ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Ottobre

2014

Rapporto tecnico N.53

Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures

Giuseppe Calabrese, Ugo Finardi and Elena Ragazzi

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

RAPPORTO TECNICO CNR-CERIS

Anno 9, N° 53; Ottobre 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.

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

The Commission is not responsible for any use that may be made of the information contained therein, the sole responsibility lies with the authors.

Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures

Giuseppe Calabrese, Ugo Finardi and Elena Ragazzi * [1]

National Research Council of Italy
Institute for Economic Research on Firm and Growth
CNR-CERIS Collegio Carlo Alberto - via Real Collegio, n. 30
10024 Moncalieri (Torino) – ITALY

*Corresponding author: e.ragazzi@ceris.cnr.it
☎ 011-6824.930

ABSTRACT: This study presents an analysis of costs deriving from the implementation of security standards for SCADA systems of electric critical infrastructures. It is produced concluding the path of ESSENCE project and it starts from the experience of the two case studies performed in its context. It aims at obtaining a reasoned measure of the costs needed to implement the standards. The first section contains an introduction describing the main hurdles and sets of problems encountered in the implementation of cost analysis. Then the generalities of the two case studies are introduced, followed by the detailed evidence outlined from both. At the end of the study useful suggestions for Transmission System Operators and Generation Operators are offered, besides a reasoned set of figures assessing the costs on the implementation of security systems.

Keywords: cost analysis; SCADA systems security standard; electric critical infrastructures.

JEL code: D61, G17, H56, L94

[1] This report is based on Activity "Cost analysis of standard compliance. The authors thank all the Essence staff who contributed, directly or indirectly, to this task; in particular: Marco Alessi, Marco Biancardi, Luca Guidi, Daniela Pestonesi, Alberto Stefanini, Tadeusz Włodarczyk.

SUMMARY

1. INTRODUCTION

Analysing costs of implementation of standards for the security of SCADA[2] systems of electric critical infrastructures is a complex exercise. Countermeasures included in standards are made of a complex mixture of hard and soft components, of new procedures and organisational assets. For this reason many cost items may be hidden and difficult to evaluate in their real extent. Only a simulation based on a real case study may lead to a realistic estimate. The variables are many, including the number of standards and of countermeasures to adopt, and there are several issues relating to each country and its characters. Thus it is important to start highlighting some relevant points, partly deriving from the case studies implemented in the context of the Essence project.

The first relevant fact to point out is the extreme complexity of protection, as possible attacks considered by standards encompass several layers of the network structure, distributed at several locations[3]. Besides the physical level has to be considered as well, and thus the need to protect the boundaries of the structures, and further threats deriving from personnel.

Moreover many countermeasures are encompassed in different standards[4]. This means that there is intersection between standards in terms of the presence of common countermeasures. Then, a relevant hurdle is the fact that costs of standards implementation might entail the cost of the same countermeasure in more than one standard. Thus the cost of single (possible very expensive) countermeasures might apply to more standards. These, in turn, 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. Since congruence between standards is great but not complete, a further line of analysis should assess the marginal effort to be borne by a firm who already decided to comply to one standard on a voluntary basis, in case another standard became mandatory. In the case studies we observed that standards like NIST, ISO, ISA/IEC are more or less compatible, but this comparison should in the future be made more precise. This detailed analysis could release the reluctance of electricity utilities to further invest on security against cyber-attacks, even on a voluntary basis.

A further conceptual hurdle is the fact that some countermeasures are more relevant than others. That is, some of the countermeasures that standards foresee are more important and effective than others, whatever the costs of implementation and maintenance. Thus, some controls and countermeasures are mandatory, while other ones can be considered as optional/additional. In consequence of this it is always important to properly identify the weaknesses existing in the single critical infrastructure (or to the local/national system)

[2] Supervisory Control And Data Acquisition

[3] For a carefully presentation of the impact of malicious incidents, or natural ones, on the main layers of an electric system, please see Antonio Diu (2014), "Terms of reference for the trials" Ceris technical report, special Essence series N. 51. http://www.ceris.cnr.it/ceris/rt/RT_51.pdf

[4] For a review of reviews the main existing or forthcoming standards that can directly or indirectly concern the power systems -analyzing their matureness, wideness and specificity of scope, points of strength and weakness – 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 report, special Essence series N. 47. http://essence.ceris.cnr.it/images/documenti/RT_47.pdf

at the point of application of standards. This is useful to evaluate vulnerabilities and then possible risks, and then – once identified them – to implement the correct countermeasures.

It must also be noted that cyber systems used to operate power facilities differ substantially from those commonly implemented in ICT and, thus, also security differs in large scale.

