

# Rapporto tecnico N.57



**Trial evaluation: conclusive lessons  
from Essence case studies**

Fernando García Gutiérrez, Elena Ragazzi



## RAPPORTO TECNICO CNR-CERIS

Anno 9, N° 57; Dicembre 2014

### *Direttore Responsabile*

Secondo Rolfo

### *Direzione e Redazione*

CNR-Ceris

Istituto di Ricerca sull'Impresa e lo Sviluppo

Via Real Collegio, 30

10024 Moncalieri (Torino), Italy

Tel. +39 011 6824.911

Fax +39 011 6824.966

[segreteria@ceris.cnr.it](mailto:segreteria@ceris.cnr.it)

[www.ceris.cnr.it](http://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](mailto:e.viarisio@ceris.cnr.it)



Copyright © Dicembre 2014 by CNR - Ceris

All rights reserved. Parts of this paper may be reproduced with the permission of the author(s) and quoting the source.

Tutti i diritti riservati. Parti di questo rapporto possono essere riprodotte previa autorizzazione citando la fonte.

## ESSENCE

### *Emerging Security Standards to the EU power Network controls and other Critical Equipment*

*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 project have been published in the "Special Essence series on security standards for critical infrastructures", hosted in the "Ceris Technical reports series". The published titles, available at <http://essence.ceris.cnr.it/index.php/documents/2-uncategorised/14-reports>, are:

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



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 systems 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.*

# Trial evaluation: conclusive lessons from Essence case studies\*\*


Fernando García Gutiérrez

*DELOITTE ADVISORY SL  
Pza. Pablo Ruiz Picasso, 1,  
Torre Picasso, 28020 Madrid, España*

Elena Ragazzi\*

*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](mailto:e.ragazzi@ceris.cnr.it)

 011-6824.930

**ABSTRACT:** Several cyber-security frameworks have been developed to protect critical infrastructures from cyber-attacks, but it was rather difficult to anticipate costs and benefits of their adoption, although worldwide experience had shown that both are huge. This report summarises the results of the ESSENCE project, discussing the methodology used in the case-studies, and discusses the open issues and the policy implications. The analysis clearly shows that from a mere economic viewpoint, electric companies have no incentive to increase their security levels, as the annual costs of those countermeasures is much greater than their direct cost of the economic losses derived from 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.

JEL code: D61, G17, H56, L94

Keywords: impact analysis; SCADA systems, security standards; electricity, critical infrastructures

\*\* This report is based on Activity 6 “Evaluation of the trials”. The authors thank all the Essence staff who contributed, directly or indirectly, to this task; in particular: Marco Alessi, Marco Biancardi, Enrique Doheijo, Luca Guidi, Alberto Stefanini.

## SUMMARY<sup>1</sup>

1.	Introduction	7
1.1	Scope of this report	7
1.2	Evaluating the cost-benefit analysis: background	8
2.	Evaluation method	15
2.1	Trial evaluations	15
2.1.1	Kind of attack studied	15
2.1.2	Consequences of the attack	16
2.1.3	Which countermeasures are necessary to block the attacks.	16
2.1.4	How much does it cost to implement these countermeasures?	16
2.2	The cost analysis	17
2.3	The benefit analysis	17
2.3.1	The damage for firms	18
2.3.2	The damage for private users and for the society	18
3.	Description of the case studies	20
3.1	Italian case study	21
3.1.1	Studied scenarios	21
3.1.2	Case study	22
3.1.3	Countermeasures	23
3.2	Polish case study	24
3.2.1	Studied scenarios	24
3.2.2	Simulation of attacks	25
3.2.3	Use of standards and proposed countermeasures	26
3.3	Open issues and future directions of research	27
3.4	Summary of trial evaluations: good practices	30
4.	Conclusions of the evaluation (Summary of findings)	34
4.1	Key findings from the case studies	34
4.1.1	Vulnerabilities and countermeasures	34
4.1.2	Costs and benefits of standard implementation	35
4.2	The legacy of Essence: policy suggestions and open issues	37
4.2.1	Countermeasure actual implementation	37
4.2.2	The choice among standards	38
4.2.3	Policy and regulation issues	39
5.	References	40

<sup>1</sup> Although the report is the result of joint work and the conclusions have been discussed and agreed by both authors, sections 1, 2.2, 2.3 and 4 have been written by Elena Ragazzi and sections 2.1 and 3 by Fernando García Gutiérrez.

## 1. INTRODUCTION

### 1.1 Scope of this report

The Essence project, funded by the CIPS EU programme, was designed to evaluate costs and benefits of applying emerging security standards to the European power grid controls systems, based on two case studies. Industrial control systems are vulnerable to cyber-attacks that might affect large portions of the European power system, due to the interconnection of this last, making repair difficult and causing huge societal and economic impact. To counter this threat, which is common to several networked infrastructures such as the oil and gas and the water networks, as well as power, oil and chemical process plants, several standard frameworks are being proposed.

When more than two years ago this project has been conceived, a lot of work on the definition and also on the technical assessment of standards against malicious attacks had been done. Nevertheless, in Europe no clear position had emerged and, even, some standards had failed to be completed for years. Substantially it was hard to come to a full stop, because of many reasons, but one of them was the lack of concrete experience on what generalized standard compliance would imply. The USA experience showed that applying a standard is cumbersome and costly, that benefits are unclear and their perception depends a lot on the political mood of the period. But how much this judgment could be transferred in Europe was unclear as well. In Europe the actual situation of the electricity infrastructure is generally more updated, but the public opinion has a lower appreciation of security and defence countermeasures.

The idea that moved the promoters of the project was that, to exit this impasse, two dimensions were necessary:

- *Concreteness*. Only a close look into some real electricity facilities could lead to detailed and grounded estimates of the impacts of standards for European utilities.
- *Multidisciplinary integration* of technical and socio-economic assessment<sup>2</sup>. To identify costs and benefits on an objective basis, it is necessary that the economic evaluation reflects precisely the detailed features of the compliance process on the one hand; and on the other that this assessment is based on the characteristics (time, duration, geographical area and type of customers involved) of the simulated blackouts caused by malicious cyber-attacks.

This report goes through the two Essence case studies, based on an Italian generation company and on the Polish Transmission System Operator (TSO) and browses the main findings of the two activities of analysis

---

<sup>2</sup> For this reason we accepted the challenge of integrating a very heterogeneous partnership, composed of:

- one multinational generation company (Enel) and one TSO (PSE), to consider the operation point of view.;
- furthermore two consultancy firms specialized in risk assessment and in security of the control systems in the electricity sector (ADC)
- from the socio-economic side, IEN, a research body specialized on energy and electricity, University of Western Piedmont, with competencies on utility regulation and management, and CNR, an Institute of CNR specialized in industrial economics, policy evaluation, and accountancy data management.

(cost of standard compliance and benefit analysis) that have been carried out. The case studies concern very concrete simulations of likely situations in which an attack performed by a cyber-terrorist could take advantage of some vulnerabilities of the system and generate huge effects in terms of generalised black-outs. For this reason the results of the two case studies will be summarized in this report so as to drop any critical information. But these reports would like to go beyond a mere presentation of the main findings, assessing the methodology adopted and the features of the results which stem from this methodology. This assessment will lead to verifying whether there is room for improvement, above all in terms of reliability, precision and generality of estimates.

The aim of this assessment is not only to discuss and validate the results, but also to bridge them towards future challenges and research directions which are still to be explored. In particular, as underlined above, the main peculiarity of the Essence approach is its concreteness, deriving from the strict connection of the two simulations to the actual situation of two electricity utilities. But this concreteness is to the detriment of generality. Essence case studies highlight a feasible methodology to assess the impact in specific situations, but the final issue for its legacy is how to transform this methodological tutorial in a sound assessment at a EU27 scale.

## 1.2 Evaluating the cost-benefit analysis: background

The mission of the Essence project is to evaluate the effect of a particular type of policy, i.e. a regulation imposing the adoption of a particular standard. The perspective is then that of impact analysis, which requires assessing the effect of a policy on an outcome variable. To correctly isolate the effect of the policy it is necessary to compare two situations that differ just in the presence of the regulation.

For this reason the first dimension of the evaluation concerns the implementation of standards, and is the comparison between:

- A *situation without regulation*, where each firm autonomously decides a certain level of protections and undertakes consequently some investments and countermeasures which turn into some security costs;
- A *regulated situation* in which the minimum level of protection is established by the regulation itself, and which, in the case of Essence is represented by one security standard. The security cost is expected to be higher because, in the opposite situation (i.e. all firms investing by their own the correct level of resources in security, and would incur in no increase in costs) regulation would not be necessary<sup>3</sup>.

But in the case of security countermeasures, the assessment becomes more complicated because, whereas security costs are incurred in any case, security benefits emerge only in case of an attack whose consequences the countermeasures were designed to nullify or mitigate. To assess the benefits it will then be necessary to introduce a new dimension of evaluation, concerning the attack scenario. The evaluation compares the electricity system performances in two situations:

- Without cyber-attack.
- With cyber-attack.

---

<sup>3</sup> The need for a regulation is clearly highlighted by Essence results which will be presented in this report, and is discussed in the conclusions.



Of course relevant attacks are only those that really do threat the system operations, and which could overcome present countermeasures. It is in fact hardly imaginable a situation of a firm without any protection. Table 1 summarises the evaluation scheme.

