Elena Ragazzi[1] and Alberto Stefanini[2]

1. *Corresponding author* elena.ragazzi@ircres.cnr.it CNR-Ircres, Via Real Collegio 30, 10024 Moncalieri (TO), Italy. Tel. +390116824930. Fax +390116824966
2. Novareckon Srl. Via Tagliamento, 4 – 43036 Fidenza (PR) Italy, +39.347.3640214 *alberto_stefanini@virgilio.it*,

Are security standards for electricity infrastructure a good choice for Europe?

Evidence on cost and benefits from two case studies

Article submitted to the **International Journal of Critical Infrastructures** https://www.inderscience.com/jhome.php?jcode=ijcis *Pre-print (Author's original manuscript prior to peer review)*

We gratefully acknowledge that most of the work presented in chapters 4-7 was achieved under funding by the 2011 CIPS Programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" within the ESSENCE Project. Partners of the project were ABB SpA – Power System division (Italy), ADC Consulting Slne (Spain), CNR-Ceris (Italy), Deloitte Advisory SL (Spain), Enel Ingegneria e Innovazione SpA (Italy), IEN (Poland), PSE Operator SA (Poland), Università del Piemonte Orientale (Italy). All detailed project reports and supplementary documents may be found at *http://essence.ceris.cnr.it/*

Abstract

Electricity system controls are vulnerable to cyber-attacks that can seriously impact and even inhibit their operation. Such attacks may affect large portions of the power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber-security of control and communication systems is now strong worldwide. Several cyber-security frameworks have been developed, but it is rather difficult to anticipate costs and benefits of their adoption, and this hampers their generalized adoption.

This paper focuses on the conclusions emerging from the outcome of two case studies performed in order to evaluate these costs and benefits on a rational base. The likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities, and the costs of standard adoption are estimated on an objective basis.

Keywords

Security standards, electricity systems, cybersecurity, cost-benefit analysis, security policies

The Authors

Elena Ragazzi, born in Torino in 1964 is since 1989 a researcher in applied economics at CNR-Ircres, an institute of the Italian National Research council specialized in industrial studies, in innovation economics, policy evaluation. Her research interests concern the study of regulated industries, above all the electricity sector, and policy evaluation. She has been the project manager of several European and national projects, with strong multidisciplinary approach.

Alberto Stefanini, born in Padua 1949, received a full honours degree in Electronic Engineering from the University of Bologna, 1974. He is currently retired and holds a consultancy. Since Oct. 2012, he is a partner of Novareckon knowledge brokers (www.novareckon.it), a company to develop entrepreneurial and social ideas through best findings from European applied research, multidisciplinary knowledge systems and an international consulting network. Until Nov. 2009, he was with the Joint Research Centre, Institute for the Protection & Security of the Citizen, where he was involved in studies on critical infrastructure protection, with specific focus on the power system. He has been very active with the European framework programme since the early seventies, and contributed to launch a large number of European projects in the energy and the IT sector.

Although the paper has been jointly conceived and its contents agreed among the authors, sections 1 to 3 may be attributed to Alberto Stefanini and sections 4-6 to Elena Ragazzi. The conclusive chapter 7 was jointly elaborated.

1. Introduction

Since many years, power system controls are vulnerable to cyber-attacks that can seriously impact on their operation. Such attacks may 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 strong worldwide and keeps increasing. Several cyber-security frameworks have been developed or are under development at present, both in form of guidelines and proper standards, but it is rather difficult to anticipate costs and benefits of their adoption, and this hampers their generalized adoption. The US experience so far showed that applying a standard is cumbersome and costly while benefits are not fully clear to all the stakeholders involved [1, pp. 2, passim] and their perceived utility depends a lot on the political mood of the period, how much this experience could be transferred in Europe is unclear as well. The electricity infrastructure is generally more robust in Europe [2] [3], although the public opinion has a lower appreciation of security and defence countermeasures (ref. [3, pp. iii, Tab. 1] shows that SAIDI, the system average interruption duration index is 10 times higher in the US than in Germany and about 3 times than UK).

The cyber-security in power grids has peculiar features. Power grids are complex systems, made up of many components whose complex interactions are not effectively computable: under one perspective, it may be regarded as a self-organized critical system, a system that perpetually steers itself toward a dynamic equilibrium, where small perturbations have long-range effects [4]. At a macroscopic level, the overall system is always in the transient state from one equilibrium to another, and its dynamic behaviour is governed by its intrinsic properties: under specific conditions, it may enter a critical state: the main purpose of its controls is to avoid such conditions. The system is non-linear and because of the difficulty of solving non-linear problems, power system controls used to linearize the problem based on some assumptions. These assumptions may lead to loss of important information. Because of that, and to be more realistic, most modern approaches tend to use nonlinear theory (bifurcation and chaos) to establish real nonlinear models [5].