The first, main difference is due to a fact that has a very high impact on the security of SCADA system of electric critical infrastructures. That is, technologies are often used for a time much longer than their usual lifetime in general IT companies. A meaningful example is that of Microsoft Windows XP operating system. This is still commonly exploited inside Intelligent electronic devices and in the office system of the automation sector. Nevertheless its support by the producer has ceased in April 8th, 2014. In power stations equipment this operating system will instead be at work for many years after its cessation.

This fact is mainly due to high costs of substitution. In turn, these high costs are first of all those of equipment and of workload of specialists. Then there are also costs depending on the need to stop the infrastructure in order to dismantle the equipment and then to replace it, program it and test it. Moreover there is a relevant need of continuity (plants can’t be fully stopped), of precision of time parameters of devices and of reliability of communications. Finally, in the case of power facilities it is not possible to break operational services.

Costs for the implementation of security standards are of different types. First of all, fixed costs, independent on the number of critical infrastructures to protect, exist. Such costs are relative to the complex of the system (regional, national etc.) to be protected. A second type of costs are those that are scalable as they are relative to the single infrastructure, and thus depend on how many infrastructures must be protected.

Moreover, besides costs of initial implementation, also costs of maintenance and continuous upgrading must obviously be taken into consideration. Such running costs encompass costs for personnel as well as costs for the maintenance of physical infrastructures, of hardware and of the software.

A final important note is relative to the state-of-the-art of SCADA systems security in the critical infrastructures of different operators in different countries. It is rather obvious that, at the present stage, every operator has already implemented some security instruments in order to reduce the vulnerability of the systems. Thus, as Essence case studies show, attaining a common level of security following the common adoption of standards at European level will, in general, entail in practice lower (or even much lower) costs than starting from an hypothetical 0 level. This independently from which standard or guideline will become mandatory because, as reported above, several countermeasures are encompassed in more than one standard.

2. EVIDENCE FROM THE CASE STUDIES

The last years have witnessed an escalation of cyber-attacks. These have become more copious and much more sophisticated, and their consequences have been more catastrophic. Thus it is in the interest of enterprises to multiply efforts in order to overcome the consequences of possible attacks due to failures in the information security systems. These breaches can result in attacks affecting infrastructures and possibly compromising data of key value.

As above underlined, general information system security present differences with security for industrial automation and control systems. In the latter, requirements for integrity, availability, performance, and immediate access are higher. Moreover potential impacts of an attack on such systems might entail, besides losses of money and public confidence, regulatory requirements violation, damage to equipment and environment, and endangerment of public and employee safety. Thus the critical role of security in industrial automation and control systems is a relevant driver towards the adoption of standards and the identification of countermeasures to be compliant with them.

In order to prepare suitable case studies, due diligence has been followed in order to choose critical yet realistic situations. The cases start from the intrinsic characters of the power grids and of their interconnections at European level. Critical conditions have been studied, and the case of hypothetical cyber-attacks have been applied to specific locations and timings. The two case studies hypotheses of the Essence project are relative to: an attack to the dispatch of energy in an urban area; an attack to a production plant affecting a wide area. In these cases, after the hypothetical cyber-attack, a load shedding takes place. Thus a proper time for recovery is needed, following a specific procedure. In the case studies the prolonged black out affects households as well as productive activities of different kind.

The impact of the interruption of energy supply is dependent on several factors related to the customers. Basically, electricity customers can be divided into different groups: residential, industrial, commercial and services. First of all, the type of customer (household, production plants etc.) has to be considered. Then other relevant factors are the load demand at time of outage, its duration, the specific moment of outage (period of the year and of the day), as well as the specific day of the week (working day or weekend). In fact different types of customers could be more or less exposed to the effects of electric interruptions. They could for instance incur in higher or lower costs depending on the different times of the year. This might be due in turn to the seasonal nature of their activities and needs: for instance some industries in some season or months are more active than in other.

The costs of electricity supply interruption in households depend primarily on the presence of persons at home during power outages. Moreover the kind of electric furniture (such as cooling/heating systems) or of safety equipment is relevant for the social cost.

In general the consequences of the disruption of electric system (and consequent interruption of dispatching) can be classified either as direct or indirect socio-economic impacts.

The direct economic impact resulting from sudden cuts of power supply includes for instance: lost production; idle but paid-for resources; spoilage of raw materials or food; damage to equipment; direct costs associated with human health and safety; utility costs associated with interruption; inconvenience due to lack of electricity at home; lack of transportations; personal injuries. Indirect impacts for example are: civil turmoil and looting during extended blackout; failure of industrial safety device in entities, necessitating neighbouring residential evacuation, etc.[5]

2.1 Standards implementation

There are different kind of problems entailed by cyber-attacks. Thus implementation of countermeasures should be considered meaningfully in order to have an impact on the three different categories of problems.