**TABLE 1: DIMENSIONS FOR THE EVALUATION OF THE TRIALS**

		Standard implementation (regulation)	
		No. Every firm has freely implemented some countermeasures	Yes. All firm are requested to adopt an equal and higher number of countermeasures
Attack scenario	No relevant attack to the system		
	Yes, some attack is ongoing and can interfere with the system operations		

In any cell of Table 1 one has to calculate:

- The cost of running security measures. They should be the same per column except for costs associated with taking emergency actions in response to attacks (the so called recovery costs).
- The cost of producing (or purchasing) electricity and the cost of supplying it (in normal conditions and in case the attack causes disturbances able to disturb the operative management of electricity supply).
- The effect of interruptions in supply on the economy and the society (only in case the attack causes major disturbances which cause black-outs).

In both cases – countermeasure implementation and consequences of black-outs or other disturbances - the view must encompass the whole electricity system and not just a single operator or part. Although the unbundling process, which has been necessary for the introduction of competition in some phases of the electricity supply, has separated the operation of different phases in electricity supply, security has to be guaranteed for the whole system (generation, distribution, transmission) because its parts are interconnected, and failures in the protection infrastructure at any point may have consequences at all levels. This of course introduces some difficulty in the assessment because costs and benefits have to be estimated taking into account what happens all along the production chain, no matters it happens to be managed by different firms. The partial view is not only incomplete, but in some particular cases could prove misleading. For example it might happen that thanks to the attack, which causes a reduction in general supply, the local market prices increase and some firms might earn more, and even take advantage of the situation strategically so hampering the restoration of normal conditions.

The impact evaluation is based on some monetary indicators, which are explained in the following Table 2 and Table 3.

TABLE 2: SCHEMA OF ECONOMIC INDICATORS FOR THE IMPACT EVALUATION

Evaluation item	Protection scenario	Attack scenario	Cost category	Output of simulation	Output of case study / additional information available, from other sources	Description of indicators and type of information
A	Current situation and countermeasures	Attack NO	Operative cost of power supply	How much does it cost to supply electricity without attack and without the standard?		Total cost of production (or price of purchase) of the energy (generation + imports) exchanged in the scenario.
B	Current situation and countermeasures	Attack NO	Operative cost of security		How much does it cost to manage actual security systems?	Cost to maintain countermeasures operative and in service (personnel, material, and asset depreciation), associated with the present level of protection against cyber-attacks.
C	Current situation and countermeasures	Attack Yes	Operative cost of power supply (higher; internal cost)	How much does it cost to supply electricity in case of attack?		Total cost or price of the energy used in the scenario (in case of not complete black-out). The expected increase in costs is associated with the difficulty to supply power <sup>4</sup>

<sup>4</sup> In case of lower load and some losses in generation units, the average cost or price, is expected to be higher but could also be lower than the previous values. This increase (reduction) is a cost (benefit) for the company.

D	Current situation and countermeasures	Attack Yes	Cost of black-out	Which region will be affected by the blackout? For how long?	Characteristics of the customers not supplied?	The cost of the Blackout could be divided into: <i>Cost for the company</i> (physical destruction of equipment and cost of spare parts to be replaced, harm to employees) and the <i>losses generated to clients</i> due the black-out. The last one depends on their characteristics and on black-out duration and time venue. <sup>5</sup>
E	Current situation and countermeasures	Attack Yes	Increase in cost of security (emergency action)		How much would it cost to run current security countermeasures under attack?	The expected increase in ordinary is associated to costs associated with taking emergency action in response to attacks. (Recovery costs)
F	Standard countermeasures	Attack NO	Operative direct cost of security		How much does it cost every year to manage the countermeasures necessary to comply with the standard?	Current personnel and SW costs associated to security monitoring systems and security configuration management, considering a level of protection from cyber-attacks (each level has a different cost) suitable for the standard and the type of plant: personnel (internal or external) costs, personnel continuous training, enterprise-wide licensing, annual maintenance, ongoing compliance resource requirements. Transitory losses in productivity due to unfamiliar procedures and permanent losses in productivity due to time to comply security requirements should also be assessed.

<sup>5</sup> This item assesses mainly the direct or indirect costs (or reduction in utility) that customers face in case of interruption. This effect varies according to type of customers and their activities. So a lot of heterogeneous information has to be collected: type of consumers (industrial by size, commercial and services; residential, agriculture). Data on the economic and social direct and indirect impacts. Time of the interruption, number of consumers and their position in space.

G	Standard countermeasures	Attack NO	Investment (Depreciation)		<p>How much has to be spent to comply with the standard starting from the current situation? Which is the duration of investments (in order to calculate depreciations)?</p>	<p>New monitoring systems (HW and SW components) for plant components and infrastructures, for the level of protection indicated by the standard or suitable to the type of plant (each level has different cost). This may include a number of HW and SW for the implementation of the countermeasures (antivirus protection, backup infrastructure, data loss prevention, SCADA protocols validation, firewall and IPS protection, LAN segmentation, communication confidentiality, and so on), as well as training for the employees. Investment may also concern, in case of plants already protected in some way, the cost to adapt previous SW, HW and infrastructure to the requirements. In this case analysis of devices in order to verify if they fit in standard requirements and, eventually, cost associated to the change and the cost of tool integration.</p>
H	Standard countermeasures	Attack NO	Operative cost of power supply (it will probably be higher than without the standard)	How much does it cost to supply electricity without attack and with the standard?		<p>Total cost or price of the energy (generated or purchased) exchanged in the scenario. Considering also cost associated to operations and maintenance in normal conditions.</p>
I	Standard countermeasures	Attack Yes	Operative cost of power supply (it should be higher, the difference is the cost of the attack for the firm)	How much does it cost to supply electricity with the attack and with the standard?		<p>Total cost (generation or purchase) of the electricity exchanged in the scenario.</p>

J	Standard countermeasures	Attack Yes	Cost of blackout	Which region will be affected by the blackout? For how long? (It should be zero, or a smaller region, or for a shorter time)	Characteristics of the customers not supplied?	Same list as for item D
K	Standard countermeasures	Attack Yes	Increase in cost of security (emergency action)		How much would it cost to run standard security countermeasures under attack?	The expected increase in ordinary security costs is associated to costs associated with taking emergency action in response to attacks. (Recovery costs)

Table 2 describes the procedure that has to be adopted to assess the impact of standard on the whole system. The second and third columns indicate the two dimensions of comparison described in Table 1. Then, column 4 concerns the types of cost or effect to be considered. These encompass the cost of power (production, purchase and supply), the cost of running security countermeasures (with or without the standard, including also recovery costs), and the effects for the economy in case of blackout. These values have to be assessed for every specific case. In particular the actual level of countermeasures may differ a lot, as will be seen in case studies. A hypothetical, very unrealistic, situation in which no security countermeasure is implemented (which is referred in Table 4 as “no protection” case) would imply that current costs of security (item B) are zero. The cost of security includes both annual operative costs of management and maintenance, and the depreciation of investments. To highlight this, the operative cost of security with standards has been split into two items (F and G).

The information on these costs in the case study comes from two different sources: a simulation showing what would happen in the electricity system in a particular situation (time, day of the year, location) with or without attack. This will return the real flows of electricity exchanged, the cost of power supply and, eventually, the impact of the blackout generated by the disturbance. This information has to be integrated with other information coming from different sources, concerning on the one hand the type of customers involved by the blackout, and on the other the technical and organisational cost of security.

The assessment comes from the comparison between the different items that have to be calculated.

**TABLE 3: RELEVANT INDICATORS FOR THE IMPACT EVALUATION**

Calculation	Content	Notes
I + J + K	What happens in case of attack when adopting a standard	They include the socioeconomic effect of the blackout, the cost of supplying electricity - if the blackout is not total - and the recovery costs (the costs associated with the actions necessary to restore the normal situation).
C + D + E	What happens in case of attack without the standard	
<b>(I + J + K) – (C + D + E)</b>	<b>BENEFIT (in terms of avoidable cost)</b>	<b>The expected sign is minus (reduction in costs and negative effects, thanks to standard compliance).</b>
F + G	Cost of security with the standard	They include both annual costs and depreciation of investments. “A” could hypothetically be zero in the “no protection” theoretical case.
A	Cost of security without the standard	
H - B	Increase in the cost of electricity supply with the standard	It could be positive in case extra reserve capacity or more strict operative conditions are requested.
<b>(F + G + H) – (A + B)</b>	<b>COST of standard compliance</b>	The expected sign is plus.

## 2. EVALUATION METHOD

In the present section, the methodology for the Essence evaluation is lightly and clearly defined. Both, a high level quality and quantity assessment of case studies carried out during the project and a description of the subsequent cost and benefit analyses are included on the section.

On the subject of the trial evaluations overview, the following subsections response a set of questions raised in the following bullets:

- Which kinds of attack are considered in the case studies of Essence project? Where are they? When? What infrastructure?
- What are consequences of the happened event? Which are the direct effects on the infrastructure? How do they affect to their dependent activities?
- What are the countermeasures are necessary to block the attacks of the case studies? In which way are the implementations of the standards able to be used as a countermeasure to enhance the security of the infrastructures?
- What is the way to estimate how much the implement these countermeasures costs?
- How has it been evaluated the benefit of standard implementation?

### 2.1 Trial evaluations

In this chapter, the methodology used to evaluate the case studies (Poland and Italy) will be described. Diverse aspects of the case studies will be examined, to provide a broad view on them.

#### 2.1.1 Kind of attack studied

Case studies have been proposed for two countries: Poland and Italy. In both cases, a particular, but representative case has been studied.