Another dimension of complexity (and potential vulnerability) in power system is multi-jurisdictionally: stakeholders play different roles (e.g. regulators, owners and operators). They have jurisdictional limits. They may be competitors or have different sizes and consequently different attitudes towards cyber risk management [6]. All this inevitably leads to different attitudes and standpoints which reflect into different security concepts and languages [7].

Finally, cyber threats are elusive: although power systems are in ‘A clear and present danger’ [8], the way the cyber menace materializes, the type of attack, their frequency and intensity can hardly be forecast, and only in the short term. All the above are drivers for the adoption of a common approach to cyber security in the power sector, possibly based on a shared cyber security framework.

This paper is based on results deriving from a study performed over 2012-2014 to evaluate the costs and benefits for the adoption of a shared approach to cyber security on a rational base, including the development of a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts, the identification of the main power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities. Finally the main emergent frameworks for ensuring industrial control systems security where identified so as to establish the costs of their adoption on an objective basis. We will

focus on the conclusions emerging from the outcome of two case-studies, concerning a broad portion of the Italian power generation capability (involving one large Italian Region) and the Polish Transmission System. Both confirmed that cyber-attacks able to exploit current vulnerabilities of the two systems could turn into large and extended blackouts. Based on current and prospected security standards, the project identified the key organizational and technical countermeasures needed to increase the security level of the involved infrastructures so as to neutralize possible attacks. Although these do not totally eliminate existing vulnerabilities, they make the occurrence of serious events much less likely. The analysis estimates the cost that a country should deal with in the adoption of security standards in the transmission and generation of electricity.

The adopted methodology quantifies the cash flows for the implementation and maintenance of the security standards. The total costs involved were evaluated, as well as the ones to be borne by the operators starting from the current situation so as to comply with the standards requirements. These are compared with the cost of a black-out due to a cyber-attack. Ad hoc methods were used to estimate the impact for utilities, households and the economy on the whole. With reference to the Italian case, the total damage for industry and business ranges from 35 to 46 € millions; between 36 and 64 € millions for the residential segment, while the damage for the operating company due to non-sold energy is about 2 € millions. A similar range of values resulted from the Polish trial.

Our paper firstly overviews the rationale and the main concepts concerning the current and emerging standards, then the case studies scope and the methodology used to evaluate costs and benefits of standard adoption are presented. Finally, the outcome of the case studies and their policy implications are discussed.

2. Key concepts and history of relevant standards

The main features and common basic principles of security standards can be better understood having a quick look on their history. The ISO 27000 series [9] is a growing family of ISO/IEC Information Security Management Systems standards that took form in the early ’90, when the British standard BS 7799 was devised. The core principles of information security were recognized to be:

- Confidentiality, i.e. how to prevent the disclosure of information to unauthorized individuals or systems;
- Integrity, meaning that data cannot be modified undetectably;
- Availability, the property ensuring that information is available when it is needed.

These principles inform a set of Common Criteria which were elaborated to ensure that the process of specification, implementation and evaluation of a computer security product is conducted in a rigorous and standard manner. The Common Criteria were stated by the ISO/IEC 15408, an international standard for computer security certification, in three parts, issued in 2009 and last revised in 2015 [10].

The widespread use of Internet for communication within online decision support, monitoring and control for industrial and business systems and processes - included key infrastructures such as electricity, oil, gas and water networks and the financial and banking networks and systems - made those systems vulnerable to computer viruses and hacking. This was officially recognised first by the Presidential Directive PDD-63 [11] emanated under Bill Clinton’s presidency in May 1998 and was sustained by the spread of malicious attacks to critical infrastructures over the last decade.

The security of ICSs (Industrial Control Systems) has a specific feature, because security controls must be compatible with the real-time requirements of ICSs. Since the late nineties many industrial organisations, like the API (American Petroleum Institute), the NERC (North American Electricity Reliability Council), the

VGB (Vereinigung der Großkesselbesitzer- the European association of large power utility operators) and the WIB (the International Instrument Users' Association) issued cyber security guidelines for their affiliates. Meanwhile the US National Institute for Standard and Technologies, NIST, initiated the Special Publications 800 series to present documents of general interest to the computer security community [12]. The first official standard issued was the NIST 800-53, the Guide for Assessing the Security Controls in Federal Information Systems and Organizations that became a reference for many industrial end users. This is now complemented by the SP 800-82 Guide to Industrial Control Systems (ICS) Security, currently in its 2nd revision. Compliance to NIST standards is compulsory and binding for US federal agencies.

The last and most comprehensive framework so far addressing Industrial Control System Security is the ISA-99, issued since 2007 by the International Society of Automation (ISA) and later endorsed by the International Electro-technical Commission (IEC) as the IEC-62443. ISA/IEC-62443 [13] is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems.

Meanwhile the NERC, a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America, has issued since the early 2000s a complete set of guidelines, the NERC-CIP 001 to 010 [14], to ensure protection of the bulk power system as a critical infrastructure. These guidelines later became standards whose compliance is mandatory by electrical utilities affiliated to NERC.

