Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies

Elena Ragazzi*

CNR-Ircres,
Via Real Collegio 30,
10024 Moncalieri (TO), Italy
Fax: +390116824966
Email: elena.ragazzi@ircres.cnr.it
*Corresponding author

Alberto Stefanini

Via Tagliamento, 4,
43036 Fidenza (PR), Italy
Email: alberto_stefanini@virgilio.it

Abstract: Power system controls are vulnerable to cyber-attacks that can seriously affect and even inhibit their operation. Such attacks may affect large portions of the power system, make repair difficult and cause huge societal impact, so pressure to ensure cyber-security of control and communication systems is now strong worldwide. Several cyber-security frameworks were developed, but it is rather difficult to anticipate adoption costs and benefits, and this hampers their generalised adoption. This paper focuses on the outcome of two case studies (concerning the Italian power generation and the Polish transmission systems. The socio-economic impact of failures and the costs of standard adoption are estimated on an objective basis. It is up to public authorities to decide whether to require the adoption of security standards to operators in the electric system. The nature of public good of security underlines the necessity of public support for this operation, but we discuss the extent and the management of this support.

Keywords: security standards; electricity systems; cybersecurity; cost-benefit analysis; impact evaluation; network security plans; security policies; regulations; power system controls; countermeasures.

Reference to this paper should be made as follows: Ragazzi, E. and Stefanini, A. (2019) 'Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies', *Int. J. Critical Infrastructures*, Vol. 15, No. 3, pp.206–229.

Biographical notes: Elena Ragazzi is a Researcher in Applied Economics at the CNR-Ircres, an institute of the Italian National Research Council specialised in industrial studies, in innovation and sustainable 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 received a full honours degree in Electronic Engineering from the University of Bologna, 1974. He is currently retired and holds a consultancy. Since October 2012 he is a partner of Novareckon Knowledge Brokers (http://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 November 2009, he was with the Joint Research Centre, Institute for the Protection and 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 '70s, and contributed to launch a large number of European projects in the energy and the IT sector.

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 generalised adoption. Earlier US experience showed that applying a standard is cumbersome and costly while benefits are not fully clear to all the stakeholders involved [Hoebich, (2008), p.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.[1] The electricity infrastructure is generally more robust in Western Europe than the USA (Martino, 2016; Mc Daniel et al., 2015). Martino, quoting the CEER (2015) benchmarking report 2015, shows that SAIDI, the system average interruption duration index, is four times higher in the USA than in Germany and about three times than UK.

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-organised critical system, a system that perpetually steers itself toward a dynamic equilibrium, where small perturbations have long-range effects (Robinson, 2003). 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.

By consequence, the loss of a control equipment function may lead to catastrophic consequences, as shown extensively by Stefanini (2006, pp.12–20). This vulnerability was exploited by hackers to disrupt power systems in several recent occasions (Cherepanov and Lipowski, 2017; Fire Eye, 2016). Another dimension of complexity (and potential vulnerability) in power system is multi-jurisdictionality: 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 (Bartnes Line et al., 2016). All this inevitably leads to

different attitudes and standpoints which reflect into different security concepts and languages (Stefanini and Masera, 2009).

Finally, cyber threats are elusive: although power systems are in 'a clear and present danger' (Poulsen, 2011), the way the cyber menace materialises, the type of attack, their frequency and intensity can hardly be forecast, and only in the short-term.

This paper is based on the results of ESSENCE, a study project performed over 2012–2014 to evaluate the costs and benefits for the adoption of a shared approach to cyber security on a rational base. The study methodology included:

a the development of a common understanding of industrial needs and requirements regarding the cyber security of control systems

b the identification of the main power system vulnerabilities induced by control systems in two broad case studies

c the selection of a set of relevant standards to ensure security of the target control systems concerning the reference cases

d an orderly estimate of the costs involved for the adoption, implementation and maintenance of one (or more) of the above standards to ensure cyber security of the relevant target systems

e the evaluation of the likely socio-economic impact of failures due to faults and attacks exploiting the said vulnerabilities.

The two case studies concerned 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 organisational and technical countermeasures needed to increase the security level of the involved infrastructures so as to neutralise 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 core of the adopted methodology concerns quantification of the cash flows for the implementation and maintenance of the identified 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.