- **Italy:** An attack on a power generation plant in a specific region, while the electric cable which connects a specific region and the mainland is being maintained. The case is considered to be quite likely. The attack is supposed to happen at 10 am of the third Wednesday of September, lasting for 6 hours. The attack scenario is focused on the effect of a concrete plant.
- **Poland:** in a specific region around a big city depends on three substations to receive electricity. An attack on these three substations can lead to a total blackout in the city. No particular scenario has been studied, but effects of a total blackout in the city have been reviewed.

### 2.1.2 Consequences of the attack

To estimate consequences of attacks, the load profiles of Italy and Poland have been gathered to the electricity needs during the attack. Consumption has been divided into sectors to estimate economic effects. Firstly, the total electricity consumption in the studied day has been calculated. Then, this consumption has been divided into different economic sectors (industry, agriculture, households, etc.).

Using these data, estimations of the load profile in a normal day similar to the studied day have been carried out. That way, the electricity that consumers would have used if they had not had their supply cut can be estimated. This has been done for different time periods and sectors.

The amount of electricity that each sector cannot use can be calculated. Besides, a recovery path has been proposed, estimating how much electricity is available for use, in different periods while the problem is solved. The first sectors to receive electricity are considered. Then, the effect of the lack of electricity has been evaluated.

Apart from the reduction in consumption by different sectors, the socio-economic impact has been evaluated. In the case of Italy, the attack is supposed to happen at the third Wednesday of September. The blackout would begin at 10 am, and 6 hours would be needed to recover the supply. There is no power supply until 1 hour and 15 minutes have passed.

### 2.1.3 Which countermeasures are necessary to block the attacks.

For both scenarios the potential countermeasures - based on standards - necessary to contrast the threats have been considered. Standards which have been taken into account include NERC, NIST and ISA, and have been described into high detail. These standards describe IT tool management procedures that can increase security of the power system.

Finally, according to standards, a number of countermeasures which can be applied are proposed. Countermeasures are based, mainly, on the following topics:

- Isolate security zones, to avoid the propagation of an attack between different parts of the system.
- Hinder, or make difficult the access to equipment by attackers: protect physically equipment, use of strong passwords, keep updated authorised users, etc.
- Use the system only for what it has been created: do not install unauthorized software, and do not use the Internet for unintended objectives.
- Restrict connection to portable computers, USB memory flicks, CDs, DVDs, etc.
- Ongoing monitoring of the system and use of antivirus software.
- Create plans for incident response, and keep these plans updated.
- Use of “demilitarized zones” and anti-DoS devices.

### 2.1.4 How much does it cost to implement these countermeasures?

Finally, the cost of implementing the countermeasures has been considered. To do so, it has been necessary to estimate the number of countermeasures and time to implement them. Cost for equipment (ICS Systems, backup systems, etc.) has been taken into account. Finally, the number of professionals needed to implement



measures, along with cost per hour and number of hours needed to implement each countermeasure has been considered.

Finally, the total cost of implementing each measure in each considered facility is estimated. Along with this, cost of maintaining measures is calculated. As a result, the total cost of implementing the countermeasures can be estimated.

## 2.2 *The cost analysis*

The costs calculated for the countermeasures selected in the two case studies are direct input of the cost analysis. This is particularly true in the case of the Polish case, which concerns a transmission system operator. Due to the interconnection of the grid it manages, any other solution than a whole country protection would not be acceptable. So the cost estimated in the case study already represents the cost for a country-wide protection of the grid. Moreover, since a part of the costs are fixed, but another part is linked to the number of substations present in the system, the data collected are a good basis to assess the scalability of the investment required.

The estimation of the investment and of the maintenance costs for a country is less linear in the case of generation. The presence of multiple operators acting as competitors does not allow to have detailed information on the operating situation of each plant and on the actual protection level. The Italian case study considered the costs connected to standard compliance for the whole firm included in the case study (ENEL). In particular governance costs cover the protection of the whole group, since procedures must be uniform in the whole company to ensure protection, while only the cost concerning the protection of Enel plants located in Italy is included.

These data concerning the Enel case-study have then been the basis for an estimate of the cost for the protection of the whole Italian generation system. Since this depends on the hypothesis on the operating conditions of the main generation plants, the country-scale estimate is expressed as a range. Furthermore, no serious scalability considerations could be done, because the costs strongly rely on the characteristic of the generation park, which varies a lot among European countries.

A complete picture for a protection at the whole country level would require also to consider the importance of protecting the greatest distribution networks. Essence project didn't include a case study on this, so an extension in analysis would be highly recommended.

## 2.3 *The benefit analysis*

Although cyber-attacks may cause many disturbances to the electricity system, the project concentrated on the most invasive consequence, black-outs, which can induce serious inconveniences to all kind of users: electricity firms, other firms and households. This damage occurs at multiple levels. Each level has to be investigated with appropriate techniques and represents the benefit of standard implementation, in the sense that it is an avoided cost for the economy.

### 2.3.1 *The damage for firms*

Blackouts may cause direct losses (damage to equipment and to raw materials) and indirect damage (stop in production) to firms. Qualitative interviews showed that:

- The ratio of indirect damage is in general much higher than the one of direct damages to plants
- The value of this last is often not negligible, but varies a lot, even within the same industry, following the plant characteristics. So, no macro, aggregate estimate is possible. The case studies offered some qualitative evidence on the nature and characteristics of this damage.

The basis for the calculation of the indirect damage is the quantity of electricity not sold in case of black-out. This has been obtained as an output of the case-studies. One must then assess how great is the economic damage deriving from the supply interruption. Here again some differences exist. First of all, for the electricity operators, it is necessary to estimate the lost revenue at all the levels of the service (generation, transmission, distribution, sale), considering the added value and the correct tariffs at that time (day and hour). For what the other industries are concerned, to pass from the quantity of electricity not delivered to economic damage, the VOLL (Value of the Lost Load) has been applied. It is a ratio, calculated from macro-economic statistics, comparing the value added registered in a certain time frame and in a specific area and the electricity consumed in the same context. The estimate will be more precise the more these ratios are calculated for specific industries, but the level of specificity is bounded by the availability of detailed data for the required industry and geographical area. The greater is the area of the blackout, the more detailed industry data will be available. Moreover, some detail will be lost when combining the taxonomy of industries applied by the national statistical office, and the one used for electricity statistics. These may be different and so it will be necessary to aggregate some industries, to reach a common classification. In the benefit analysis the maximum possible level of detail has been applied to each situation, considering available data.

Finally, in the case of firms, it must be considered that the electricity dependence is uneven among sectors: some kinds of activities can be carried on even in absence of electricity. Their weight largely depends on the type of production. Some scenarios taking into account this limited energy dependence have been estimated too.

### 2.3.2 *The damage for private users and for the society*

As for non-economic electricity users, there are many sources of damages linked to a black-out:

- Individual material damage (for example food spoilage)
- Individual immaterial damage (impossibility to practice the planned activities, anxiety to be blocked in unpleasant situations, the necessity to spend time to restart programmed domestic appliances)
- Collective damage (impossibility to supply essential services, increased criminality)

The third assessment requires several specific inquiries, which go out the scope of the Essence project, so the assessment connected to the case study was restricted to the first two types of damage and was based on a survey.

After a careful evaluation of the available methodological alternatives, the questionnaire was based on the concept of “Willingness to Accept”, i.e the willingness to be compensated for a blackout by a stated amount of money. In particular, after some questions aimed at obtaining some variables on the characteristics of the

users and also to increase their awareness on the importance of electricity in their life, the participants to the survey were asked to choose to accept or to refuse a set of different scenarios, represented by different blackout duration and discount value combinations. About 500 questionnaires in Italy and 120 in Poland were collected, which is a quite large number, if one considers that any respondent returned 7 observations (assessed scenarios), large enough to run the following econometric estimates. Anyway the reliability and precision of the benefit estimate would increase by adopting more sophisticated sampling techniques. Finally, to obtain the value of the damage caused by the interruption it is then necessary to use these data as an input for a model, where the probability of choosing a given blackout scenario (and therefore the associated utility for the respondent) is a function of the blackout characteristics, of the respondent and household characteristics and of the country of residence. The estimated parameters can be used to predict the value of the utility lost with the interruption.

### 3. DESCRIPTION OF THE CASE STUDIES

In this section a picture of the case studies is done including a **summary of the most important and public information** of them, elaborated in “*Deliverable 4: Italian Case Study*” and “*Deliverable 5: Polish Case Study*” of Essence project. This description contains a **short explanation of the scenarios studied**, a **general overview of the situations** in terms of power system numbers and narrative of the potential events, and **the countermeasures applied** for each case. A set of common characteristics will be listed in the introductory part of the section before entering in this description.

The Essence project targeted the global assessment in the analysis for the cost effective implementation of emerging standards in the control systems of a very special infrastructure, the power network. The level of automation on this infrastructure is considered very high due not only to the physical properties of the electricity but also to the necessities of the electric market and the linked business. The electricity supply (considering the whole power value chain) and this business support many economy sectors contributing significantly to the gross domestic product in all developed countries.

