as well as on the security standards that are taken as reference. This fact is reflected also in the results of ESSENCE. As the table below shows, different categorizations of costs have been exploited, in turn deriving from the elaboration and the application to the specific case of different security standards. The cost categorizations presented in the table can also serve as a useful instrument in order to help disentangle the problem of how costs voices should be organized when protecting a system. The interdependency among measures motivates why it is quite difficult to adopt the same classification scheme for any ICS control, as it is apparent from the following table, which reports the summary of the requirements classification performed by the introductory report on the terms of reference for the case studies, as well as by the two case studies.

The case studies kept a different baseline of implemented measures, hence a different classification scheme, notwithstanding the attempt made on the terms of reference report to convene a unifying scheme. The former report was based on ISO 27000, IEC 62351 and NIST 800-53, while the Polish case also took due notice of the NERC standards, and the Italian one was based mainly on the IEC 62443 classification. Moreover, the target plants have different configurations, because a SCADA for a substation controls about 300 input/output lines, while a large power plant control is layered (as seen in the two sub-sections above) and requires overall control over several thousand lines.

The table below presents a summary comparison of the three classifications. The final table instead contains the list of countermeasures – organized according to the items reported in table XX – presented in the terms of reference ESSENCE report, and the citation of the standard that contains them.

18 NARUC has taken a similar approach, by introducing its Primer, now in its Version 3.0. Keogh M., Thomas S. (2017) *Cybersecurity. A Primer for State Utility Regulators. Version 3.0*. National Association of Regulatory Utility Commissioners.

Table 11 - Three classification schemes adopted by ESSENCE

Classification of requirements **Terms of reference for the trials**	**Cost categories** **Polish case study**	**Hardening cost categories** **Italian case study**

• Security policy and procedures (requirement 1)
• Organizational security (reqs. 2-7)
• Personnel security (reqs. 8-14)
• Physical and environmental security (reqs. 20-37)
• System and services acquisition (reqs. 40-51)
• Configuration management (reqs. 52-61)
• Strategic planning (reqs. 65-74)
• System and communication protection (reqs. 75-108)
• Information and document management (reqs. 112-119)
• System development and maintenance (reqs. 120-126)
• Security awareness and training (reqs. 130-135)
• Incident response (reqs. 136-152)
• Media protection (reqs. 154-160)
• System and information integrity (reqs. 161-173)
• Access control (reqs. 174-203)
• Audit and accountability (reqs. 205-220)
• Monitoring and retrieving of control system security policy (reqs. 222-227)
• Risk management and assessment (reqs. 228-239)
• Security program management (reqs. 240-250)[19]
	• Antivirus protection
	• Backup infrastructure
	• Data loss prevention
	• SCADA protocols validation
	• Firewalls and IPS protection
	• Integrity of communication
	• Physical access control
	• Change of existing system configuration
	• LAN segmentation
	• Maintenance work
	• Procedures
	• Redundancy
	• Remote and external access-centralized system
	• Communication confidentiality (substation and centralized system)
	• Security events monitoring, managing, and reporting
	• Physical, environment
	• Vulnerability management
		• Standard
		  ○ Malicious software prevention
		  ○ Configuration management
		  ○ Cryptography and key management
		  ○ Backup and recovery
		  ○ Network security
		  ○ System acquisition, development, and maintenance
		• Human resources security
		  ○ Prior to employment
		  ○ Training and awareness
		  ○ After employment or upon reassignment
		• Physical and environmental security
		• Business continuity management
		• Incident management
		• Compliance and improvement
		• Access control

[19] It is apparent that the full list provides gaps w.r.t. the natural numbers sequence, both within categories and in the transition from one category class to another, as if some previously envisaged requirements were later withdrawn.

Table** 12 – **Organizational and personnel security measures collected by ESSENCE

Type of protection		Standard describing security		
		ISO 27001/ISO27002	IEC 62351	NIST 800-53
Security policy and procedures				
1	Security policy and procedures	X		X
Organizational security				
2	Management policy and procedures	X		X
3	Management accountability	X		X
4	Baseline practices	X		X
5	Coordination of threat mitigation	X		X
7	Termination of third parties access	X		X
Personnel security				
8	Personnel security policy and procedures	X		X
9	Position categorization	X		X
10	Personnel screening	X		X
11	Personnel termination	X		X
12	Personnel transfer	X		X
14	Third-party personnel security	X		X
Physical and environmental security				
20	Monitoring physical access	X		X
22	Visitor records	X		X
23	Physical access log retention	X		X
31	Alternate work site	X		X
32	Portable media	X		X
33	Personnel and asset tracking	X		X
35	Information leakage	X		X
37	Physical device access control	X		X
System and services acquisition				
40	Life-cycle support	X		X
43	Software license usage restrictions	X		X
46	Outsourced control system services	X		X
47	Developer configuration management	X		X