This paper follows the scheme involved by the study methodology, where Sections 2, 3 and 4 concern steps a to c of the study, while Section 5 focuses on step d and Section 6 on step e. Finally, the scope and limitations of the study and its policy implications are discussed.[2]

2 Key concepts and history of relevant standards

Quoting the home page on the IEEE website *beyond standards* (IEEE Standard Association, 2011): "standards form the fundamental building blocks for product development by establishing consistent protocols that can be universally understood and adopted. This helps fuel compatibility and interoperability and simplifies product development, and speeds time-to-market. Standards also make it easier to understand and compare competing products. As standards are globally adopted and applied in many markets, they also fuel international trade" helps understanding why, when trying to establish a shared approach to cyber security on a rational base, one may only resort to the existing and incoming standards having relevance to control systems security.

The main features and common basic principles of those standards can be better understood having a quick look on their history. The ISO 27000 series[3] is a growing family of ISO/IEC Information Security Management Systems standards that took form in the early '90s, when the British standard BS 7799 was devised. The core principles of information security[4] were recognised to be:

- confidentiality, i.e., how to prevent the disclosure of information to unauthorised individuals or systems
- integrity, meaning that data cannot be modified undetectably
- availability, the property ensuring that information is available when it is needed.

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 (The White House, 1998) emanated under Bill Clinton's presidency in May 1998 and was sustained by the spread of malicious attacks to critical infrastructures over the last two decades.

The security of industrial control systems (ICSs) has a specific feature, because security controls must be compatible with the real-time requirements of ICSs. Since the late 90s many industrial organisations, like the American Petroleum Institute (API), the North American Electricity Reliability Council (NERC) and the VGB (Vereinigung der Großkesselbesitzer – the European association of large power utility operators) 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 (Joint Task Force Initiative, 2014). 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 ICSs security, currently in its 2nd revision. Compliance to NIST standards is compulsory and binding for US federal agencies.[5]

The last and most comprehensive framework so far addressing ICS 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) (2009) as the

IEC-62443. ISA/IEC-62443 is a series of standards,[6] 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 (NERC, 2017), has issued since the early 2000s a complete set of guidelines, the NERC-CIP 001 to 014 (NERC, 2003–2009), 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 organisations	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	Industrial communication networks – network and system security	End users/product or service providers	Now complete (2018)	Most complete framework for IACS (Ind. and automation control systems)
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 USA 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 (NIST, 2014, 2018) that follows the President executive order 13636, *improving critical infrastructure cybersecurity* (Obama, 2013), which recognises that the national and economic security of the USA 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.

Indeed, cyber pressure on critical infrastructures was kept high since the early 2000. The Titan Rain episode, a series of coordinated attacks on American computer systems dates back to 2003, although they were known to have been ongoing for at least three years. The attacks were allegedly Chinese in origin, although their precise nature, e.g., state-sponsored espionage or random hacker attacks, and their real identities remain unknown (Homeland Security News Wire, 2015).

The potential for disruption of power systems was shown first by the Idaho National Laboratory in 2008, with the memorable Aurora test (Burckhart, 2008). Since then, the potential of cyber-attacks for incapacitating the institutions of whole countries was demonstrated during the attack on Estonia in 2007 and confirmed by the cyber wars that were contemporary to Russia campaigns in Georgia and South Ossetia in 2008 (Danchev, 2008).

In view of the high dependency of its economy on the internet, the USA are greatly exposed to cyber-attacks. Therefore they responded to this advanced persistent threat (Lord, 2017) through an articulated policy which involved mobilising large capabilities in both defence and power projection thanks to their advanced technology and large military budget. The United States Department of Defense recognises the use of computers and the internet to conduct warfare in cyberspace as a threat to national security, but also as a platform for attack. Since 2009, this policy among other materialised in the institution of a US cyber command whose mission is "to plan, coordinate, integrate, synchronize and conducts activities to … conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/allied freedom of action in cyberspace and deny the same to our adversaries" (USCYBERCOM, 2018).[7]

Europe has followed in the steps of the USA 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* (European Council, 2008). 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.[8]

Notwithstanding the huge public effort to confront cyber-crime, many sources underline the increasing risk connected to cyber-attacks against ICSs. Piggin (2016), 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. This was confirmed by several recent episodes targeting big plants and infrastructures in Europe and worldwide:

- In May 2017, the UK National Health System fell victim to a large-scale cyber-attack which affected around 50 health trusts in England, including hospitals, GP surgeries and pharmacies, as well as 13 NHS organisations in Scotland (Evenstad, 2017).