The implemented cases draw a number of parallel scenarios including a certain number of common characteristics. In the analysis, for both cases, **how the implementation of different measures could impact in costs has been compared with the calculation of the consequences derived from the alternative impact of having a blackout in the power network considered.**

As it is commented in section 2.1.1, the two case studies conducted the analysis in different type of facilities, with different ITC systems to control it; however, **they have in common the analysis of more than one attack scenario** as it will be explained during the present section: two for the generation facility in Italy, and three different kind of attacks to access substations with several consequences depending on the level of the intrusion in the communication and control systems. This point would allow future assessments to include multiple evaluations in the implementation of measures. This multiple evaluations in the implementation of measures means that the future assessments could be performed considering two different approaches. On the one hand considering the implementation of a standard or part of a standard (countermeasure with specific cost) could prevent against one or various threats (different events to face), and on the other hand that the implementation of several actions (countermeasures) could be overlapped to prevent a single threat (one type of event).

The goodness of the power network functioning could be measured using different performance indicators such as Average Interruption Frequency Index (SAIFI), percentage of capacity used in a circuit or the non-served energy. In both case studies **the targeted indicator to estimate the cost of the impact in case that an attack would have success is the non-served energy.** This meter let the analyst to cross-match the direct effect on the power network and macro-economic data to estimate this impact.

**The area involved** in both cases is **regionally wide-ranging.** The extension reached by the potential threat encompassed in the case studies would affect to more than one million of people (in each case) and there would be direct impact in the daily economic activities of industry and service sectors in a large scale. This point supports the usage of macroeconomic information for industrial and services activities and macro social figures for households developed in other similar studies.

**Summarizing, the mutual features of the two case studies are:**

- + **The method for calculating the impact derived from the implementation of common standards.**
- + **The analysis of more than one attack scenario.**
- + **The selection of a common performance indicator to estimate the cost of the impact in case that an attack would have success is the non-served energy.**
- + **The size of the area involved.**

### 3.1 Italian case study

#### 3.1.1 Studied scenarios

In the case of Italy, two possible scenarios have been considered:

- An attack using a malware able to replicate itself on the infected network. The malware would affect randomly processes running on the operative system, making impossible to control operations in course. It would be impossible to receive or delivery commands or malware would modify the behaviour of components of the SCADA system. Attacks can be produced after the connection of a mass storage device (such as an USB pen-drive or optical disk), or by opening an infected attachment received by a trusted email.
- An attack aimed at saturating the network traffic, hindering data exchange between field and operators. This way, controllers would be shown old information which cannot be updated, and so they would lose control of installations. It can be produced by using the packet amplification attack, such as a smurf attack or a fraggle attack. Smurf attacks produce a big amount of ICMP Echo Requests traffic to a broadcast address, with each ICMP Echo packet containing the address of the victim. When the packet of requests arrives at the destination network, all hosts on the network send requests to the spoofed address, multiplying the number of requests received by the victim. This makes the victim system become unavailable.

Both attacks would make big effects on the network, but effects as well as duration of the recovery processes would be different.

In case that malicious software affect one or more computers of the control system, it is possible that the attack is propagated to the network, generating a DoS on the network, making it collapse.

On the other hand, an attack which could saturate the network traffic would make this system unavailable for users. Operators would suffer important delays in the reception of updated data, with digital readings totally frozen. Thus, it would be impossible to monitor plants, or ensure its correct operation. If the situation is recognized to be critical, the emergency procedures can be started, and the operator should push the emergency stop push-button. Besides, these plants have automatic safety mechanisms able to automatically stop them. This system is known as the Emergency Shut Down system or ESD system.

The intervention methodology varies depending on which of both attacks are being produced.

Regarding malware attacks, the first action should be to disconnect all computers from the network to avoid infection of other computers connected to it. Then, all computers should be scanned to detect malware in execution, to stop and remove it from the system. Finally, once all computers have been cleaned, they should be reconnected, one by one to the network, making sure the infection is not produced again.

If an antivirus is already installed on the computer, and it is able to remove the infection from each computer, the infection could be eliminated in few hours (4-8 hours). On the contrary, if the antivirus is unable to solve the problem, then the time to make the system functional would depend on the number of affected computers, but it can be estimated to be about a few days.

Regarding the DoS scenario, the attack would affect only few computers, and then they can be isolated and tested to detect abnormal behaviour. Time to re-establish communication can be estimated to be about 6 hours.

Additionally, plants which have been stopped cannot be put into operation immediately, because it is necessary to warm them up before restart. Time to restart plants will vary between 1 and 6 hours in the case of a malware attack and 1-2 hours in the case of a DoS attack. Thus, total recovery time for both studied scenarios would vary between 12-56 hours regarding the malware attack, and 6-10 hours in the example of a DoS.

### 3.1.2 Case study

If power generation is not immediately recovered, load shedding procedures would be applied to balance the unavailable power. These procedures create a priority list, i.e. a list ordering power consumers according to their needs for electricity, and the effect of a cut of supply: pumping water, large industries (some of them can be subjected to load shedding), small and medium industries and households. If the power is not restored, blackouts take place.

Finally, the selected Scenario to study has been the one that makes the biggest effect: a complete blackout. The attack is supposed to happen at mid-morning of a working Wednesday, when the total load on the region grid is about 3.000 MW. After the blackout, two generation plants are started to restore voltage and frequency. In 1 to 3 hours, other plants can be recovered. After 3 hours, the power is recovered, along with the link between the island and mainland (but no power is exchanged). Then the production units are synchronised with the mainland, making it possible to exchange power.

To evaluate the socio-economic impact of the cyber-attack on the region, the daily load profiles in the region in a normal day and in the case of a blackout have been compared. In the day chosen to carry out the study by hypothesis it takes place the maintenance of the connection cable between this region and the rest of the system. The attack is supposed to take place at 10:00 am.

The load profile of the chosen day, detailed to the quarter of an hour was obtained by recorded statistics. Power consumption, per quarter of hour, for all sectors has been obtained. Then, the estimation of the amount of electricity used by each economic sector has been carried out, taking into account yearly consumption for these sectors.

For the case of the attack, the hourly load profile for all sectors has been estimated. To do this, the amount of power available for use, has been considered. In the first 15 minutes, there is no power available. Electricity recovered is used by the major cities. After 1 hour and 15 minutes, there are 120 MW available to use by these cities. After 3 hours and 15 minutes, there are 600 MW, used by residential and services sectors in

these cities. Considering that by then the connection with mainland will have been restored, it can be assumed that, after 3 hours and 30 minutes, some industrial activities can use electricity. Finally, after 6 hours, the electricity supply is totally restored.

### 3.1.3 Countermeasures

Countermeasures should ensure that the plant can stand a cyber-attack and that the supply is ensured. They are focused specially on ICT components, which are used to ensure monitoring and control, and depend on some characteristics of the installed system.

Some countermeasures to ensure that communication using both wired and wireless links are secure are:

- Strict configuration of network access points;
- Use of dedicated, cabled links for safety-related functions;
- If applicable, setup of IDS/IPS to detect attacks and for alarming via alternative channels;
- Redundant connection of components, using different protocols or communication routes.

Security architecture is based on the segmentation of the Control System Network, dividing the system into security zones and creating layers of protection which isolate the most critical parts of the system. Access to security layers must begin in the least trusted and go to the most trusted, and connections must be implemented only between secure interconnections. Besides, all resources in a security zone must have the same minimum level of trust, and if not, additional security measures must be taken.

In the case studied, the system must be divided into security zones, according to its functionality, its criticality and its physical location. All resources within a security zone must have a minimum level of security, and to achieve this, the following measures can be taken:

- Each trusted zone should be kept small and independent, and be administered from the inside.
- Physically protect all equipment.
- Disable all unnecessary network connections, services, file share methods.
- Ensure that all connections between a trusted network zone and other networks are secure.
- Use strong passwords, and change them regularly, to ensure that only authorized users can log on to the system.
- Update authorized users, user groups, and access rights, ensuring that they are according to the current responsibilities of all individuals and current authorities.
- Do not use the system for e-mail, Internet browsing or other functions do not related to the main function.
- Avoid installation of unauthorized software.
- Use virus scanner on all system nodes.
- Restrict or disable connection of portable computers, USB memory flicks and other removable data carriers.
- If CDs, DVDs, USB memory sticks or other removable data carriers are used, they should be checked for viruses before using.
- Monitor the system to detect intrusion attempts.
- Use antivirus software, and keep it updated.

- Create plans for incident response, including recovery plans.
- Currently and periodically review compliance of the organization, systems and installations with security policies, procedures and practices.

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

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

### 3.2 Polish case study

#### 3.2.1 Studied scenarios

For the case of Poland, the case study considers a serious disturbance on the 3 substations owned by PSE Transmission Operator, which can lead to an outage in the a given area. Substations are very vulnerable to cyber-attacks, and risks of these attacks are high.

Attacks can be produced when an attacker is able to access substations, using a malicious code, invalid commands or achieve to control ICT systems. Access can be achieved by:

- Attacking local or remote ICT systems (using public access or the central SCADA system, which provides access to multiple objectives).
- Independently attacking local ICT systems on many substations.
- Attacking local ICT system on one substation, and then penetrating next substations or intermediary systems.

Effects of attacks depend on the level of the intrusion:

- Level 0- Intrusion affects a single device. This attack makes effects only on the part of the system affected. If the attacked device is not a component of control substation, the only consequence can be data theft.
- Level 1- The attacker can drive a single system for a power system. This attack makes the same effects that a Level-0 attack.
- Level 2- The attacker can communicate to most systems, but maximum effects will be no bigger than a Level-0 attack.



- Level 3- The attacker takes control of all electric power facilities, by attacking the central SCADA system.