[5] R. Billington (chair); Methods to consider customer interruption costs in power system analysis. Task Force 38.06.01, CIGRE 2001.

These are:

- limit as much as possible the propagation of an attack carried out on levels such as organizational (diversification of service providers), network transmission (heterogeneous structure of devices all of which are built facilities which supply agglomeration) and operation of ICT systems on stations (removing vulnerabilities, hardening, separation, white listing, firewalls),
- maximizing the probability of attack detection during the phase of attack identification, implemented through the building of intersystem communication nodes and inter-control points (which will automatically detect malicious attempts to communicate), construction of honey pot traps type and construction of systems for automatic analysis and correlation of events,
- minimizing the duration of any single failure.

The stated countermeasures are possible points of departure for countering each threat and permit initial estimation of the total effort required to repulse each threat. Countermeasures against risk are required to ensure that the critical infrastructure may operate well and in particular that the security of supply is ensured. Particularly, this includes all ICT components, which directly deal with energy for monitoring and control 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. The first one is the requirements definition of the architecture. These must ensure the implementation of the main important and well known security mechanisms.

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

Starting from the IT architecture, common security architecture must be based on the segmentation of the Control System Network. This means partitioning of the system into distinct security zones and implementation of protection layers to isolate the most critical parts of the system.

This means that:

- 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).

Once built according to the above described assumptions, a security strategy should significantly reduce the number of potential cyber attackers to only a very small group of experts. Such expert are those whose knowledge, budget and time allow to break any security using methodologies that are transparent to monitoring systems. In fact, in practice, the high probability of being detected at the first error committed during attack should be an effective deterrent. This should discourage the vast majority of attackers to implement attacks. Nevertheless other methods to perform an attack, for instance using physical attack, may still be as effective as the (discouraged) cyber-attack.

Particularly, in the considered Italian Use Case, defence in depth 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, a zone requires that all resources inside its borders have a certain minimum level of security as determined by the organization’s security policies. In order to ensure a high security zone the trust level must be very high.

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.

After the selection of necessary countermeasures, it was necessary to verify how they were dealed with by the most relevant and mature standards. This analysis was conducted on one standard specific for the energy sector (NERC), two standards/guidelines on the information system (ISO/IEC 27001 – *Information Technology – Security Techniques* and NIST 800-53 – *Recommended security controls for information systems*) and finally two standards on ICS (ISA 99-03-02 – *Security for Industrial Automation and Control Systems* and NIST 800-82 – *Guide to Industrial Control Systems Security*). All those standard recommend similar countermeasures, although some technical or procedural details may differ.

Coming to the Polish case, a set of 211 countermeasures has been identified, including:

- a set of 54 countermeasures, which act to block feasibility of remote attack by unauthorized persons (remote attack means that was realized from different system than attacked),
- a set of 78 countermeasures, which act to block possible local attack (with physical access to console of a system or its products) either by staff or by unauthorized persons,

- a set of 40 countermeasures, which interact to allow hazard on identification stage reconnaissance and preventing its escalation,
- a set of 39 countermeasures, which interact to shorten downtime of systems that have been successfully attacked

With reference to these countermeasures, three standards have been identified as particularly relevant for the Polish case study analysis. These are: the ISO /IEC 27000 - Information Security Management Systems series of standards; the NIST SP-800-53 - Information Security, Recommended Security Controls for Federal Information System and Organizations; the IEC 62351 - Power system management and associated data exchanges.

The three standards/guidelines have been selected starting from the comparison of ISO standards (used by TSOs in Europe) with the standard NIST (which is used in the U.S. and by the TSOs in the United Kingdom). A further instrument used for the selection was the comparison of the countermeasures described in these standards with those presented in the attack scenarios in order to determine their impact on minimizing risks[6].

As above described, countermeasures are often not specifically dependent on the standard; on the contrary, some countermeasures might be foreseen by more than one standard. The choice of countermeasures should be preceded by the operational analysis of the transmission system. This should be properly built and designed for methods of dealing with failures. In fact, under a general point of view, transmission systems should be designed in order to maintain continuity in case of failure according to the N-1 criterion. In consequence of this design of the network only the coincident presence of multiple failures is able to disrupt significantly the performance of its operability as a whole.

In principle this strategy should be adapted to the design of ICT security inside each single substation. That is, a key feature should be the implementing of such countermeasures that are able to limit the spread of cyber attacks and incidents and, with respect to a single object, to minimize the impact of duration of disruption of the dispatching of power supply.