- Ukraine was the subject of repeated cyber-attacks over 2015–2016 (Cherepanov and Lipovski, 2017; Symantec Security Response, 2016). The hugest was on December 23, 2015, when three regional Ukrainian electricity distribution companies – Kyivoblenergo, Prykarpattyaoblenergo and Chernivtsioblenergo – suffered power outages due to a cyber-attack (Fire Eye, 2016).
- According to the Bundesamt für Sicherheit in der Informationstechnik (BSI) in December 2014 a steel mill in Germany was the target of a well-informed cyber-attack that "was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage" (Lee et al., 2014).

Notwithstanding the articulated defence policy of the USA and the wide awareness in its business community, a recent survey provides a grim assessment of the current situation in the USA: "2017 was another record year for cybercrime. According to the Online Trust Alliance (OTA), the number of cybersecurity incidents nearly doubled from the previous year. This led Jeff Wilbur, director of the OTA initiative at the internet society, to call it the 'worst year ever in data breaches'" (Loeb, 2018). The ICS CERT Incident Response Pie Chart 2017 (National Cybersecurity and Communication Centre, 2017) shows that the energy sector keeps being a major target of cyber-attacks (59 off 290, 20.34%), although this share has been reducing in recent years, and was overtaken by the critical manufacturing sector (21.62%). This was probably due to the better protection connected to NERC-CIP enforcement, while until 2013 a large majority of incidents reported by ICS CERT (52%) involved energy control systems. This assessment by PWC (2014) is echoed by a recent and reliable industrial source (Schierolz and de Wijs, 2011), 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 standards" 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.

A vivid review of what happened related to security of the bulk (i.e., transport) electric system in the US was depicted by Hoebich (2008). This thesis provided 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 made 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, several key issues it raised 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 (Garcia et al., 2013).

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

As shown in the previous section, at the beginning of the research project a lot of work on the definition and also on the technical assessment (Masera and Stefanini, 2008; Finardi et al., 2013) 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 converging on a common fixed framework. Substantially the lack of concrete experience on what generalised 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 conclusions are 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:
  a regulated scenario (compulsory standard implementation) versus non-regulated scenario (actual countermeasures implemented on a voluntary basis)
  b regulated scenario versus no protection at all (unrealistic situation useful only as benchmark).

- Cost analysis identifying:
  a investment costs and maintaining costs
  b governance costs, software and hardware requirements.

Both cases identified some situations in which ICSs 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 and indirect 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 six 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 there is not a node managing power close to 3,000 MW, 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 (Calabrese et al., 2014). The project identified the key organisational 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 organisation's security policies. The main countermeasures to be adopted can be summarised as follow:

- deploying anti-(D)DoS devices and services
- traffic filtering
- utilising timely patch management
- deploying anti-virus software
- performing system hardening
- system and network segregation
- use of 'demilitarised 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 were identified, including:

- 54 countermeasures, aiming at hampering remote attack by unauthorised persons
- 78 countermeasures, which try to block possible local attacks either by staff or by unauthorised 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 Angeletti et al. (2014) and Bartoszewicz-Burczy et al. (2014). A discussion of the Italian case study is also available in Bruno et al. (2015). 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 TSO 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 a 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: Calabrese et al. (2014)

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: Calabrese et al. (2014)

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 is concerned, 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. In all case studies analysed, anyway direct emerging costs represented only a small share respect to the avoided income due to stops in prediction.

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 3,065 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 Bruno et al., 2014, 2015).

The results rising from the two case studies are summarised 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			

Note: *Min-expected-max.

Source: Ragazzi and García Gutiérrez (2014)

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. The 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 with one security standard, both in generation and in transmission. It is nowadays still 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 database 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 (for a discussion of the escalation ladder and of counteractions proper for any stage of the conflict, see Kostyuk, et al., 2018). 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 After ESSENCE: replicability and limits of the study

This section is to reflect on the main principles deriving from the study and, after taking into consideration its limitations, to provide a guidance in view of its application and extension. One obvious limit is implied by the fact that many new threats emerged after our study.[9] ENISA keeps an updated map of the top 15 threats identified through its yearly Threat Landscape Reports (ENISA, 2018) which provide descriptions of the threats, highlight their most interesting features, include trends and statistics, enlist ransomware threats, and discuss specific attack vectors and specific mitigation actions. The above can be used as a first guidance to the main emergent threats. Contrary to expectations that with the surge of malware syndromes compliance costs could multiply with respect to the ones reported by ESSENCE, these are reported to have somewhat fallen in 2018 (with a reduction of 43% in 2018; 48% in 2017 and 2016 respect to 2013). The decrease could be associated with the use of outsourcing,[10] although it may also relate – worryingly to a lack of required resources (English and Hammond, 2018).