48	Developer security training	X		X
49	Supply chain protection	X		X
50	Trustworthiness			X
51	Critical information systems components	X		X
Configuration management				
52	Configuration management policy and management	X		X
53	Baseline configuration	X		X
54	Configuration change control	X		X
55	Monitoring configuration changes	X		X
56	Access restriction for configuration change	X		X
60	Addition removal and disposal of equipment	X		
61	Factory default authentication management	X		X
Strategic planning				
65	Interruption identification and classification	X		X
68	Testing	X		X
69	Investigating and analysis	X		X
70	Corrective action	X		X
71	Risk mitigation	X		X
72	System security plan update	X		X
73	Rules of behavior	X		X
74	Security-related activity planning	X		X
System and communication protection				
75	System and communication protection policy and procedures	X		X
77	Security function isolation	X		X
78	Information in shared resources	X		X
79	Denial of service protection	X	X	X
81	Boundary protection	X		X
82	Communication integrity	X	X	X
83	Communication confidentiality	X	X	X
84	Trusted path	X		X
85	Cryptographic key establishment and management	X	X	X

86	Use of validated cryptography	X	X	X
87	Collaborative computing devices			X
88	Transmission of security	X		X
89	Public key infrastructure certificates	X		X
90	Mobile code	X		X
91	Voice over Internet protocol			X
93	Security roles	X		X
94	Session authenticity	X	X	X
100	Honeypots			X
101	Operating system independent applications			X
102	Confidentiality of information at rest	X		X
104	Virtualization techniques			X
105	Covert channel analysis			X
107	Transmission preparation integrity	X		X
108	Non-modifiable executable programs	X		X
Information and document management				
112	Information classification	X		X
115	Information and document retrieval	X		X
116	Information and document destruction	X		X
117	Information and document management review	X		X
118	Media marking			X
119	Security attributes			X
System development and maintenance				
120	System maintenance policy and procedures	X		X
121	Legacy system upgrade	X		X
122	System monitoring and evaluation	X		X
123	Backup and recovery	X		X
125	Periodic system maintenance	X		X
126	Maintenance tools	X		X
Security awareness and training				
130	Security awareness and training policy and procedures	X		X
131	Security awareness	X		X
132	Security training	X		X

133	Security training records	X		X
135	Security responsibility testing	X		
Incident response				
136	Incident response policy and procedures	X		X
139	Incident response training	X		X
140	Continuity of operations plan testing	X		X
141	Continuity of operations plan update	X		X
142	Incident handling	X		X
143	Incident monitoring	X		X
144	Incident reporting	X		X
145	Incident response assistance	X		X
147	Corrective action	X		X
148	Alternate storage site	X		X
150	Alternate control center	X		X
151	Control system backup	X		X
152	Control system recovery and reconstitution	X		X
Media protection				
154	Media protection policy and procedures	X		X
155	Media access	X		X
156	Media classification	X		X
157	Media marking	X		X
159	Media transport	X		X
160	Media sanitization and disposal	X		X
System and information integrity				
161	System and information integrity policies and procedures	X		X
162	Flaw remediation	X		X
163	Malicious code protection	X		X
164	System monitoring tools and techniques	X		X
165	Security alerts and advisories and directives	X		X
166	Security functionality verification	X		X
167	Software and information integrity	X		X
169	Information input restrictions	X		X
170	Information input validation	X		X