Attacks on level 0-2 makes smaller effects by themselves, however, they can provide access to other objects and final results can be similar to a level 3 attack.

Some factors which can increase the likelihood of an attack are:

- Use of devices from a single manufacturer for many power facilities.
- Use of the same contractor, or the same group of contractors for servicing and maintenance.
- Lack of security monitoring tools in substations, or unsecure communication tools.

The first two vulnerabilities can be profited by external service providers, or attackers who have infected software used by contractors. External service providers can transfer infection to many objects, as they have to work with many of them.

The third vulnerability can provide the attacker with access to central SCADA or to other power facilities.

Besides, the three attacks can be carried out by a person who normally is allowed to access the system, such as disappointed employees.

### 3.2.2 *Simulation of attacks*

To simulate an attack and estimate its effect on the electric system, the following assumptions were adopted:

- All communication levels between systems of TSO were studied, looking for vulnerabilities in different systems, which could be used as method of attack.
- Attackers are supposed to have time enough and expertise to look for vulnerabilities, unless appropriate security measures are taken.
- If communication between different systems or objects is discovered, attacks could be spread on other levels of the network.

Besides, a list of countermeasures to detect and interrupt attacks was studied, taking into account:

- Maturity of the EU and Polish law.
- Reduction of the likelihood of a remote attack.
- Reduction of the likelihood of a local attack.
- Increase in the likelihood of detection of an attack in the reconnaissance phase.
- Minimize duration of the incident.

Detailed analysis of each of the proposed countermeasures has been carried out, to evaluate vulnerabilities of the system to each level of attack. As a result of the application of protective measures to the Polish Power System, as well as a number of countermeasures implemented in the Central SCADA system and business system, it can be concluded that only attackers with large funds and high knowledge could carry out this attack. A physical attack remains being more feasible and cheaper than a cyber-attack.

To estimate effects of an attack on the Polish Power System, data on the electricity consumer groups in the area affected were collected. As a result of this, the gross domestic product generated by each sector has been estimated.

Thus, effects of an electricity cut depends on the affected sector, the duration of the electricity cut, the period of the year and the moment of the day, as well as the type of day of the week (working day or weekend).

Effects can be divided into direct and indirect. Direct economic impact include the loss of production, spoilage of raw materials or food and equipment damage, while direct social impacts come from lack of electricity at home to lack of transportation.

Indirect impacts include civil disobedience during a blackout, failure of industrial devices, etc.

The studied electricity interruption took place in Warsaw, at 5 p.m., lasting for 6 hours and affecting a variety of customers.

### 3.2.3 Use of standards and proposed countermeasures

Countermeasures are chosen taking into account the N-1 criterion: failure of one single element of the transmission network should not disrupt the network. Thus, only the occurrence of a number of problems should disturb operation.

Countermeasures should avoid the spread of the cyber-attack, minimizing its effect and duration.

Three types of substations have been studied:

- Substations in urban agglomerations.
- Substations discharging power plants.
- Substations of international trade.

Failures in substations which discharge power plants can produce an important loss of power in the system, which cannot be compensated. Then, the National Power System would be divided into areas excluded from power.

Regarding substations in international borders, this situation has been studied in the Polish-German border. A sudden shutdown of such a substation could cut electricity flow from the north to south Germany, threatening electricity stability of the German power system. To avoid these effects, it is necessary to design the system according to the N-1 criterion.

Finally, failure effects have been studied. The area receives electricity only from these substations, so this failure would lead to a total blackout of the city. Countermeasures to take in order to avoid this attack should be focused on:

- Hinder attack propagation, by means of diversification of service providers, use of heterogeneous devices in the transmission network, and ensuring security of the ITC systems (eliminating vulnerabilities, creating firewalls).
- Increase probability of attack detection: construction of intersystem communication nodes and inter-control points, honey pot traps and automatic analysis and correlation of events.
- Minimize duration of failures.

These assumptions can reduce the number of potential cyber attackers to only those with bigger knowledge, budget and time. Only these attackers could break the system without being detected, as if they made mistakes, the monitoring system could detect them. Thus, attackers could choose other methods, like physical attacks.

### 3.3 Open issues and future directions of research

The power sector and the facilities included on its network are under a complicated framework for its operation. A lot of relevant factors, such as **the continuous technological improvements** (at different layers in which information and communication technologies are one of these layers) **linked to the necessity to maintain the operation of old facilities and to establish the coexistence of different levels of performance in the network**, or special regulatory conditions, or the inevitability quality of safety and - what is really important in the Essence approach - “**different levels of security for facilities and equipment which subsist in a common infrastructure**”, accentuate this challenging work.

In addition to this fact, the current activity in **industrial sectors is more dependent from electricity than households or service sectors**. Even if the rational sense invite to think about the similar dependency in the service sector than in the industrial one, the energy intensity on the first one and the chance to continue operating many activities during a blackout is higher and derived from this. **There are also strong and more differentiated evidences on direct damages resulting from blackouts to industrial processes**.

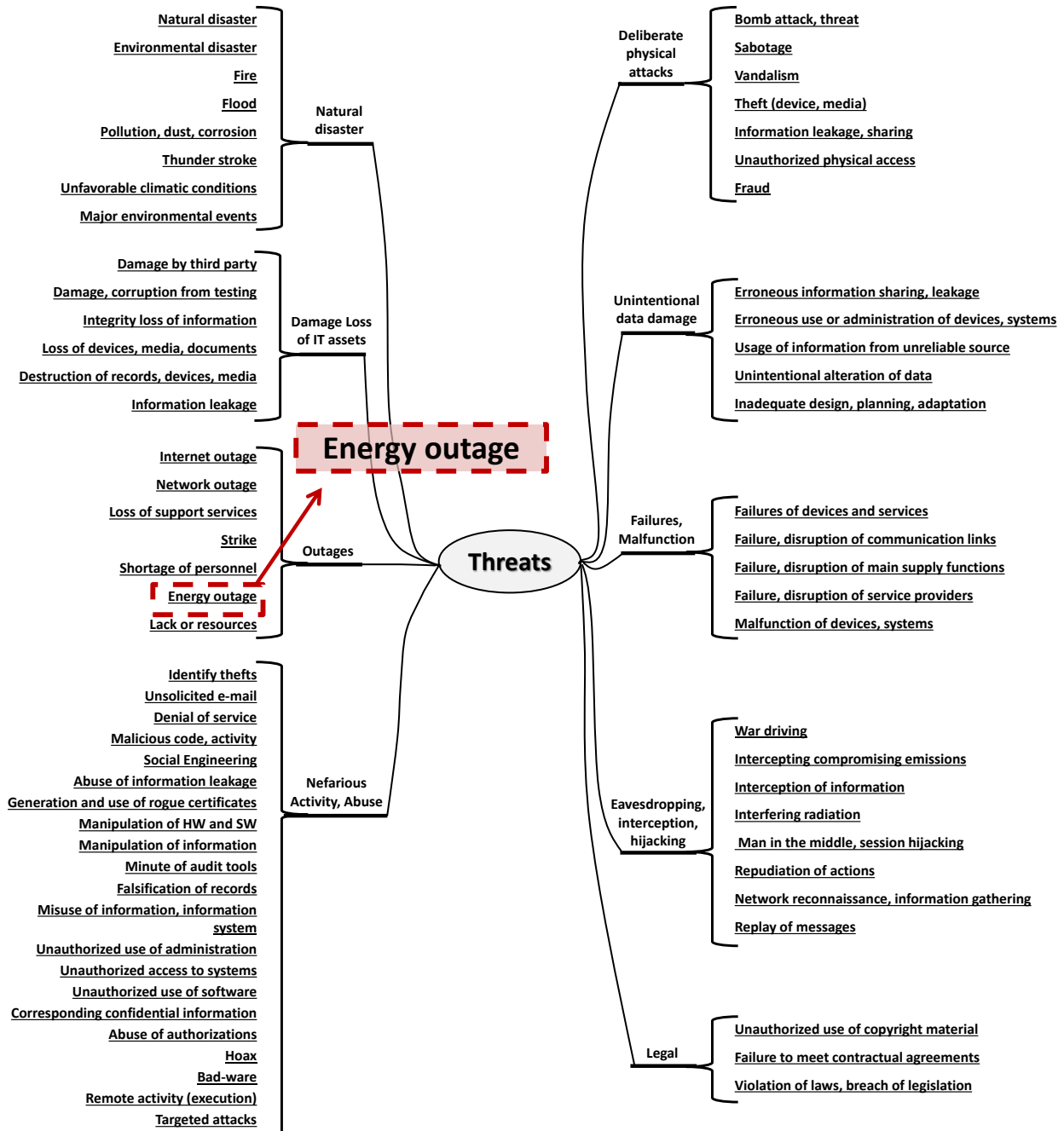
For example, many manufacturing chains have to stop during a blackout, or, uninterruptible power supply (UPS) systems support longer for service sector activities than industrials. In industrial activities, sometimes instead of an UPS, the companies provide factories and manufacturing chains with alternative power supply facilities in order to avoid potential blackouts. A detailed description and use of electricity could be checked in chapter 3 (description and use of electricity) in a deliverable of SESAME project<sup>i</sup>. On this research document, there are a list of tables estimating the qualitative impact of a blackout by type of consumer and sectors. More over some qualitative evidence has also been obtained through some case studies in Essence<sup>ii</sup>. The whole value chain of energy supply and its working operation failures produce events and disruptions in the energy supply. The work done in the case studies could be used again for new analysis in different ways. Two main categories of possible extensions could be considered:

- **Use the results of the Essence project as road map to do similar evaluations in other electricity services or in other critical infrastructures.** For example an important group of facilities whose protection should still be assessed concerns the distribution of electricity. In particular, in this field, the topic of the security of ‘*Smart-grids*’ is attracting a lot of interest, due to the complexity of their operation. The ‘*Smart-grids*’ is the name of the “digital two-way communications between consumers, or even in some cases ‘*prosumers*’<sup>6</sup> of electricity’ and electric power companies sector”. In accordance with many recent publications, there are a list of existing threats for the electricity supply infrastructure as consequence of the development of the new ‘*Smart-grids*’. One of these threats is the loss of energy derived from a potential blackout generated by hackers. In an ENISA<sup>7</sup>’s report<sup>iii</sup> on threats in the area of smart grids and good practice guide - Smart-grid Threat Landscape and Good Practice Guide - is stated that an important threat could be connected to the “Manipulation of information” and that it could have an impact on power supply: “...*False data are injected by an attacker in the smart grid traffic. The attacker injects false or malicious DR events in DRAS (Demand Response Automation Server), causing blackouts and instability of the grid...*”. This is not the only one threat. In Figure 1 there is a picture with the list of all identified threats for a Smart grid infrastructure.