A second area where the ESSENCE outcome may need careful review concerns the standards landscape presented in Section 2, on two respects:

a This is even more fragmented that the one considered by ESSENCE. A recent survey (privately performed by a stakeholder association) shows that there are many other related norms and guidances that should be considered, in addition to the ones mentioned in Section 2, when the overall security policy and stand-up of a large utility is concerned:

- the ENISA guidance to smart grid stakeholders, providing a set of minimum cyber security measures
- IEC 62357 TC57 – architecture for power system information exchange
- IEC 62443 – 4.3.2.6.1 develop security policies
- IEC 62443 – 4.3.2.6.2 develop security procedures
- IEC 62351 security standards for the power system information infrastructure (in particular IEC 62351-1, IEC 62351-2, IEC 62351-3, IEC 62351-6, IEC 62351-7 and IEC 62351-11)
- IEC 60870 systems used for telecontrol standards: supervisory control and data acquisition
- IEC 61970 application program interfaces for energy management systems (EMS) standard
- NISTIR 7628 – SG.AT-2 security awareness – general requirement
- NISTIR 7628 – SG.MA-3 smart grid information system maintenance
- NISTIR 7628 – SG.SA-2 security policies for contractors and third parties
- NISTIR 7628 – SG.PS-5 personnel transfer
- ISO/IEC TR 27019 – 8.1.2 screening
- ES-C2M2 the electricity subsector cybersecurity capability maturity model
- IEC 61850 communication protocols for intelligent electronic devices at electrical substations standard
- NISTIR 7628 – SG.AT-1 awareness and training policy and procedures.

Of the above, surely the IEC 62351, 62357, 60870 and 61850 earmarked in the list, specifically concern control and communication equipment and their security.

b Even restricting the scope to the frameworks considered in Table 1, the experts involved in the ESSENCE advisory panel could not reach an agreement on a reference standard to recommend: "with respect to standard proliferation, the panel favours promoting a general purpose standard such as ISO/IEC2700x although it recognized that, as far as ICSs are concerned, it should be complemented by the IEC 62443 standard and the ISA99 family of documents. Other choices, such as standards by US derivation like the NIST 800-82 and the NERC standards, were locally favoured in some cases but are not believed, in the main, to be a valid option as far as the general EU situation is concerned." However, it is recognised that recertification is very expensive: "relevant organisations should provide mapping between different standards" (Stefanini, 2015). The statement raises an important point: certification costs are considerable (within the ESSENCE exercise they were considered to amount to some 30% of the cost of the equipment), hence recertifying an ICS according to a different standard, as local constraints may require, is very expensive.[11] This remark also shows how important would be to keep a map of the

prescriptions raised by the main standards, which often overlap, possibly by instrumenting a comparative ontology, in such a way as not to repeat the whole certification process any time.

Another direction of research connected with cost assessment concerns the scalability and transferability of estimates. Operative scenarios vary a lot among countries and operators and so a parametric approach appears simplistic. While an estimate based on the assumption of proportionality of costs respect to the size (of the territory, or of the population served, or of the firm) would be too rough to be acceptable, a calculation adopting the ESSENCE approach (based on the sequence vulnerabilities-countermeasures-costs) requires a considerable effort. A further work on the nature and scalability of the detailed cost components could represent a way to go towards a cost function of cyber-security protection.

8 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: 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 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.

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. Moreover, 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 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. The commission recognised this need and issued a proposal for a regulation on risk-preparedness in the electricity sector, COM(2016) 862 (European Commission, 2016), to repeal the directive on security of the electricity supply (2005/89/EC) currently in force (this latter contains a rough framework of objectives to be achieved by the member states in the area of security of the electricity supply). The proposed regulation addresses situations where an *electricity crisis* exists in a member state because there is a *significant electricity shortage* or electricity cannot be supplied to the end-consumer due to damage to the electricity infrastructure (Art. 2). The causes of electricity crises include extreme weather conditions, cyber-attacks and fuel shortages (p.2). Member states currently take different approaches to preventing and managing electricity crises. In future, they will be obliged to increase cooperation at regional level on measures to manage cross-border electricity crises (p.3).[12]

The European Network of Transmission System Operators (ENTSO-E)[13] should regularly draw up and update regional crisis scenarios and identify the most relevant risks (art 13). Within ten months after entry into force of the regulation, ENTSO-E must determine – on the basis of its own methodology developed in advance – the "most relevant electricity crisis scenarios" for each system operation region (art. 6 in conjunction with art. 5).