172	Information output handling and retention	X		X
173	Predictable failure prevention			X
Access control				
174	Access control policy and procedures	X		X
175	Identification and authentication policy and procedures	X		X
176	Account management	X		X
177	Identifier management	X		X
178	Authenticator management	X		X
179	Account review	X		X
180	Access enforcement	X		X
181	Separation of duties	X		X
182	Least privilege	X		X
185	Device identification and authentication	X		X
186	Authenticator feedback	X		X
187	Cryptographic module authentication	X		X
188	Information flow enforcement	X		X
189	Passwords	X		X
190	System use notification	X		X
192	Previous logon (access) notification	X		X
193	Unsuccessful login attempts	X		X
194	Session lock	X		X
198	Access control for mobile devices	X		X
203	User-based collaboration and information sharing			X
Audit and accountability				
205	Audit and accountability policy and procedures	X		X
206	Auditable events	X		X
207	Content of audit records	X		X
208	Audit storage capacity	X		X
209	Response to audit processing failures	X		X
210	Audit monitoring, analysis, and reporting	X		X
211	Audit reduction and report generation	X		X
213	Protection of audit information	X		X

214	Audit record retention	X		X
215	Conduct and frequency of audits	X		X
218	Security policy compliance	X		X
219	Audit generation			X
220	Monitoring for information disclosure	X		X
Monitoring and retrieving of control system security policy				
222	Monitoring and retrieving control system security management policy and procedures	X		X
223	Continuous improvement	X		X
224	Monitoring of security policy	X		X
225	Best practices	X		X
226	Security accreditation	X		X
227	Security certification	X		X
Risk management and assessment				
228	Risk assessment policy and procedures	X		X
229	Risk management plan	X		X
230	Certification, accreditation, and security assessment policies and procedures	X		X
231	Security assessments	X		X
233	Plan of action and milestones	X		X
234	Continuous monitoring	X		X
236	Risk assessment	X		X
237	Risk assessment update	X		X
238	Vulnerability assessment and awareness	X		X
239	Identify, classify, prioritize, and analyze potential security risks	X		X
Security program management				
240	Information security program plan	X		X
241	Senior information security officer	X		X
244	Information system inventory	X		X
245	Information system security measures of performance	X		X
248	Risk management strategy	X		X

249	Security authorization process	X		X
250	Mission/business process definition	X		X

Bibliography

Angeletti, V., et al. *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.* Torino: CNR CERIS, 2014.

Bartosewicz-Burczy, Hanna, Clementina Bruno, Fernando Garcia, e Tadeusz Wlodarczyk. *Polish case study. Scenario-based assessment of costs and benefits of adoption of comprehensive CIP standards.* Torino: CNR CERIS, 2014.

Cherepanov, Anton, e Robert Lipovski. *Industroyer: Biggest threat to industrial control systems since Stuxnet.* 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (consulted on August 28, 2018).

Christopher, Jason D., Fowad Muneer, John Fry, e Paul Skare. *ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2) - Version 1.1*. Washington DC: U.S. Department of Energy (DOE), 2014.

CMMI Institute. *What is CMMI?* 2019. https://cmmiinstitute.com/cmmi/intro (consulted on 08 16, 2019).

Diu, Antonio. *Terms of Reference for the Trials.* Rapporto Tecnico CNR CERIS, Anno 9, n° 51, Torino: CNR CERIS, August 2014.

EPRI. *Cyber Security Metrics for the Electric Sector.* Product Brief, Palo Alto, Ca., USA: EPRI, August 2017.

Finardi, Ugo, Elena Ragazzi, e Alberto Stefanini. *Considerations on the implementation of SCADA standards on critical infrastructures of power grids. Ceris Technical Report N. 47 http://essence.ceris.cnr.it/images/documenti/RT_47.pdf* . Ceris Technical Report N. 47, http://essence.ceris.cnr.it/images/documenti/RT_47.pdf , 2013.

Fire Eye. «CYBER ATTACKS ON THE UKRAINIAN GRID: WHAT YOU SHOULD KNOW.» 2016. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf (consulted on August 08, 2018).

IEC - Int'l Electrotechnical Commission. *IEC TS 62443-1-1:2009.* 2009. https://webstore.iec.ch/publication/7029#additionalinfo (consultato il giorno August 29, 2018).

Masera, Marcelo, e Alberto Stefanini. *Towards Standardisation Measures to Support the Security of Control and Real-Time Systems for Energy Critical Infrastructures.* Luxembourg: Office for Official Publications of the European Communities, 2008.

Ragazzi E., Stefanini A., (2019), "Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies" in International journal of critical infrastructures, Vol. 15, No. 3, 206-228. https://www.inderscience.com/info/inarticletoc.php?jcode=ijcis&year=2019&vol=15&issue=3

Symantec Security, Response. *Destructive Disakil malware linked to Ukraine power outages also used against media organizations attacks.* 2016. https://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations (consulted August 28, 2018).