In adapting this strategy to the single transmission facility, a distinction should be made between at last three types of substations that are present in the power dispatching network, and which are particularly important:

- substations which supply electric power to urban agglomerations;
- substations which distribute to the network the production capacity of power plants;
- substations for international connection of power transmission networks.

3. THE COST ANALYSIS: EVIDENCE FROM THE CASE STUDIES

This section aims to identify the state-of-the-art security practices and countermeasures developed and achieved by leading international bodies and institutions which have been focusing and engaged on such a subject first and more heavily, and to quantify the subsequent financial effort necessary to adopt them. The

[6] See Essence deliverable “Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria”. RAPPORTO TECNICO CNR-CERIS Anno 9, N° 48; November 2013. ISSN online: 2282-5665. http://www.ceris.cnr.it/ceris/rt/RT_48.pdf

official publications (i.e. standards, recommendations, guiding policies, guidelines, paper of prescriptions, ...) issued by pertinent and remarkable institutes have been retrieved, classified, sorted out according a given structured collection model, allowing us to select the most effective measures for each official document.

The analysis estimates the cost that a country should deal with in the adoption of security standards in the transmission and generation of electricity. The methodology adopted determines the cash flow for the implementation and maintenance of the security standards.

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. Nevertheless, hardware and software suffer depreciations and should be realistically replaced in a range of time from 5 to 10 years.

Unfortunately, it was impossible to similarly arrange and detail the costs related to the adoption of security standards in the transmission and generation of electricity. Transmission system operator and generator companies present distinct peculiarities that make difficult to define a common itemized scheme.

In both national cases two situations have been considered: costs that should be borne by a country who hasn’t implemented any security countermeasure and costs that should be borne starting from the current situation in the two case studies, in order to manage a higher supplementary security.

3.1 Costs related to the adoption of security standards in a transmission system operator

ICT systems for power facilities are heavily different from those employed in IT companies. Differences are due not to a different use of technology, but to the methods employed for their implementation and integration with other systems. As mentioned in the introduction, obsolete systems continue to be used in, due to difficulties in their substitution and to impact costs (e.g. Microsoft Windows XP). This means that equipment and IT systems providers are not able to remove all vulnerabilities in the products they offer.

Another reason for complications associated with implementation of IT security for substations are different needs in terms of continuity, certainty of time parameters of devices and reliability of communications sent by them. That is, power generation and distribution activities cannot be interrupted in providing or receiving energy, as it may happen in other production systems and businesses, for the time of the substitution and testing of the IT systems.

Moreover, installed countermeasures cannot introduce delays in transmission of signals, e.g. packet Goose (Generic Object Oriented Substation Events) in accordance with IEC 61850, and shall not affect increase time process protection, which would result in delay in sending a packet. Filtering at network level cannot cause changes in sequence of packets or modify their contents or drop packets, which could cause misrepresentation of transmission.

Thus, while developing proposals for lists of recommended standards, one should take into account not only their costs, but also to estimate the difficulty of their implementation. This in turn results from the need to maintain the required quality parameters for IED (Intelligent electronic device) work on substations. That is, the higher the degree of complexity, the less the likelihood of success in their implementation.

On the basis of the experience of the Polish partner of the Essence project, the following list of countermeasures has been drawn up based on security impact assessment, organised by group of homogeneous countermeasures.

Table 1: Complete list of countermeasures to be implemented in all areas

GROUP OF COUNTERMEASURES	**COUNTERMEASURES**
Antivirus protection	Mobile code; Malicious code protection
Backup infrastructure	Backup and recovery; Control system backup; Control system recovery and reconstitution
Data loss prevention	Information leakage; Information in shared resources; Portable media
Scada protocols validation	Information input restrictions; Information input validation
Firewalls and IPS Protection	Denial-of-service protection; Boundary protection; Covert channel analysis
Integrity of communication	Communication integrity
Physical access control	Physical access control; Physical device access control
Change of existing system configuration, maintenance work, maintaining access control	Portable media; Access restriction for configuration change; Configuration settings; Configuration for least functionality; Factory default authentication management; Management port partitioning; Session authenticity; Architecture and provisioning for name/address resolution service; Secure name/address resolution service (authoritative resolver); Secure name/address resolution service (Recursive or caching resolver); Information system partitioning; Alternate command/control method; Account management; Identifier management; Authenticator management; Access enforcement; Least privilege; User identification and authentication; Permitted actions without identification and authentication; Device identification and authentication; Information flow enforcement; Passwords; System use notification; Previous logon (access) notification; Location of control system assets; Session lock; Remote session termination; Wireless access restrictions; Time stamps; Session audit; Control systems connections; Timely maintenance
LAN segmentation	System connections