Table 1 – Main standards and added value with respect to guidelines

Standard	Reference sector	Stakeholders involved	Compliance	Added value
ISO 27000 **ISO 27033**	IT in general IT networks	End users and product manufacturers	May be required in specific market segments	Compliance as a quality mark
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	US federal agencies Service/Product providers to the above	Compulsory and binding for US federal agencies	Needed in practice for products in any relevant sector (e.g. defence)
NIST 800-82	Industrial Control Systems (ICS) Security	id.	id.	id.
ISA/IEC-62443	Automation	End users/product or service providers	Work in progress	
NERC CIP 001-010	North American power system	NERC affiliates (electrical utilities and grid operators)	Mandatory for NERC affiliates	Consensus based

3. Socio-political impact so far in the US and in Europe

On the whole, the standards mentioned provide a set of instructions about how to implement inside an organisation an information security risk management system, so as to deal with the business risk associated with use, ownership, operation, involvement, influence and adoption of IT within an enterprise in a systematic way. For instance, the NIST developments are now part of a whole Framework for Improving Critical Infrastructure Cybersecurity [16], that follows the President Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* [17], which recognizes that the national and economic security of the United States depends on the reliable functioning of critical infrastructure. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber-risks to critical infrastructure.

Europe has followed in the steps of the US with considerable delay: its main Directive on the identification and designation of EU critical infrastructures dates back to 2008, the *Council Directive 2008/114/EC* [18]. Since Europe is not a federal state, its implementation did not alter substantially current policies on CIP in the member states so far. Although it originated some important initiatives such as the European Programme for Critical Infrastructure Protection – EPCIP - which also funded the ESSENCE project, its impact was limited also by financial constraints. In fact, notwithstanding the fact that in Common Foreign and Security Policy, security is the second pillar and fight against crime is the third, security related investments directly managed by the European Commission remain a very small share of the USA federal budget[1].

Notwithstanding the huge public effort to confront cyber-crime, many sources underline the increasing risk connected to cyber-attacks against industrial control systems. Piggin [19], who also reports some recent successful attacks to European power operators, observes that the sophistication of attacks is increasing as is the likelihood that they will be physically destructive and cause significant loss.

A recent survey [20] provides a grim assessment of the current situation in the US: '*cybersecurity incidents multiply in frequency and cost, the cybersecurity programs of US organizations do not rival the persistence and technological prowess of their cyber adversaries. Organizations do not adequately address employee and insider vulnerabilities, nor do they assess the security practices of third-part partners and supply chains. Most do not strategically invest in cybersecurity and ensure that it is aligned with their overall business strategy*'. The ICS CERT Incident Response Summary Report [21] provides a reliable survey on the industry practice where relevant data about frequency and incidence of cyber security events are provided. It must be observed that the energy sector is a fundamental target of the attacks. Until 2013 a large majority of incidents reported by ICS CERT (52%) involved energy control systems. This share has been reducing in recent years, probably thanks to the better protection connected to NERC-CIP enforcement: by 2016 the energy sector accounted only for 20% of the incidents and was overtaken by the critical manufacturing sector. The assessment of [20] is echoed by a recent and reliable industrial source [22], which believes that '*security is still an underestimated problem and still very much a work in progress*', describes '*the prevailing confusion in the industry regarding the numerous different standard*' and points out '*a pragmatic approach that recommends actions for end users and vendors*'. The paper also provides a practical example of a real-world standard assessment in a European power plant.

[1] Although the comparison may seem inappropriate, in view of the fact that the EU is not a federal state, it is worth noting that the EU budget (http://www.consilium.europa.eu/en/policies/eu-annual-budget/eu-budget-2015/) in 2015 allocated 2,147 million€ to the heading "Security and citizenship", while the 2015 budget of the US Department Homeland Security (http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf) summed up to 60,918 Million$.

A vivid review of what happened related to security of the Bulk (i.e., transport) electric system in the US is depicted by Marianne Hoebich [1]. This thesis provides a historical perspective on key developments in cyber critical infrastructure protection efforts to secure the bulk power grid system, by examining 21 key developments that occurred from 1997 to 2008. The Hoebich survey makes distinction in between efforts made by the public sector (DHS - Department of Homeland Security, DOE - Department of Energy and FERC - Federal Energy Regulatory Commission) and the private sector (NERC – the North American Electricity Reliability Corporation). *'The three main issues that were identified are the impact of economics, major power outages, and the ineffective partnership efforts between the DHS and the private entities within the electricity sector. These issues will need to be solved in the future so cyber critical infrastructure protection for the bulk-power grid system can proceed'*. Although this report is now quite outdated, the key issues it raises appear still valid. The economic burden connected to standard implementation, the difficulty to clearly forecast it, and the high number of stakeholders involved, explain why a generalised adoption of standards appears still far to come even if the risks connected to cyber-attacks are already widely described and discussed in the literature [23] .