This proposal gives an outstanding role to the ENTSO-E and requires the opinion of the utilities and the other stakeholders involved. However, the proposal appears to face a long way before it is adopted. Looking into the amendments asked by the parliament and the council (European Council, 2018, 24 April), key areas of disagreement appear to concern:

- the degree of compliance with the objectives of the EU (amendment AM1)

- the cross-border effects that require coordination among member states (AM2)
- the role of member states (AM3)
- consistency between the provisions of this regulation and the network code on emergency and restoration (AM4)
- several issues related to degree of solidarity asked to member states (AM6)

On the specific subject of cyber risk, worth also noting that a number of utilities have established the ENCS, the European Network for Cyber Security.[14] ENTSO-E and the ENCS have recently (June 2017) signed a memorandum of understanding on the subject.[15]

Table 5 Summary of objectives and roles for an EU strategy for cyber-protection of electrical critical infrastructures

EU Initiative	*Objectives*	*Stakeholders involved*
COM(2016) 861 and 862	Agree upon a framework to manage electricity crises (included cyber-attack induced ones).	EU political authorities (commission, parliament, council)
	Establish cross-border *system operation regions*.	EU Agency for the Cooperation of Energy Regulators (ACER) on proposal of the ENTSO-E
	Identify the most relevant electricity crisis scenarios at the national level.	Member states
	Appoint one authority to establish a risk-preparedness plan.	
	Inform the commission and the electricity coordination group of the extent to which CI ownership could jeopardise the security of supply and the risk mitigation measures.	
MoU ENTSO-E and ENCS	Achieve a memorandum of understanding on cyber risk management.	Sector associations (TSOs and utilities)
EECSP recommendations	Review existing legislation and achieve an agreed risk management approach and a set of recommended technical measures.	TSOs and utilities

Concerning existing legislation, 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 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" (EECSP, 2017). 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.[16]

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-economic 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 a participative approach to reach an agreed and sustainable solution. In the main, although the initiatives discussed above (i.e., the proposal for a regulation on risk-preparedness in the electricity sector COM(2016) 862, the memorandum of understanding in between ENTSO-E and the ENCS and the EECSP recommendations) are uncoordinated and do not involve the same stakeholders, summarily they configure a strategy, including a set of harmonised objectives to be reached, where each stakeholder category plays a role, as summarised in Table 5.

Acknowledgements

We gratefully acknowledge that most of the work presented in Sections 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/

Although the paper has been jointly conceived and its contents agreed among the authors, Sections 2, 3 and 7 may be attributed to Alberto Stefanini and Sections 4, 5 and 6 to Elena Ragazzi. Sections 1 and 8 have been jointly elaborated.

References

Angeletti, V., Guidi, L., Pestonesi, D., Biancardi, M., Alessi, M., Abrate, G., Bruno, C., Erbetta, F., Fraquelli, G. and Lorite-Espejo, A. (2014) *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 No. 55 [online] http://essence.ceris.cnr.it/images/documenti/RT_55.pdf (accessed 20 November 2018).

Bartnes Line, M., Tøndel, I.A. and Jaatun, M.J. (2016) '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*, March, Vol. 12, pp.12–26.

Bartoszewicz-Burczy, H., Bruno, C., Garcia, F. and Wlodarczyk, T. (2014) *Polish Case Study. Scenario based Assessment of Costs and Benefits of Adoption of Comprehensive CIP Standards*, Ceris Technical Report No. 56 [online] http://essence.ceris.cnr.it/images/documenti/RT_56.pdf (accessed 20 November 2018).

Bruno, C., Abrate, G., Bartoszewicz-Burczy, H., Cortes, A., Diu, A., Doheijo, E., Erbetta, F., Falavigna, G., Finardi, U., Fraquelli, G., Guidi, L., Lorite-Espejo, A., Moiso, V., Pestonesi, D., Ragazzi, E. and Wlodarczyk, T. (2014) *Benefit Analysis. Assessing the Cost of Blackouts in Case of Attack. Evaluation based on Italian and Polish Case Studies*, Ceris Technical Report No. 52 [online] http://essence.ceris.cnr.it/images/documenti/RT_52.pdf (accessed 20 November 2018).

Bruno, C., Guidi, L., Lorite-Espejo, A. and Pestonesi, D. (2015) 'Assessing a potential cyberattack on the Italian system', *IEEE Security & Privacy*, September/October, Vol. 13, No. 5, pp.42–51.

Burckhart, L.A. (2008) *Cyber Attack! – Lessons Learned: Aurora Attack* [online] https://www.fortnightly.com/fortnightly/2008/01/cyber-attack-lessons-learned-aurora-attack (accessed 28 August 2018).