Maintenance work	Personnel termination; Monitoring physical access; Emergency shutoff; Personnel and asset tracking; Power equipment and power cabling; User installed software; Testing; Investigating and analysis; Corrective Action; Risk mitigation; System security plan update; Media marking; Legacy system upgrade; Periodic system maintenance; Security responsibility testing; Incident response training; Incident handling; Incident response assistance; Incident response plan; Corrective action; Media sanitization and disposal; Security functionality verification; Predictable failure prevention; Security accreditation; Security certification
Procedures	Coordination of threat mitigation; Security policies of third parties; Termination of third parties access; Personnel security policy and procedures; Position categorization; Personnel screening; Personnel transfer; Access agreements; Third-party personnel security; Physical and environmental security policies and procedures; Visitor control; Visitor records; Physical access log retention; Delivery and removal; Systems and services acquisition policy and procedures; Allocation of resources; Acquisitions; Control system documentation; Software licence usage restrictions; Security engineering principles; Supply chain protection; Configuration assets; Addition removal and disposal of equipment; Strategic planning and procedures; Control system security plan; Roles and responsibilities; Planning process training; Rules of behaviour; Mobile code; Security roles; Confidentiality of information at rest; Heterogeneity; Information and document retention; Information handling; Information classification ; Information exchange; Information and document classification; Information and document destruction; Unplanned system maintenance; Maintenance tools; Maintenance personnel; Non-local (remote) maintenance; Security awareness; Security training; Incident response policy and procedures; Continuity of operations plan; Continuity of operations roles and responsibilities; Incident reporting; Fail-safe response; Media protection policy and procedures; Media access; Media classification; Media storage; Media transport; System and information integrity policies and procedures; Malicious code protection; Information output handling and retention; Access control policy and procedures; Identification and authentication policy and procedures; Separation of duties; Remote access policy and procedures; User-based collaboration and information sharing; Publicly accessible content; Audit and accountability policy and procedures; Response to audit processing failures; Conduct and frequency of audits; Auditor qualification; Security assessments; Critical infrastructure plan
Redundancy	Alternate work site; Alternate storage site; Alternate control center
Remote and external access (centralized system)	Remote access; Access control for mobile devices; External access protection
Communication confidentiality (substation and centralized system)	Communication confidentiality; Trusted path
Security events monitoring, managing	Configuration change control; Monitoring configuration changes; Interruption identification and classification; Collaborative computing devices; System

and reporting	monitoring and evaluation; Incident monitoring; Flaw remediation; System monitoring tools and techniques; Software and information integrity; Error handling; Account review; Authenticator feedback; Unsuccessful login attempts; Auditable events; Content of audit records; Audit storage capacity; Audit monitoring, analysis and reporting; Audit reduction and report generation; Protection of audit information; Audit record retention; Security policy compliance; Continuous monitoring; Honeypots
Physical, environment	Emergency power; Fire protection; Temperature and humidity controls; Water damage protection
Vulnerability management	Vulnerability assessment and awareness; Security alerts and advisories and directives

3.1.1 The Polish case

In order to perform a cost analysis of the implementation of countermeasures, in the Polish case two conditions have been taken in account. The first one is that of costs that should be borne by a transmission system operator (TSO) not having any security, that is, “Cost starting from 0”. The second one is the existing situation in Poland, that is costs that should be borne starting from the current state of the art in order to attain sufficient supplementary security.

In the analysis of the Polish case, the following assumptions were made:

- Countermeasures are calculated for 100 substations;
- Information Industrial Control Systems (ICS Systems), Office Systems (MMS office) in primary and in backup data centre counted 100 servers;
- Implementing of the security standards refers to the acquisition and installation of hardware and software;
- Maintaining of the security standards refers to the annual cost of the implemented countermeasures, that is software licences, warranties, upgrading and personnel;
- The costs of 1 man-hour for an expert worker is € 20;
- Redundant Internet nodes count for a total of 40 servers;
- The Polish transmission system operator (PSE) employs at present 2,000 employees.

The analysis can be performed for different needs, that is: the implementation and maintenance of countermeasures for minimizing remote attacks; the implementation and maintenance of countermeasures needed for minimizing the effects of a local attack; the implementation and maintenance of countermeasures needed for preventing the propagation and escalation of an attack and the implementation and maintenance of countermeasures needed for shortening the duration of the effects of a cyber attack.