4. The rationale of a cost-benefit evaluation of security standards based on two case studies

As shown in the previous section, at the beginning of the project a lot of work on the definition and also on the technical assessment [24] [15] of standards against malicious attacks had already been done. Nevertheless, in Europe no clear position had emerged while some standards failed to be completed for years. Many operators adopted different types of protections – above all the Transmission System Operators (TSOs) - but without a shared design. Substantially the lack of concrete experience on what generalized standard compliance would imply was an obstacle against regulation. 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. 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 hypothetical blackouts caused by malicious cyber-attacks.

The project conclusions were largely based on the outcome of two case studies, concerning a broad portion of the Italian power generation capability and the Polish Transmission System. No evaluation concerned a distribution network, which could represent an important basis for a future extension of research activities.

Although the two case-studies differ for many features, such as the type of activity, the relevant attack scenarios and even the countermeasures to be implemented, they bear some common characteristics and, to allow a joint assessment, they have been approached with a methodology which included the following common activities:

- Identification of the most likely attack scenarios able to seriously hamper the infrastructure operation;
- Detailed listing of the countermeasures able to block the attacks or to mitigate their consequences and comparison between the different standards;

- Detailed study of the consequences of a successful attack (duration of black-out and recovery path, extension of the region involved, type and profile of consumers not supplied in the various phases of the recovery, and amount of electricity not sold);
- Cost assessment has been based on two comparisons:
    - Regulated scenario (compulsory standard implementation) versus non-regulated scenario (actual countermeasures implemented on a voluntary basis)
    - Regulated scenario versus no protection at all (unrealistic situation useful only as benchmark)
- Cost analysis identifying:
    - Investment costs and maintaining costs
    - Governance costs, software and hardware requirements.

Both cases identified some situations in which Industrial Control Systems (ICS) bear important vulnerabilities. These power system weaknesses are clearly confirmed by some past blackouts due to natural phenomena and technical failures (e.g. Italy 2003, USA and Canada 2003, Germany and other Europe countries 2006, India 2012). These events may cause very high direct damage, both to the productive sector (agriculture, industry, services) and to residential users. In case-studies' scenarios attackers exploit these vulnerabilities and lead to sudden shutdown of some power generation plants or of some substations of the transmission grid, which in turn cause a region-wide black-out lasting 6 hours and involving million users. In the Italian case study the cyber-attack is carried out through well forged malware diffusion within the process control network act to damage the OS, or through DDoS and targets a power generation plant (400 MW) during the maintenance period of the cable connecting the area to the rest of the national grid during the day hours of peak request. This because in Italy, in order to consider an event as critical, it should occur together with other conditions, since in Italy there is not a node managing power close to 3000MW, which is the threshold over which the system is unable to react. In the Polish case study, hypothetical serious disturbance on three substations result in cascading loss of power supply in the entire Warsaw city.

5. Cost of countermeasures

One of our main goals was the calculation on an objective basis of the cost of standard compliance, on which very limited evidence is available in the literature [25]. The project identified the key organizational and technical countermeasures needed to increase the security level of the involved infrastructures. Although these do not totally eliminate existing vulnerabilities, they make the occurrence of serious events much less likely. The relevant countermeasures were identified by surveying many standards and guidelines. In particular for the protection of generation plants the analysis concerned one standard specific for the electricity systems (NERC), two standards as far industrial controls are concerned - ISA 99-03-02 and NIST 800-82 - and two standards specific for the information system, ISO/IEC 27001 and NIST 800-53. NIST 800-53 was surveyed also for the case-study concerning the protection of the grid, together with ISO 27002 and IEC 62351 (Information Security for Power System Control Operations, a very specific standard for standard Remote Technical Units). The comparison among them is that there are not huge differences among the prescribed countermeasures, leading to compliance costs that are similar.

We considered both governance costs and hardware and software (hw/sw) costs. The Governance cost refers to the design, operation and maintenance of corporate policy and procedures for the logical security of all the company divisions and refers to the whole firm or group. The hw/sw cost are related to the design,

acquisition, operation and maintenance of the technical devices to secure hosts and networks of each power plant and data network and is a value associated to each production unit.

In the Italian case, the considered system has to be divided into security zones, according to its functionality and criticality and to its physical location. This means to identify security zones by grouping of logical or physical assets that share common security requirements. To establish a desired level of trust, it is required that all resources inside a zone have a certain minimum level of security as determined by the organization's security policies. 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.