Calabrese, G., Finardi, U. and Ragazzi, E. (2014) *Cost Analysis of Standard Implementation in the SCADA Systems of Electric Critical Infrastructures*, Ceris Technical Report No. 53 [online] http://essence.ceris.cnr.it/images/documenti/RT_53.pdf (accessed 20 November 2018).

CEER (2015) *CEER Benchmarking Report 5.2 on the Continuity of Electricity Supply – Data Update*, CEER, Brussels, Ref. C15-EWG-112-03, 8 October [online] https://www.ceer.eu/documents/104400/-/-/cbc48e6a-5d5e-a170-ae1d-7b7b298d46a4 (accessed 21 November 2018).

Cherepanov, A. and Lipovski, R. (2017) *Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet* [online] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (accessed 28 August 2018).

Danchev, D. (2008) *Coordinated Russia vs. Georgia Cyber Attack in Progress* [online] https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/ (accessed 28 August 2018).

EECSP (2017) *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* [online] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (accessed 2 December 2017).

English, S. and Hammond, S. (2018) *Cost of Compliance 2018: Outsourcing, Cyber Resilience, Data Protection and GDPR. Thomson Reuters* [online] https://www.reuters.com/article/bc-finreg-compliance-cost-cyber-gdpr/cost-of-compliance-2018-outsourcing-cyber-resilience-data-protection-and-gdpr-idUSKBN1KF2NE (accessed 29 August 2018).

ENISA (2018) *ENISA Threat Landscape Report 2017 – 15 Top Cyber-Threats and Trends*, ENISA, Heraklion, Greece.

European Commission (2016) *Proposal for a Regulation of the European Parliament and of the Council on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC* [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0862 (accessed 31 August 2018).

European Council (2008) *Council Directive 2008/114/EC*, Official Journal of the European Union, Brussels.

European Council (2018) *Proposal for a Regulation of the European Parliament and of the Council on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC*, Council of the European Union, Brussels.

Evenstad, L. (2017) *CW500: How the NHS WannaCry Cyber Attack Unfolded* [online] https://www.computerweekly.com/news/450428252/CW500-How-the-NHS-WannaCry-cyber-attack-unfolded (accessed 28 August 2018).

Finardi, U., Ragazzi, E. and Stefanini, A. (2013) *Considerations on the Implementation of SCADA Standards on Critical Infrastructures of Power Grids*, Ceris Technical Report No. 47 [online] http://essence.ceris.cnr.it/images/documenti/RT_47.pdf (accessed 20 November 2018).

Fire Eye (2016) *Cyber Attacks on the Ukrainian Grid: What You Should Know* [online] https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf (accessed 8 August 2018).

Garcia, F., Alessi, M., Bartoszewicz-Burczy, H., Cortes, A., Pestonesi, D. and Włodarczyk, T. (2013) *Attack Scenarios. Threats, Vulnerabilities and Attack Scenarios Along with their Selection Criteria*, CERIS Technical Report No. 48 [online] http://essence.ceris.cnr.it/images/documenti/RT_48.pdf (accessed 20 November 2018).

Hoebich, M. (2008) *Status Report on Cyber Critical Infrastructure Protection Involving the Bulk-Power Grid System*, Purdue University, West Lafayette, IN 47907-2086.

Homeland Security News Wire (2015) *The Lesson of Titan Rain: Articulate the Dangers of Cyber Attack to Upper Management* [online] http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management (accessed 26 October 2018).

IEC (2009) *IEC TS 62443-1-1:2009* [online] https://webstore.iec.ch/publication/7029#additionalinfo (accessed 29 August 2018).

IEEE Standard Association (2011) *Beyond Standards* [online] https://beyondstandards.ieee.org/general-news/what-are-standards-why-are-they-important/ (accessed 26 August 2018).

ISO (2013) *The ISO 27000 Directory* [online] http://www.27000.org/ (accessed 28 August 2018).

ISO (2018a) *Future 27000 Standards* [online] http://www.27000.org/future.htm (accessed 28 August 2018).

ISO (2018b) *ISO/IEC 15408 Information Technology – Security Techniques – Evaluation Criteria for IT Security* [online] https://www.iso.org/standard/50341.html (accessed 28 August 2018).

Joint Task Force Initiative (2014) *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute for Standards and Technologies, NIST.

Katina, F., Zio, E., Keating, C.B. and Gheorghe, A.V. (2016) 'A criticality-based approach for the analysis of smart grids', in *Technology and Economics of Smart Grids and Sustainable Energy*, pp.1–14, Springer, Singapore.