<sup>6</sup> Agent in the electricity market which generates (produces) and consumes electricity

<sup>7</sup> European Union Agency for Network and Information Security

The implementation of the emerging standards, coincident in many cases with the ones used in the Essence case studies, could help to enhance the protection of the whole infrastructure against these existing threats. In the same report published by ENISA, a set of standards as the ones published by NIST or IEEE, are presented as a solution for mitigating the likelihood of the threats. So that, the use of Essence methodology could be considered for similar case studies in the Smart-grid infrastructure.



Source: elaboration based on smart grid threat landscape and good practice guide, enisa

FIGURE 1: OVERVIEW OF THREATS ASSUMED FOR SMART GRID ASSETS.

- The interest in Essence results derives from the absence, as far as we know, of other similar studies, but their reliability and generality could be improved by **making deeper analysis: in more detail, more extension** or in **other regions**, using partially or as a whole the Essence results process to elaborate them. Here is a list of possible examples.

One example of these deeper analysis could be done by studying the behavior of the response in the energy consumption as well as its impact in the one of the economies included in the case studies. In case **project results** could be **updated and improved** by more precise estimates of this impact in the regions, being in a position to better calculate this impact (above all for households, using representative stochastic samples, for example) than in the case studies done.

Other examples of suggested future work could be to use the methodology used in Essence project and the results regarding the socioeconomic impact and benefit analysis (households, industry and services) for **evaluating different threats which could produce comparable impacts in the power network although they do not concern the cyber-protection**. These attacks are not in the scope of the project, nevertheless they could produce similar generalized black-outs and so the same cost-benefit methodology could be applied. Other types of threats include human physical threats, accidental threats or natural threats. A more detailed list can be found in the work developed in the deliverable “D1.1 Analysis of historic outages”<sup>iv</sup> of SESAME project, publicly available on <https://www.sesame-project.eu/publications/deliverables/d1-1-report-on-the-analysis-of-historic-outages/view>. Moreover, the implementation of security standards produces a list of countermeasures to protect the power facilities against different threats. There would be the possibility to use Essence methodology and results for the **evaluation of other countermeasures to enhance power network security**. There is a more detailed list of countermeasures to protect the power facilities in the work developed in the deliverable “D1.4 Incident-response system”<sup>v</sup> of SESAME project, public available on SESAME website <https://www.sesame-project.eu/publications>.

Other possible improvements in the impact evaluation include the enlargement of the geographical dimension. This does not only imply to **do the same analysis considering additional events for a larger region**, but also to build probabilistic samples of private users in different regions, so as to guarantee a certain level of statistical representativeness.

The already **mentioned continuous technological** improvements in the Electricity and ITC sectors (both linked to Industrial Control Systems (ICS) of electricity systems) requires to infrastructure managers to keep on being in the state-of-the-art regarding security issues in these sectors and subsectors. These security issues directly linked to power supply, electricity infrastructures safety or regulation frameworks and standardization, are continuously changing and progressing. These evolutions create the inevitability caution to not forget that Essence research activities have been developed in a particular context, with specific hypothesis, so the future analysis should have to take into account these factors, and test the possibility to transfer the strong results emerging from the case studies and discussed in the following section, to other contexts.

**Summarizing, the OPEN ISSUES and future directions of research beyond Essence project activities and results are:**

- + **Use these results in a similar case study of other part of the value chain of the energy infrastructure or other critical infrastructures**
- + **Elaborate deeper analysis in different ways:**
  - **Updating and improving the project results and producing a more precise cost benefit evaluation.**
  - **Evaluating different threats which could produce comparable impacts in the power network.**
  - **Evaluating other countermeasures to enhance power network security.**
  - **Doing the same analysis considering additional events for a larger region and representative samples of end users.**
- + **Remain innovative in the sectors and subsectors related to Essence research activities: Power supply, Electricity infrastructures safety, ITC Security, regulation frameworks and standardization, etc.**

### 3.4 Summary of trial evaluations: good practices

Since the statement of good practices in the revision in oneself work (Essence consortium defining good practices of the work done) is a rather difficult task, the first step in the sake of objective evaluation, is to gather some information from reputed works in similar or comparable approaches.

The main issue to remark is the establishment of an appropriate framework, data collection and execution of the realistic cases for elaborating an accurate cost-benefit evaluation. Considering that the implementation of emerging standards aims at enhancing security levels in the power infrastructure, it is important to have in mind that benefit of a security measure is a function of three elements:

- The **probability of a successful attack** on the targeted infrastructure(s).
- The **losses** sustained in the successful attack.
- The **reduction in risk when the measure** is applied.

Due to the particular characteristics of the attacks, **the probability of a successful attack on the targeted infrastructure has not been included in the analysis of the project.** The Directive on attacks against Information Systems, which was adopted by the European Council on 22 July 2013, combats cyber-attacks against information systems and includes the creation of a data base repository of cyber-attacks by sector. Despite this, during the project activities, and in particular at the early stages of the project, when the activities were scheduled, the Essence team did not identify public information available. The availability of

**this kind of information on cyber-attacks**, in particular for the power sector and its infrastructures, **could improve the risk analysis, and allow to consider the different probability of the various threats.**

A really good practice carried out during the Essence project was the calculation of the losses sustained in the successful attack for both cases. This quantification for the cases has been made using a comparable scheme with similar characteristics as area affected or timeframe. The results of **losses estimations are comparable and could be considered for contrasting with other evaluations.**

The utilization of security standards for power controls has not been completely drawn on in a prototype built during the project. The security standards were used considering previous principles postulated and observed and a technology formulation was postulated, and this means that some applications have been formulated <sup>8</sup>. **There is the assumption that the implementation of the measures would increase security levels and reduce inherent risk is.** The establishment of metrics for the estimation or risk reduction would improve the qualitative results of the case studies.

A set of good practices for a similar analysis could be found in different specialized bibliography. Some of the reference reports at international level are the “Financial Management Reference” series published by the Department of Finance and Administration of the Australian Government. Under this series two particular publications about the targeted activity can be found: “Introduction to Cost-Benefit Analysis and Alternative Evaluation Methodologies”<sup>vi</sup> and “Handbook of Cost-Benefit Analysis”<sup>vii</sup>. These publications provide guidance in the use of cost-benefit analysis (CBA) for evaluation and decision-making.

This guidance, apart from describing the analysis process, includes the welfares of its application, a set of good practices and possible barriers to proceed with a CBA and some existing alternatives such as the elaboration of a “financial evaluation” or the execution of a “cost-effectiveness analysis”. Summarizing the main rules to proceed with a case, it is important to consider the **efficiency allocation of resources and the performance of the actions** in the process, the **estimation of the opportunity cost**, the identification of **compensations among different actors (to face the problem of costs and benefits not incurred by the same agents)** and the establishment of **an adequate cost benefit rule**. A little further ahead there will be some comments on this.

The efficiency allocation of security investments is linked to the performance of power infrastructure in the provision of an effective energy supply (in this case electricity) to the customers. In the cases of Essence

<sup>8</sup> This could be a complete classification of innovation process steps:

- 1) Idea. Unproven concept, no testing has been performed
- 2) Basic research. Principles postulated and observed but no experimental proof available.
- 3) Technology formulation. Concept and application have been formulated
- 4) Applied research. First laboratory tests completed; proof of concept
- 5) Small scale prototype built in a lab environment (“ugly prototype)
- 6) Large scale prototype tested in intended environment
- 7) Prototype system tested in intended environment close to expected performance
- 8) Demonstration system operating in operational environment at pre-commercial scale
- 9) First commercial industrialisation. Manufacturing issues solved
- 10) Full commercial application, technology available for consumers

ESSENCE works has been on steps 2-3. A complete proof of concept would require to go to step 4.

project, the established situations in attack scenarios (**latent** and **realistic scenarios**) are threats that would not only imply the affection of the power infrastructure and the operation companies, but the disturbing of the electricity market would also affect household and industrial sectors.