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

- 54 countermeasures, aiming at hampering remote attack by unauthorized persons,
- 78 countermeasures, which try to block possible local attacks either by staff or by unauthorized persons,
- 40 countermeasures, which interact to allow hazard on identification stage reconnaissance and preventing its escalation,
- 39 countermeasures, which interact to shorten downtime of systems that have been successfully attacked

Starting from the output of the case studies, which are based on the costs that should be borne by a specific firm, the analysis calculated the cost that a country should deal with in the adoption of security standards in the transmission and generation of electricity. Detailed information on the attack scenarios, selected countermeasures and cost calculation may be found – with a detail level compatible with the necessity to avoid exposure of confidential and critical information – in [26] and [27]. A discussion of the Italian case study is also available in [28]. In the Italian case, some assumptions have been made to assess the number of plants (belonging to several operators) it would be necessary to protect, whereas in the Polish case study, concerning the national TSO, the whole protection of the Polish transmission grid is included in the assessment. This also explains why in Table 2 in the Polish case the cost may be estimated precisely, due to the fact that a unique transmission system operator is in charge of the system. In the Italian case a lot of big and small generation companies operate and so an estimation range was pointed out. The adopted methodology quantifies the cash flows for the implementation and maintenance of the security standards. Some of the costs, specifically the ones related to the design, acquisition and implementation of countermeasures, are investment costs to be borne only once, at the initial time (CAPEX); other costs, specifically those related to the maintenance of the countermeasures, are operational costs to be borne annually (OPEX).

In both cases two situations have been considered: costs that should be borne in an hypothetical scenario where no security standards had been implemented yet (Cost starting from 0) and costs that should be borne

starting from the current situation in order to manage a higher supplementary security (Delta cost). Of course the first columns are recorded just as reference, to understand the share of total investment which has already been afforded, since no power system is actually deprived of any protection.

Table 2: Total cost of implementing and maintaining countermeasures in Poland and in Italy (000 €)

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

Source: [25]

Table 3 shows more detailed data for PSE, the Polish TSO. Moreover, as a tool for the generalisation of the results, a quantification of the total effort (no implemented protection) necessary for a smaller (30 substations) and larger (200 substations) TSO is provided, adopting a non-proportional scale.

Table 3: Total cost of implementing and maintaining countermeasures in a TSO (€)

		SMALLER COUNTRY	POLAND	LARGER COUNTRY
Implementing	Substations	6,047,200	1,5118,000	27,212,400
	Information control systems	1,453,280	3,633,200	6,539,760
	Office systems	2,905,920	7,264,800	1,3076,640
	TOTAL CAPEX	10,406,400	26,016,000	46,828,800
Maintaining costs/ Software	Substations	834,900	2,087,250	3,757,050
	Information control systems	155,216	388,040	698,472
	Office systems	510,496	1,276,240	2,297,232
	Total maintaining Software	1,500,612	3,751,530	6,752,754
Maintaining costs/ Labour	Substations	208,800	696,000	1,392,000
	Information control systems	54,000	180,000	360,000
	Office systems	116,700	389,000	778,000
	Total maintaining labour	379,500	1,265,000	2,530,000
	TOTAL OPEX	1,880,112	5,016,530	9,282,754

Source: [25]

6. Assessment of the economic impact involved

As in every evaluation exercise, impact analysis derives by the comparison between the regulated and the unregulated situation. 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. The benefits are in fact represented by the possibility to avoid the consequences of an attack, which may assume different forms, such as *blackouts* (loss of power lasting a period of time), *brownouts* (non-complete drop in voltage),

transient faults (loss of power lasting few seconds), etc. Our study focused on the evaluation of the economic value of the most disruptive consequence, i.e. of blackouts in selected areas, since the case study underlined that these events are far from being unlikely. Both case-studies showed in fact that an attack born in conditions of vulnerability lead to extended and durable blackouts. Since security standards will hamper the huge inconveniences of a blackout, the benefits have been estimated as the socio-economic damages which one could avoid when implementing the correct countermeasures.

The estimates include impact on households, on electricity firms, and on other firms. As far as the productive sector, just losses in production (avoided income) are included in the figure, while direct damages to processes are not, since the values differ very much following the process and the type of firm. A large blackout may in fact also result into damage that does not directly depend on production loss. Although this cannot be quantified by a macroeconomic approach, some qualitative information may be extracted by analysing past blackouts. They relate to emerging costs related to damages to production lines, to the deterioration of raw materials and products and to long restarting times. A precise day was set for the attack in the case study, in order to evaluate the indirect economic impact of the blackout (lost production). A great detail in the load profile in the unruffled situation is fundamental to describe correctly the process of recovery after the blackout. The load profile for each major category of users on a quarter-hour basis has been obtained by the national TSOs. The damage for each sector was calculated relying on its measure of the Value Of Lost Load (VOLL=VA/EC, where VA is the value added and EC the yearly energy consumption). Some estimates also took into account the limited energy dependence of some economic activities.

The cost of the blackout for the electricity sector was evaluated in terms of value of the energy non-supplied to final customers, considering the generators and the other operators of the electricity chain.

For individuals, a survey-based methodology (stated preferences) was adopted. In particular we adopted an approach estimating the willingness to accept (WTA) blackouts of certain durations, provided that the supplier would have compensated the household with a bill discount. The core section asking to "give a value" to different black-out scenarios was complemented by list of variables aimed at profiling the household in a socio-economic perspective and in terms of power consumption. We collected 623 questionnaires, of which 456 contained all the relevant information and could be employed for the estimates, generating seven observations each (one for each choice task), but some (127) observations were eliminated as a consequence of the outliers detection procedure. As a result, the database consists of 3065 observations. Finally we estimated an econometric model aimed at evaluating the whole damage suffered by a household during a blackout. Both economic direct cost (for example food spoilage) and social costs are included in the analysis, with reference to the domestic life of individuals, but not indirect effects (increased criminality, failures in providing essential services other than electricity supply).