The most recommended way to increase the level of security is the comprehensive implementation of countermeasures in all areas. The above reported approach allows us to realize economies of scale and is the most effective for meeting costs: it means realistically paying to implement systems that support and automate the execution of processes for maintenance and monitoring of safety, and that human resources dedicated to maintaining security processes are better utilized.

Table 2: 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
Maintenace 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**

Table 2 shows the total cost for implementing (initial investment) and maintaining (annual management) in Poland the security standards encompassing the listed countermeasures in the case of "Cost starting from 0". That is € 26,016,000 for implementing and 5,016,280 for maintaining.

Table 2 can also be the basis for estimating the cost of the implementation of countermeasures in other TSOs as reported in section 3.1.

The final element of the analysis is the summary of the costs of implementing and maintaining the countermeasures in the current Polish situation (Delta cost).

For this reason an analysis of the level of security implementation (as percentage) by Polish TSO has been performed. This analysis shows that at present, when considering different network levels, security has been implemented in different percentage. As this kind of data are confidential, these percentages (on which the case study relies) cannot be disclosed for each technology area.

The total cost of implementation of additional countermeasures not yet existing in Poland is € 7,486,000 and the additional annual cost for maintaining the implemented countermeasures is € 2,457,200.

3.2 Implementation costs of security standards in a generation company

Countermeasures against risk are required to ensure that the plants operate well and, in particular, that the security of supply is ensured. Particularly, this includes all ICT components, which directly deal with energy for monitoring and control such as SCADA systems. The security of these systems 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.

In the case study of the implementation costs of security standards in a generation company, every security requirement has been evaluated and categorized with respect to two main dimensions: governance and technical requirement. This last dimension (i.e. technical) is divided in three categories: hardening, network technical requirements, and host security requirements.

Governance costs

This cost typology identifies governance requirements established in international standards, best practices and policies on the industrial control system security in the energy sector SCADA systems.

The costs related to the governance requirements have been 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. Costs refer to the definition of a high level team within the company that implements yearly all the organizational aspects of the security program.
- 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. Costs refer to the definition of one technical skilled team in order to cover all the aspects of the internal organization and one technical skilled team in order to control the external parties.
- Security policy: this area includes all security requirements concerning policies, procedures and plans of actions on SCADA and industrial control system security. Costs refer to the definition of a team of ICS-IT skilled people.
- 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. Costs refer to a consultancy contract with a security company.
- Asset Management: this area includes all security requirements concerning asset management needed to achieve and maintain appropriate protection of SCADA and industrial control systems assets. Costs refer to a consultancy contract with a security company. Also automated technical solution for asset management can be implemented.

Costs for the adoption of hardening requirements

Most systems offer network security features to limit outside access to the system. Software such as antivirus programs and spyware blockers prevent malicious software from running on the machine. Yet, even with these security measures in place, systems are often still vulnerable to outside access. System hardening, also called operating system hardening, helps minimize these security vulnerabilities.

Therefore, 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.

Particularly, standards may provide the guidelines to implement the capabilities necessary to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services. It explicitly requires enabling only ports and services required for operations and for monitoring cyber assets.

Typical costs related to these countermeasures are: malicious software prevention; configuration management; cryptography and key management; backup and recovery; network security; system acquisition, development and maintenance; human resources security; physical and environmental security; business continuity management; incident management; compliance and improvement; access control.

Costs for the adoption of network technical requirements

This cost typology identifies network technical requirements established in international standards, best practices and policies on the industrial control system security in the energy sector SCADA systems.

In compliance with the methodology of analysis identified, the network technical requirements have been included in the following areas:

- Communication and Operations Management: this area includes all requirements concerning security aspects of communication management on industrial control system environment (e.g. network secure architecture, perimeter security, secure communication protocols) and operation management on industrial control system environment (e.g. configuration and change management, backup and recovery, monitoring);
- Access Control: this area includes all security requirements to protect SCADA and Industrial control system from unauthorized access to network, system, devices and information.

Costs for the adoption of host security requirements

This cost typology identifies, for each micro-area, host security requirements established in international standards, best practices and policies on the industrial control system security in the energy sector SCADA systems.

- Access control: In this section access control requirements for host security are collected and analyzed across the international standards, best practices and policies on the industrial control system security in the energy sector SCADA systems.
- Communications and operations management: Configuration management involves identifying the configuration of a system at given points in time, systematically controlling changes to the

configuration, and maintaining the integrity and traceability of the configuration throughout the system lifecycle.

- The standard indicates the controls that are used to verify modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
- System acquisition, development and maintenance: Systems/services acquisition deals with contracting and procurement of control systems components and associated services to ensure that no additional vulnerability is introduced throughout the system lifecycle management processes, without revision of the relative risk and without application of proper countermeasures.