The opportunity cost of the unsupplied energy in the cases in Essence project involves energy customers, however the cost of implementing the emerging standards for the facilities is always supposed to be supported by the company owner of the facility affected. The impact of the cost of implementing measures directly upsets the utility in the Italian case study and the power network manager for the Polish one. In a CBA it is important to compare costs and benefits, but for the scope of Essence, and of the regulator as well, it is **also essential to identify which actors support costs and which ones receive benefits**.

**One missing point in the scope of the project the establishment of a set of rules to apply an adequate cost benefit analysis.** The results show that there is a cost associated to the threat in the hypothesis of success of the attack to the different facilities, which faces the cost to improve the security on them. For example, the elaboration of an analysis like in the paper “Balancing the Risks, Benefits, and Costs of Homeland Security”<sup>viii</sup> elaborated by Homeland Security Affairs of U.S.A. provided more accurate results through the benefit generated by enhanced security measures if they have been able to prevent or protect against an otherwise successful attack for a range of losses from a successful attack and for a range of annual attack probabilities.

Another key reference, specific for the purpose of establishing an evaluation criterion of Essence work, is the “Methodology for Conducting Cost Benefit Analysis To Support Energy Security Investments”<sup>ix</sup> prepared by the, Department of Systems Engineering United States Military Academy in January of 2013. In this report it was explained the method **to conduct an evaluation case of the implementation of measures to improve the resilience of energy supply** in a Military environment. In accordance with this method, the evaluation needs to include eight different most important steps:

- 1. Define the problem / opportunity to include background and circumstances,*
- 2. Define the scope and formulate facts and assumptions,*
- 3. Define and document alternatives (including the status quo if relevant),*
- 4. Develop cost estimates for each alternative (including status quo if relevant),*
- 5. Identify quantifiable and difficult to quantify benefits,*
- 6. Define alternative selection criteria,*
- 7. Compare alternatives, and*
- 8. Report results and recommendations.*



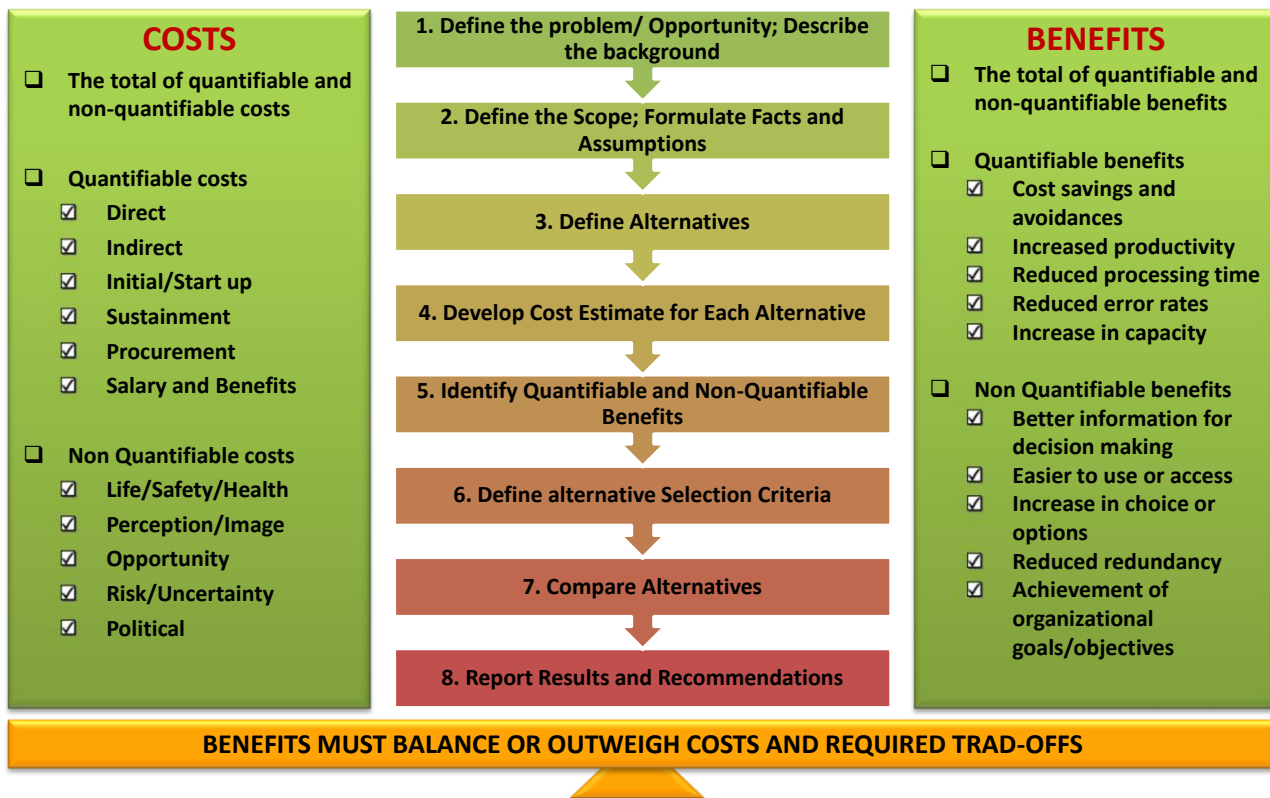


FIGURE 2: THE COST BENEFIT ANALYSIS PROCESS ACCORDING TO DEPARTMENT OF SYSTEMS ENGINEERING UNITED STATES

Among others, the work carried out during the project and the subsequent results contributed to evaluate costs and benefits of the implementation of ICT emerging standards as security measures in the field of energy to improve more reliable supply and provide a number of conceivable regulatory options. These cases could be used to exemplify (not justify by alone) actions such as raising the levy on the use of electricity or implementing changes in the regulation of electricity networks. The key question dealt with in these cases is whether and how investors responsible and policy makers should be involved in taking measures regarding security of energy supply.

The option standards implementation in different facilities for the electric infrastructure, to increase the security of electricity supply comprises several types of governmental action, including subsidies, regulation and government investments. From an economic point of view, therefore, it would be often wiser to accept consequences of supply disruptions than to pursue security of supply at any cost. This implies that players involved in the power sector investments should exercise caution in imposing measures regarding security of supply.

In addition to the ones described in the present section, any of the open issues and future ways for continuing the Essence project works, addressed in the section “3.3 Open issues and future directions of research”, applied to incoming works could be considered as “best practices” for future case studies. Many of the points raised on that section would provide better sample reliability or wider analysis of indirect costs. The enlargement of the case studies to a European view could be a driver to obtain a generalization of the results.

Some of the good (and 'not good') practices identified during Essence project activities could be summarized as follow:

- The probability of a successful attack on the targeted infrastructure has not been included in the analysis so, to improve the project results it would be interesting to collect cyber-attacks information for power sector and its infrastructures to estimate their likelihood.
- + The damages caused by blackouts in the case studies are comparable and could be considered for comparison with other evaluations.
- The improvement of resilience levels in the facilities with utilization of security standards for power controls has not been completely contrasted during the project with the implementation of a prototype. There is the assumption that the implementation of the measures would increase security levels and the reduction in risk is inherent.
- + Despite there is no explicit implementation of security standards utilization, Essence project adopted latent and realistic scenarios.
- + The identification of the actors who will incur in costs and enjoy the benefits of the investments, which is a consequence of Essence results, provides added value to the work.
- The enlargement of the case studies to a European view could be a driver to obtain a generalization of the results.

#### 4. CONCLUSIONS OF THE EVALUATION (SUMMARY OF FINDINGS)

##### 4.1 Key findings from the case studies

##### 4.1.1 Vulnerabilities and countermeasures

Industrial Control Systems (ICS) of electricity systems show important vulnerabilities, which have to be analysed on a case by case base, because they may differ a lot not only with reference to the specialization of the firm (TSO, DSO or generation) but also to the peculiar situation of any plant (connections, geographical features, state of the infrastructure, etc.).

These vulnerabilities can be exploited by attacks that may lead to sudden shutdown of some power generation plants and substations of the transmission grid. In most cases the system is resilient and can manage the situation without any external help but, in special cases the effect may be more disruptive. In both Essence case-studies a situation was detected where an attack could lead to a blackout lasting six hours, although with different recovery profiles. Hence there are situations (for example. multiple attacks, or attacks to special places and/or when the transmission grid is somewhat 'weak') in which these attacks may lead to significant blackouts that may involve millions inhabitants, inhibit large shares of productive activities and

last several hours. This underlines the importance of guaranteeing the security of all relevant nodes and not only the interconnection grid.

Countermeasures exist that can reduce the probability of success of such attacks (or, in other words, raise the cost of a successful attack), although they do not eliminate completely the risk. The defensive strategy must take into account different needs, implementing and maintaining countermeasures to minimize remote attacks; to minimize the effects of a local attack, to prevent the propagation and escalation of an attack and, finally to shorten the duration of the effects of a cyber-attack. Acting on all four levels will guarantee the maximum effectiveness (highest level of protection) and at the same time will improve efficiency, since scale economies are possible and so the global investment required is lower.

These countermeasures may be retrieved in more than one standard, so it may be said that all standards address in a way or in another the main threats. Nevertheless the choice between standards is not so straightforward, since there is not perfect congruence between standards, and because standards that seem more adequate for GenCos are not the same that fit TSOs. Since recertification is very expensive, a clear European regulation or agreed guidelines are of the utmost importance.

#### 4.1.2 Costs and benefits of standard implementation

The 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.

Results quantify the cash flows for the implementation (investment costs) and maintenance (annual operational costs) of the security standards. In both cases two situations have been considered: costs that should be borne if no security standards had been implemented yet (no protection case) and costs that should be borne starting from the current situation in order to manage a higher supplementary security (delta cost).