Kostyuk, N., Powell, S. and Skach, M. (2018) 'Determinants of the cyber escalation ladder', *The Cyber Defense Review*, Vol. 3, No. 1, pp.123–134.

Lee, R.M., Assante, M.J. and Conway, T. (2014) *ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper – German Steel Mill Cyber Attack* [online] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (accessed 28 August 2018).

Loeb, B. (2018) *Security Intelligence: Cybersecurity Incidents Doubled in 2017, Study Finds* [online] https://securityintelligence.com/news/cybersecurity-incidents-doubled-in-2017-study-finds/ (accessed 28 August 2018).

Lord, N. (2017) *Digital Guardian: What is an Advanced Persistent Threat? APT Definition* [online] https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition (accessed 28 August 2018).

Martino, S. (2016) *EPRI 2016 Outage Data for Reliability and Resiliency Survey* [online] http://grouper.ieee.org/groups/td/dist/sd/doc/2016-09-01%20EPRI%202016%20Outage%20Data%20Survey-Sal%20Martinosecured.pdf (accessed 8 August 2018).

Masera, M. and Stefanini, A. (2008) *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.

Mc Daniel, J., Friedl, W. and Caswell, H. (2015) *Benchmarking of Reliability: North American and European Experience*, Lyon, CIRED.

National Cybersecurity and Communication Centre (2017) *FY 2016 Incidents by Sector (290 Total)* [online] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (accessed 28 August 2018).

NERC (2003–2009) *NERC CIP Solutions*, North American Electric Reliability Corporation, Atlanta, Georgia.

NERC (2017) *About NERC* [online] https://www.nerc.com/AboutNERC/Pages/default.aspx (accessed 26 August 2018).

NIST (2014) *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute for Technologies and Standards, Washington.

NIST (2018) *NIST Cyber Security Framework* [online] https://www.nist.gov/cyberframework/framework (accessed 27 August 2018).

Obama, B. (2013) *Executive Order – Improving Critical Infrastructure Cybersecurity*, the White House, Washington.

Piggin, R. (2016) 'Cyber security trends: what should keep CEOs awake', *International Journal of Critical Infrastructure Protection*, June, Vol. 13, pp.36–38.

Poulsen, K. (2011) 'Report: cyber attacks caused power outages in Brazil', *Wired Magazine*.

PWC (2014) *US Cybercrime: Rising Risks, Reduced Readiness Key Findings from the 2014 US State of Cybercrime Survey*, Price-waterhouse & Coopers LLP, Delaware [online] http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf (accessed 20 November 2018).

Ragazzi, E. and García Gutiérrez, F. (2014) *Trial Evaluation: Conclusive Lessons from Essence Case Studies*, Ceris Technical Report Series No. 57 [online] http://essence.ceris.cnr.it/images/documenti/RT_57.pdf (accessed 20 November 2018).

Robinson, S. (2003) 'The power grid as complex system', *SIAM News*, December, Vol. 36, No. 10 [online] https://archive.siam.org/news/news.php?id=377 (accessed 20 November 2018).

Schierolz, R. and de Wijs, B. (2011) 'Cybersecurity in power plants: still an underestimated problem – how end users and vendors are or should be facing it', *PowerGen Europe*, Pennwell Publishing, Amsterdam.

Shearer, J. (2017) *Symantec on W32.Stuxnet* [online] https://www.symantec.com/security-center/writeup/2010-071400-3123-99 (accessed 28 August 2018).

Stefanini, A. (2006) *Electric System Vulnerabilities: Lessons from Recent Blackouts and the Role of ICT*, European Commission – Technical EUR report EUR 21551 EN, Brussels.

Stefanini, A. (2015) *Consensus Report on the ESSENCE Conclusions*, CNR-Ceris, Torino.

Stefanini, A. and Masera, M. (2009) *Is Public Private Partnership a Suitable Way to Cope with Security Issues?*, Office for Official Publications of the European Communities, Luxembourg.

Symantec (2018) *Stuxnet* [online] https://www.symantec.com/security-center/writeup/2010-071400-3123-99 (accessed 29 August 2018)

Symantec Security Response (2016) *Destructive Disakil Malware Linked to Ukraine Power Outages also used against Media Organizations Attacks* [online] https://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations (accessed 28 August 2018).

The White House (1998) Presidential Decision Directive/NSC-63 [online] https://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 20 November 2018).

USCYBERCOM (2018) *US Cyber Command – Mission and Vision* [online] https://www.cybercom.mil/About/Mission-and-Vision/ (accessed 28 August 2018).