3.2.1 The Italian case

In order to have an estimation of the total cost for Italy, the reference point is the main Italian player, that is ENEL, on which the case study simulated the implementation of the countermeasures listed in the preceding sections. It is possible to divide the costs in two main items: governance costs and hardware and software costs.

The 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 is a global value (all the business areas for all the countries).

The hardware and software 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. It 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 to be borne only once, at the initial time; other costs, specifically those related to the operation and maintenance of the countermeasures, are labour costs to be borne annually (licences, warranties and upgrading have been considered as investment costs).

Nevertheless, it could be assumed that the initial investment in governance could be amortized in 10 years and the initial investment in hardware and software could be amortized in 5 years. As a consequence, after this period of time, the investments should be scheduled again.

As in the Polish case, it is possible to define 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 (that is firewall, antivirus and so on) has already been implemented by the company.

Table 3 shows the costs related to the implementing and maintaining of a detailed security program in the governance domain, in the case of “Cost starting from 0”.

Table 3: Governance costs for a large multinational company (€)

	IMPLEMENTING	MAINTAINING
Security Program	400,000	100,000
Organization of security	1,200,000	200,000
Security policy, standards and procedures	300,000	200,000
Risk Management	290,000	190,000
Asset Management	790,000	290,000
TOTAL	**2,980,000**	**980,000**

Table 4 reports the cost analysis for the hardware and software components related to the networks and hosts security of a typical 380 MW production unit with 6 servers and 6 clients. This table too reports only the values for the "Cost starting from 0" case for the implementation and the maintenance of the security standards. The cost for the adoption of hardening requirements have been included in network and host requirements.

Table 4: Hardware and software costs for a typical 380 MWe power unit (€)

	IMPLEMENTING	MAINTAINING
Network requirements	370,000	20,000
Host requirements	125,000	90,000
TOTAL	**495,000**	**110,000**

Combining table 3 and table 4 it is possible to have a rough estimation of the cost that ENEL should 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. Actually, generation capacity that Enel owns in Italy is less than one half of the global corporate generation capacity of ENEL in the world; and so it is possible to have the assumption to charge half of the Governance costs to the Italian production.

In table 5 are reported the situations without any kind of already existing countermeasures (Cost starting from 0) and the upgrading of the current situation (Delta cost). In this second case, as data are confidential, only the total amount is reported and not those for each technology area.

Table 5: Total costs for ENEL in Italy in the two hypotheses (€)

	COST STARTING FROM 0		DELTA COST	
	Implementing	*Maintaining*	*Implementing*	*Maintaining*
Governance costs	1.490.000	490.000	0	490.000
Network and host requirements	15.345.000	3.410.000	12.400.000	1.550.000
TOTAL	**16.835.000**	**3.900.000**	**12.400.000**	**2.040.000**

The first evidence is that governance costs are not the most important contribute to the total cost, being about 9% for the implementation and 12.6% for the maintaining in the zero case. Actually, security governance is an activity serving all the business areas of the company (electricity distribution, sale and so on). So these values are estimated for the whole ENEL group and do not refer only to generation activities.

To have a yardstick to assess the value indicated above, we can refer to yearly investments carried out by ENEL. In comparison with the global Investment of ENEL (5,000 M€ in 2013) and the total investment in Italian generation (318 M€ in 2013), it is possible to note that the costs related to the security of Italian generation (i.e. major Italian generation plants) is negligible if compared with the annual investment in Italian generation plants. In the case of ENEL the values to be considered in table 5 are the “Delta cost” and have to be compared with the total investment in Italian generation. The investment for the implementation of countermeasures is 3.9% of total investment, while the maintenance of the security standards represents 0.6%.

The value above are related to the investment to be carried out by Enel, but it is important to evaluate the cost related to the whole country. This was straintforward in the Polish case-study, because it dealed with a TSO, which is a unique operator.

ENEL is the largest Italian electric utility, the second one in Europe. After the Italian market liberalization, started in 1999 with the Bersani decree, many big and small generation companies (GenCo’s) have appeared in Italy and their market share has grown in time. 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 (hardware and software) on power plants hosts and networks in Italy due to the difficulty to establish the power units and plants to be hardened. A fair assumption is to consider only the dispatchable units[7] (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.

[7] Dispatching ensures the management of generation plants connected to a grid to guarantee real time balance between demand and supply of electricity. Non dispatchable units are those generating electricity by renewable sources like sun and wind, whose activity depends on meteorological conditions and so they are always given priority.