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 the 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 done, so that it would be quickly possible to 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.

As argued above (see §1.2) failures caused by cyber-attacks may take 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 benefit analysis is focused on the form having the largest consequences. The simulation showed in fact that in both case studies an attack born in conditions of vulnerability 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 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 (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 (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 “typical family”.

The results raising from the two case studies and by the cost analysis and the benefit analysis run on them are summarized in Table 4.

TABLE 4: 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	Maintaining	3.5-6	6.5-12.9
Households*	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	Maintaining	2.5	5
Households*	30-52-61			
TOTAL	55.7-96.7			

\*Min-Expected-Max

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<sup>9</sup> because they are supposed to suffer the most from the lack of electricity. But even if a lot of attention has been put during the survey to get the consumer involved in the problem of security of supply, nowadays reliability is often taken for granted and

<sup>9</sup> The Italian case study shows the priority given in the recovery plan: first residential users in big towns, then residential + tertiary in towns, then industrial customers, finally agriculture and rural users.

so the estimated value of the blackout is still under-evaluated. This perception would probably change a lot after a large blackout is experienced. Also electricity utilities suffer from the blackout, 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, but they have not been considered, because these indenisations (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 to 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 nowadays impossible to estimate precisely 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 not able to block or mitigate an attack and their consequences are diffused and well echoed on media. This would in fact prove the feasibility of the attack and, above all, the visibility effect it carries with, which is mostly important for cyber-terrorists, unchaining an imitation effect leading to an escalation of attacks.

## 4.2 *The legacy of Essence: policy suggestions and open issues*

Essence conclusions give sound evidence to some perception and so they allow us to fix some important points in the discussion. But this is only the beginning of a process, and many question marks are still awaiting an answer. In particular the Essence approach, described in the introduction of this report, allows us to consider the estimates showed above as grounded in the reality, but this has gone to the detriment of the generality of results. This is why we are not ashamed of declaring that all our main conclusions call for further work for the sake of generality. The following paragraphs discuss then the main results emerging from the Essence case study, in the perspective of passing from specific results to an European view, and then from European evidence to regulation.

### 4.2.1 *Countermeasure actual implementation*

The case studies have shown that some of the countermeasures necessary to block cyber-attacks and to comply with security standards have already been adopted, so reducing sharply the cost of standard compliance for the two operators. But the perception is that the present situation in European countries is uneven. For this reason, it would be important to understand which is the current situation among other European utilities, and which are the investments already planned for the next future are, also showing the country specificities in the implementation process.

This evidence is strongly necessary before thinking about any form of regulation. Simply imposing a standard won't be easy. Defence is not a sector in which national governments are keen to accept common regulation. But, although threats to security are often felt as a national competency, not all member states have the financial and technical capabilities to comply in a consistent way with security requirements and

probably even fewer governments are able to identify and adopt a country specific strategy which could better fit the country specificities.

The cost analysis also shows that the implementation process is more advanced in the case of the Polish TSO, in particular regarding investments; in fact while about half of the countermeasures concerning the governance of security (maintenance costs) have already been implemented in both cases, the Polish TSO has already incurred in 71% of the investment required for standard compliance, as opposed to the Italian case study, where it has been estimated that only something in-between 25%-29% of the required investment has been carried out. This is absolutely not a surprising result. There is in fact a more diffused perception of the grid as a critical infrastructure; as TSOs are public firms (or publicly controlled firms) with a strong commitment to quality of service, which includes reliability of supply. It is hardly imaginable that a grid operator asking to the body that controls it to invest to guarantee more security, would not be funded.

On the other hand, generation companies act in a competition regime and will carry on just investments able to guarantee adequate returns. Our example showed clearly that the investment to implement security standards would not be the case, since the avoided damage in case of a big blackout for the generation firms is just a very small share of the security cost<sup>10</sup>. Moreover it must be considered that the engineering features of the electricity system, in particular the need for matching demand with supply in real time, imply that the global security level equals the one of the weakest node. For this reason, in a competitive market structure, no competitor is stimulated to invest on a voluntary basis, before that a common standard is established, and all firms are asked to comply with common minimal requirements.

#### 4.2.2 *The choice among standards*

As it was already expected from the survey of existing or forthcoming standards, the work on the case-studies let some insights emerge but didn't allow to clearly indicate one - or two - most suitable standards. The detailed analysis showed that the main standards address the most important threats with rather similar countermeasures, but the technical requirements to devices may differ and the threats are not the same for the different operators.

So the question whether to choose one single standard, or to set up different standards for the different parts of the electricity system, or if it is better to rely on more generic guidelines making each operator free in the choice of one standard is still an open issue. The final decision, which in our opinion is in charge of a supranational body, should be preceded by a long process, with a mission of reconnaissance of the strategies implemented up to now by single operators and of the specificities of the different needs, followed by a consultation phase, able to lead to a more generalized agreement. For example ENTSO-E (European Network of Transmission System Operators for Electricity) and its Technical Group on Critical System Protection which is also in charge of cyber security measures has already undertaken this process. Its twelve members are developing a common strategy which includes an information exchange platform - based on a private network - concerning threats and key mitigation strategies. A self-assessment survey among members took place last year and was the base to create a technical manual concerning Cyber Security and a tool to increase Cyber Security in three stages. Since firms are already investing in security, although at different

---

<sup>10</sup> In the Italian simulation, although the total damage for the energy sector has been estimated equal to 1.3 M€ (which is a very small fraction of the total damage), the loss for generators amounts only to 0.6 M€.

extent as argued in §4.1.2, companies should also be helped to understand the inverse perspective, i.e. whether investment done before standardization will be useful for future compliance. In particular, is the countermeasure that a firm eventually adopts to comply with one special standard, useful in order to comply with other standards that would eventually be chosen later? How to assess, once a system is certified under Standard X, what more is needed to certify it under Standard Y? And how much will it cost? Recertification is generally very expensive and is one of the explanations of the reluctance of firms to invest in the pre-regulation phase. This cost would be reduced, or nullified, in case an organization with high reputation could build official mapping tables between different standards. This detailed congruence analysis will be then a relevant direction of future research.

#### 4.2.3 Policy and regulation issues

Estimated benefits largely exceed costs of implementation, even in the case of no existing investment. This is true even considering that our estimate of the damage caused by a blackout is a lower bound and it considers one single event (on the other hand multiple attacks are to be expected after the first one, because of increased visibility and of demonstrated feasibility).

But the benefits are shared among different groups: the firms operating in the territory struck by the blackout and the society as a whole, and only a small part concerns the electricity utilities.

From a profitability viewpoint, electric companies have no incentive to increase their security levels, as the cost of protections is much greater than the direct cost of a single blackout they should eventually suffer from. This explains their reluctance to afford such huge investments. Public regulation and support to firms operating in competitive branches of the energy sector is clearly necessary. Electricity supply security is a very important feature of the electric service, since our lives and economic activities have become more and more dependent on this commodity. This is related to the fact that supply security is a non-tradable public good, i.e. one of the causes of market failure. Public goods share the properties of *non-rivalry* and *non-exclusivity* in consumption. *Non-rivalry* means that one individual consuming that good does not limit its use by other people. *Non-exclusivity* indicates that individuals cannot be excluded from consumption, in fact individuals could not choose to buy electricity plus security, or just electricity. For these characteristics, public goods are *non-tradable*, and firms tend to invest too little on them, nothing if they acted on a purely profit perspective. Market failures may be faced in different ways, such as public supply (as in the case of defence), regulation or support to private firms. All these options are interesting in the case of the security of the electricity system. So how to combine the possible options is another important open issue to be addressed by future research work and by consultations to the relevant stakeholders, after a reconnaissance of the tools that already exist in the present institutional framework at the national and EU level.

This issue opens another relevant point that should be discussed in the following times: which is the best authority to be in charge of the regulation framework? And who should decide how to manage the support for standard compliance? While working on the process that will lead to security regulation, one of the topics to be decided is which parts of the governance are to be kept at the European level, and which shall be delegated to national authorities. The possible alternative implementation scenarios shall be assessed, without losing the contact with the concrete local situation and market assets.

## 5. REFERENCES

- Bruno C. *et al.*, (2014) “Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case studies”, RT Ceris N. 52.
- Department of Finance and Administration, Financial Management Group (2006) “Introduction to Cost-Benefit Analysis and Alternative Evaluation Methodologies”, Financial management reference material N.5 .
- Department of Finance and Administration, Financial Management Group (2006) “Handbook of Cost-Benefit Analysis”, Financial management reference material N.6 .
- Farr J. V. and. Praker C.M (2013) “Methodology for Conducting Cost Benefit Analysis To Support Energy Security Investments”, Department of Systems Engineering United States Military Academy.
- Marinos L. (2013) “Smart Grid Threat Landscape and Good Practice Guide”, ENISA.
- Mueller J. and Stewart M.G. (2011) *Balancing the Risks, Benefits, and Costs of Homeland Security*.
- Reichl J., Schmidthaler M., García F. and others (2013) “SESAME (Securing the European Electricity Supply Against Malicious and accidental thrEats) Project D2.2 public effects knowledge base”.
- SESAME (2013) *Report on the analysis of historic outages*, Securing the European Electricity Supply Against Malicious and accidental thrEats.
- SESAME (2013) *System Specification of Decision Support System*, Securing the European Electricity Supply Against Malicious and accidental thrEats.