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". For more details on the methodology adopted for the benefit analysis, please see [29] and [28].

The results rising from the two case studies are summarized in Table 4. Considering the strict assumptions, the detail of electricity data and macro data employed, and the types of damages for which it has been impossible to calculate a global value, the values may be considered a lower bound, prudent estimate.

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
Source: [30]

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 private user benefit being much larger than the one referring to firms and in fact, at present, private residential users are the first to be supplied after a black-out (the priority given in the recovery plan is as follows: first residential users in big towns, then all residential plus tertiary in towns, then industrial customers, finally agriculture and rural users) because they are supposed to suffer the most from the lack of electricity. On the other hand the two values are very close, above all in the Italian case-study. Even if a lot of attention has been put during the survey (also with ad-hoc preliminary questions) to get the consumer involved in the problem of security of supply, the perception of the risk is blurred by the lack of direct experience; nowadays reliability is often taken for granted and so the estimated value of the blackout is still under-evaluated. This perception would probably change a lot in a community after that a large blackout is experienced, as did happen in some Polish regions, so explaining why the difference is more significant in that case.

Also electricity utilities suffer from the blackout, in terms of decreased sales, but the value of their damage, although not negligible, is only a small fraction of the total. Actually, in many countries, utilities will pay a fee in case of interruptions in supply, but these fees have not been considered in the cost of the black-out, because these indenisations (above all when they are bargained) are another way to estimate it, and so including them in the calculations would have meant to count some effects twice.

Considering the implementation costs, it can be seen that standard compliance will not only imply huge investments, but also increased maintenance costs. These costs 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.

Comparing benefits to costs, it can be seen that even considering the most restrictive estimate of benefits and the highest estimate of costs, one single event would be enough to completely recover the total cost of complying to one security standard, both in generation and in transmission. It is nowadays impossible to estimate precisely the probability of such an event in Europe. Although the Directive on attacks against

Information Systems, which was adopted by the European Council on 22 July 2013 to fight against cyber-attacks to information systems includes the creation of a data base repository of cyber-attacks by sector, actually public information available is not sufficient to assess the probability of the different threats. Anyway, it is widely acknowledged that this probability would strongly increase after the first event 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 of the effect it carries with, which is most important for cyber-terrorists, unchaining an imitation effect and leading to an escalation of attacks.

7. Policy implications

The discussion of the results presented above can give some hints on the way policy makers could go through the decision making process and correctly regulate the efforts to mitigate the security risks of critical infrastructures.

The joint consideration of benefits and costs linked to the adoption of security standards shows that the former may largely exceed the last, even in the unrealistic case of no existing investment. This is true also considering one single malicious event. But, if the results are clear, their policy implications are not so simple and any implementation process should withstand barriers, difficulties and opposition.

First of all, benefits are shared among different social groups: although any business operating in the territory is struck by a blackout and the society as a whole as well, only a small part of the impact of a black-out concerns electricity utilities. The implementation costs for firms are much higher than the direct cost the company would bear in the event of a blackout. Our analysis clearly shows that from a mere economic viewpoint electric companies should not increase their security levels; this explains their reluctance to afford such huge investments. But this cost is also much less than the damage to production and residential end users. For this reason public regulation and support to firms, above all to those operating in competitive branches of the energy sector, is clearly necessary.

Our case studies showed that 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 not a surprising result. There is in fact a more diffused perception of the grid as a critical infrastructure, as TSOs are public companies (or publicly controlled companies) with a strong commitment to quality of service, including reliability of supply. It is hardly imaginable that a grid operator asking its control body 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, which is not the case of security standards requirements.

Support to firms is justified by the fact that the total cost of an event for the society as a whole is by far greater than the annual cost of the said countermeasures, for this reason it is of interest for the community to take actions to raise the security level and ultimately reduce global risk. 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. But the difficulty to reach the optimal level of security is related to the fact that it is a non-tradable public good, i.e. one of the causes of market failure. 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 electric system security and the most suitable mix should be agreed at the national or supranational level.

Therefore it is up to public authorities to decide to require the overall adoption of current security standards and countermeasures to the companies operating in the electric system and the nature of public good of security underlines the necessity of public support for this operation, but the extent of this support and the way this will be managed have to be discussed.

To some extent, the Commission has already undertaken this policy by the adoption of the Directive on security of Network and Information Systems (NIS)[2] and the General Data Protection Regulation (GDPR) in 2016[3], which jointly provide a baseline for cyber security.