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. Excluding by the list of the Italian units owned both by ENEL and by other operators the units out of service, the number of plants to be protected is reduced. A reasonable estimation of the number of units to be considered is restricted to the range 50-100, depending on whether one wants to invest only on plants which are in full everyday operation, or also on plants employed sporadically following demand.

In this way is it possible to assess a range in the value of global cost related to the implementation of the countermeasures listed in section 3.2 in the Italian generation system (table 6).

Table 6: Total costs for in Italy in the two hypotheses (€)

	COST STARTING FROM 0		**DELTA COST**	
	Implementing	*Maintaining*	*Implementing*	*Maintaining*
Minimum 50 units	27,730,000	6,480,000	20,000,000	3,480,000
Maximum 100 units	52,480,000	11,980,000	40,000,000	5,980,000

4. Conclusions

In the previous section the cost assessment of the adoption of security standards in the Polish transmission system and in the Italian generation system has been reported.

In the Polish case the assessment is more precise due to the fact that a unique transmission system operator is in charge of the system, whereas in the Italian case, as in many other European countries, a lot of big and small generation companies operate. Due to this reason an estimation range has been pointed out (table 7).

In both national cases two situations have been considered: costs that should be borne if no security standards had been implemented yet (Cost starting from 0) and costs that should be borne starting from the current situation in order to manage a higher supplementary security (Delta cost).

The Polish and Italian cases can be used by other countries as methodological tutorial for their specific analysis.

When performing the analysis one can take into account different needs, that is: the implementation and maintenance of countermeasures for minimizing remote attacks; the implementation and maintenance of countermeasures needed for minimizing the effects of a local attack; the implementation and maintenance of countermeasures needed for preventing the propagation and escalation of an attack and the implementation and maintenance of countermeasures needed for shortening the duration of the effects of a cyber-attack. Our analysis showed that working at the same time on all the levels listed above is the best choice, because it guarantees both effectiveness (the highest level of security is reached) and efficiency (scope economies are possible so reducing the global investment required).

In the definition of policy recommendations, the “Delta cost” column has to be taken into account, as a number of countermeasures are yet running. In the case of Poland the required financial resources are about € 7,5 million for the additional countermeasures and € 2,5 million for the additional annual cost for maintaining. For Italy the estimation range of the financial resources required is € 20-40 million for the additional countermeasures and € 3,5-6 million for the additional annual cost for maintaining.

These data have to be compared with the impact cost of a single blackout (please see Clementina Bruno *et al.* Ceris Technical Report N. 52: Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case studies. http://www.ceris.cnr.it/ceris/rt/RT_52.pdf) and with the total investment of each operator in the electricity system. In the case of ENEL the percentage of the costs for standard compliance respect to total investment for Italy are respectively 3.9% for implementation and 0.6% for maintenance. Just as case of exercise, if the situation of the adoption of security standards in the transmission system by a country without any previous security may occur, table 8 shows a simulation for a smaller and larger a TSO than PSE (the Polish TSO). The basic assumption for the smaller and larger country is the adoption of countermeasures in respectively 30 and 200 substations. The data for Poland are the same of table 2 with the subdivision of maintaining costs in software and labour, whereas for the two example cases the simulation adopts a non proportional scale with regard the size of the TSO.

Table 7: Total cost of implementing and maintaining countermeasures in Poland and in Italy (000 €)

	COST STARTING FROM 0		**DELTA COST**	
	Implementing	*Maintaining*	*Implementing*	*Maintaining*
Electricity transmission in Poland	26,016	5,016	7,486	2,457
Electricity generation in Italy	27,730-52,480	6,480-11,980	20,000-40,000	3,480-5,980

Table 8: Total cost of implementing and maintaining countermeasures in a TSO (€)

		SMALLER COUNTRY	**POLAND**	**LARGER COUNTRY**
Implementing	Substations	6,047,200	15,118,000	27,212,400
	Information control systems	1,453,280	3,633,200	6,539,760
	Office systems	2,905,920	7,264,800	1,3076,640
	TOTAL IMPLEMENTING	**10,406,400**	**26,016,000**	**46,828,800**
Maintaining Software	Substations	834,900	2,087,250	3,757,050
	Information control systems	155,216	388,040	698,472
	Office systems	510,496	1,276,240	2,297,232
	Total maintaining Software	**1,500,612**	**3,751,530**	**6,752,754**
Maintaining Labour	Substations	208,800	696,000	1,392,000
	Information control systems	54,000	180,000	360,000
	Office systems	116,700	389,000	778,000
	Total maintaining labour	**379,500**	**1,265,000**	**2,530,000**
	TOTAL MAINTAINING	**1,880,112**	**5,016,530**	**9,282,754**