Notes

1 The way US experience can hardly be transferred as such into the European power system is argued more extensively in Section 3.

2 An overall approach to risk management in smart grids was recently proposed by Katina et al. (2016). This study focuses on two primary objectives:

a to understand how the concept of risk is currently being addressed in smart grids

b to suggest a more holistic view of risk for smart grids.

Our paper scope is limited to transport networks, rather than addressing the full spectrum of smart grids, which finds most application in the distribution area. Moreover it focuses on the socio-economic aspects of cyber security standards compliance rather than on risk management on the whole.

3 An up to date overview of the series is kept in *the ISO 27000 Directory* (ISO, 2013). Future standards of the series are anticipated in (ISO, 2018a).

4 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 (ISO, 2018b).

5 Now the NIST Cyber Security Framework seems to be the current, all-encompassing approach on which NIST invests (NIST, 2018), see also next section. This is a generalised version of the previous ones, oriented to any company having relevant business. As reported in the quoted website, the framework "can help agencies to integrate existing risk management and compliance efforts and structure consistent communication, both across teams and with leadership. It can be valuable in managing federal information and information, implementing security controls detailed in SP 800-53 revision 4, and using the methodology outlined in SP 800-39."

6 The whole series also includes standards: IEC 62443-2-1:2010, IEC TR 62443-2-3:2015, IEC 62443-2-4:2015, IEC 62443-2-4:2015/AMD1:2017, IEC TR 62443-3-1:2009, IEC 62443-3-3:2013, IEC 62443-4-1:2018. The framework defines a set of security assurance levels (SAL) which provide increasing SAL targets according to the criticality level of the implement. Cybersecurity certification programs for IEC 62443 standards are being offered globally by several recognised certification bodies.

7 Partly due to this policy, recent cyber-attacks tended to focus on wide Asian countries such as Iran, Indonesia and India. For instance, the amount of infections by the Stuxnet virus was reported to be 58.5% in Iran and 18.2% in Indonesia of the worldwide total (Shearer, 2017).

8 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://ec.europa.eu/budget/library/biblio/documents/2017/budget-adoption-factsheet-2017_en.pdf) in 2017 allocated 6 million€ to the heading 'security migration and citizenship', while the 2017 discretionary budget of the US Department Homeland Security (https://www.dhs.gov/news/2016/02/09/fact-sheet-dhs-fy-2017-budget) summed up to $40.6 billion$.

9 Some example include the infamous WannaCry (deployed in the successful attack against the UK national health system, 2017, referred in Section 3), Stuxnet [first identified in 2010, but widely deployed later to cause control system malfunctions worldwide (Symantec, 2018) included the steel mill malfunction discussed in Section 3], BlackEnergy [deployed in the 2015 attacks against the Ukrainian grid reported in Section 3, Disakil (also suspected to be the cause of the Ukrainian blackouts (Symantec Security Response, 2016)], Industroyer [the cause of further attacks against the Ukrainian grid, 2016 (Cherepanov and Lipovski, 2017)].

10 Over the last 15 years a number of Cyber Security Centres were established in several EU member countries, where an updated approach to securing an industrial ICS is usually available on a service base. Examples are represented by the NCSC in the UK and the Netherlands and the NATO CCDCOE based in Tallin, Estonia. Many more are available on several EU countries, Poland for instance features three such centres, Germany and France one.

11 Like when an equipment certified for the EU market is to be recertified for the North American one, and vice-versa. This is customary for any major product line that control equipment providers manufacture.

12 In that respect this regulation is complemented by COM(2016) 861 (European Commission, 2016), which prescribes that in future, on the proposal of the European Network of Transmission System Operators (ENTSO-E), the EU Agency for the Cooperation of Energy Regulators (ACER) will have to establish cross-border 'system operation regions' [art. 33]. Within ten months after entry into force of the regulation, ENTSO-E must determine – on the basis of its own methodology developed in advance – the 'most relevant electricity crisis scenarios' for each system operation region.

13 Representing 43 TSO over Europe and replacing all previous regional TSOs associations. The regulation will impact stakeholders at large, as the most prominent ones whose assets may impact on the operation of the whole region will be censed so as to be the subject of the regulation.

14 A non-profit organisation supporting to deploy secure European critical energy grids and infrastructure. The ENCS encompasses several large utilities across Europe and worldwide and a number of other partners and partner associations, including the ENTSO-E (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/).

15 see: https://www.entsoe.eu/news-events/announcements/announcements-archive/Pages/News/encs-entsoe-join-forces.aspx.

16 "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" [EECSP, (2017), pp.69–70].