In the case of Europe, like for the NERC countries, the whole electric system is interconnected. An event on the electricity grid in one country or macro-region may have repercussions onto many others. This moves the arena for the discussion from the national to the supranational level but adds further complexity to the process. 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 concerned. But on that respect the present landscape in Europe is quite uneven. Simply endorsing a standard cannot be a practical choice, in view of the fact that current reference frameworks are either too generic, because they refer to IT in general or ICS specifically, or were designed with reference to the North American situation and cannot be adopted as such in Europe (see Table 1). Moreover, defence is not a sector in which national governments are keen to accept common regulation. 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 country specificities. The overall aim to be addressed is to achieve a certain level of security, correlated to a pre-determined risk, by all utilities, as the security level of whole power system is ultimately equal to the one of the weakest utility.

First and foremost, there is a need that the stakeholders reach a consensus on the way to adopt and implement a common policy on the subject. This requires consensus by the stakeholder associations involved, namely the ENTSOE, the European Network of Transmission System Operators for Electricity[4], and the utilities, who have established the ENCS, the European Network for Cyber Security[5]. The two organisations have recently (June 2017) signed a memorandum of understanding on the subject[6]. On the other hand, there is a need that the Commission provides a reference framework which may be adopted by the organisations concerned. In that respect, the DG Energy has tasked an Energy Expert Cyber Security Platform (EECSP) to analyse whether the energy sector is sufficiently covered by existing legislation or if there is a need for more action to achieve an effective cyber security. The platform has provided a set of recommended actions to be taken in respect of cyber security so as to fully implement the NIS Directive and

[2] Directive (EU) 2016/1148

[3] Regulation (EU) 2016/679

[4] Representing 43 TSO over Europe and replacing all previous regional TSOs associations.

[5] A non-profit member organization supporting to deploy secure European critical energy grids and infrastructure. The ENCS encompasses several large utilities across Europe and worldwide and a number of of other partners and partner associations, including the ENTSOE (https://encs.eu/). One should note, however, the absence of EURELECTRIC, the main European utilities association, from their constituency, as well as the fact that EURELECTRIC neither mentions the topics of cyber security in its network security glossary (see: http://www.eurelectric.org/facts-terminology/terminology/networks-grids/networks/).

[6] *'The European Network for Cyber Security (ENCS) and the European Network of Transmission System Operators for Electricity (ENTSO-E) today sign a memorandum of understanding (MoU) to develop state of the art cyber security regulation, practices & standards for the electricity transmission system.'* (see: https://www.entsoe.eu/news-events/announcements/announcements-archive/Pages/News/encs-entsoe-join-forces.aspx).

the GDPR: *'This strategic framework consists of 4 strategic priorities which address key areas of threat and risk management (I), the cyber response in case of a cyber attack (II), the continuously improvement of cyber resilience (III) and the build-up of required capacities and competences (IV) for the energy sector. The overall objectives are to secure energy systems that are providing essential services to the European society and to protect the data in the energy systems and the privacy of the European citizens'* [31]. In the main, however, it is apparent that the EECSP has provided a broad and ambitious plan whose recommendations will admittedly take years to be adopted[7].

In conclusion, we are firmly convinced not only of the relevance of a generalised approach to cyber-protection of electrical critical infrastructures, but also of its socio-economical justification, as proved by the results of this study. But, in the same time we are aware that even once the decision to share a European strategy against cyber threats is taken, there remains a long process to arrive to its implementation, that requires both further research and a participative approach to reach to an agreed and sustainable solution.

References

[1] M. Hoebich, «Hoebich M., (2008), Status Report On Cyber Critical Infrastructure Protection Involving the Bulk-Power Grid System,» Purdue University, West Lafayette, IN 47907-2086, 2008.

[2] J. Osborn and C. Kawann , «Reliability of the U.S. Electricity System: Recent Trends and Current Issues,» U. S. Department of Energy, Berkeley CA 94720, August 2001.

[3] G. Rouse e J. Kelly, «Electricity Reliability: problems, progress and policy solutions,» Galvin Electricity Initiative, Feb. 2011.

[4] S. Robinson, «The Power Grid as Complex System,» *SIAM news (Society for Industrial and Applied Mathematics)*, vol. Vol 36, n. 10, December 2003.

[5] A. M. Harb, I. Batarseh, L. M. Mili e M. A. Zohdy, «Bifurcation and Chaos Theory in Electrical Power Systems: Analysis and Control,» *Mathematical Problems in Engineering*, vol. Volume 2012, 2012.

[6] M. Bartnes Line, I. A. Tøndel e M. J. Jaatun, «Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations,» *International journal of critical infrastructure protection*, vol. 12, n. March, pp. 12-26, 2016.

[7] A. Stefanini e M. Masera, «Is Public Private Partnership a suitable way to cope with security issues?,» Office for Official Publications of the European Communities, Luxembourg, 2009.

[7] *'While the recommendation on actions addresses the gaps identified by the EECSP experts,…, a further discussion and alignment with respective stakeholders is recommended to fine tune on the details to be established. The analysis in this report has considered only European policy and legislation; existing regulation and legislation of Member States would have been beyond the capabilities of the EECSP Group. It is recommended to clarify in advance that possible upcoming regulation and legislation does not contradict with existing international policy or national regulation and legislation'* [31, pp. 69-70].

[8] K. Poulsen, «Report: Cyber Attacks Caused Power Outages in Brazil,» *Wired Magazine*, 9 September 2011.

[9] ISO, «Future 27000 Standards,» The ISO 27000 Directory.

[10] ISO, «ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security».

[11] The White House, «PRESIDENTIAL DECISION DIRECTIVE/NSC-63,» 22 May 1998.

[12] Joint Task Force Initiative, «Security and Privacy Controls for Federal Information Systems and Organizations,» NIST, National Institute for Standards and Technologies, 2014.

[13] ISA, «ISA99, Industrial Automation and Control Systems Security,» ISA - International Society for Automation, Research Triangle Park, NC 27709, 2007.

[14] NERC, «NERC CIP Solutions,» North American Electric Reliability Corporation, Atlanta, Georgia, 2003-2009.

[15] U. Finardi, E. Ragazzi e A. Stefanini, «Considerations on the implementation of SCADA standards on critical infrastructures of power grids. Ceris Technical Report N. 47 http://essence.ceris.cnr.it/images/documenti/RT_47.pdf .,» Ceris Technical Report N. 47, http://essence.ceris.cnr.it/images/documenti/RT_47.pdf , 2013.

[16] NIST, «Framework for Improving Critical Infrastructure Cybersecurity,» National Institute for Technologies and Standards, Washington, 2014.

[17] B. Obama, «Executive Order -- Improving Critical Infrastructure Cybersecurity,» the White House, Washington, 2013.

[18] E. Council, «COUNCIL DIRECTIVE 2008/114/EC,» Official Journal of the European Union, Brussels, 8 December 2008.

[19] R. Piggin, «Cyber security trends: What should keep CEOs awake,» *International Journal of Critical Infrastructure Protection* , vol. 13, n. June, pp. 36-38, 2016.

[20] PWC, «US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey,» Pricewaterhouse & Coopers LLP, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf, Delaware, 2014.

[21] U. ICS-CERT, «Incident response Summary Report, 2009−2011,» ICS-CERT, http://scadahacker.com/library/Documents/ICS_Vulnerabilities/ICS-CERT%20-%20Incident%20Response%20Summary%20Report%20-%202009-2011.pdfCybercrime, 2011.

[22] R. Schierolz e B. de Wijs, «Cyber security in the power and water industries: how end users and vendors are or should be facing it,» http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/c058a88e143427f3c12578e00053f5a0/$file/3bus095405, 2011.

[23] F. Garcia, H. Bartoszewicz-Burczy, A. Cortes, D. Pestonesi e T. Wlodarczyk , «Attack Scenarios. Threats, vulnerabilities and attack scenarios along with their selection criteria,» CERIS Technical Report N. 48, : http://essence.ceris.cnr.it/images/documenti/RT_48.pdf, 2013.

[24] M. Masera e A. Stefanini, «Towards Standardisation Measures to Support the Security of Control and Real-Time Systems for Energy Critical Infrastructures,» Office for Official Publications of the European Communities, Luxembourg.

[25] G. Calabrese, U. Finardi e E. Ragazzi, «Cost Analysis of Standard Implementation in the SCADA Systems of Electric Critical Infrastructures,» Ceris Technical Report N. 53, http://essence.ceris.cnr.it/images/documenti/RT_53.pdf.

[26] L. Guidi, C. Bruno, M. Alessi, V. Angeletti, M. Biancardi, F. Erbetta, G. Fraquelli, A. Lorite-Espejo e D. Pestonesi , «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,» Ceris Technical Report N.55 . http://essence.ceris.cnr.it/images/documenti/RT_55.pdf, 2014.

[27] H. Bartoszewicz-Burczy, C. Bruno, F. Garcia e T. Wlodarczyk, «Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards,» Ceris Technical Report N.56 http://essence.ceris.cnr.it/images/documenti/RT_56.pdf, 2014.

[28] C. Bruno, L. Guidi, A. Lorite-Espejo e D. Pestonesi, «Assessing a Potential Cyberattack on the Italian System,» *IEEE Security&Privacy*, vol. 13, n. 15 September/October.

[29] C. Bruno, H. Bartoszewicz-Burczy, L. Guidi, G. Abrate, F. Erbetta, U. Finardi, G. Fraquelli, A. Cortes, A. Diu, E. Doheijo, G. Falavigna, A. Lorite-Espejo, V. Moiso, D. Pestonesi, E. Ragazzi e T. Wlodarczyk , «Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case studies,» Ceris Technical Report N. 52, http://essence.ceris.cnr.it/images/documenti/RT_52.pdf, 2014.

[30] E. Ragazzi e F. García Gutiérrez, «Trial evaluation: conclusive lessons from Essence case studies. Ceris Tecnical Report series n.57,» Moncalieri, 2014.

[31] E. E. C. S. Platform, «Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,» February 2017. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf. [Consultato il giorno 2 December 2017].