ISSN online: 2282-5665

Consiglio Nazionale delle Ricerche

CERIS ISTITUTO DI RICERCA SULL'IMPRESA E LO SVILUPPO

Novembre

2013

Rapporto tecnico N.47

Considerations on the implementation of SCADA standards on critical infrastructures of power grids

Ugo Finardi, Elena Ragazzi, Alberto Stefanini

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

RAPPORTO TECNICO CNR-CERIS

Anno 8, N° 47; Novembre 2013

Direttore Responsabile

Secondo Rolfo

Direzione e Redazione

CNR-Ceris
Istituto di Ricerca sull'Impresa e lo Sviluppo
Via Real Collegio, 30
10024 Moncalieri (Torino), Italy
Tel. +39 011 6824.911
Fax +39 011 6824.966
segreteria@ceris.cnr.it
www.ceris.cnr.it

Sede di Roma

Via dei Taurini, 19
00185 Roma, Italy
Tel. 06 49937810
Fax 06 49937884

Sede di Milano

Via Bassini, 15
20121 Milano, Italy
tel. 02 23699501
Fax 02 23699530

Segreteria di redazione

Enrico Viarisio
e.viarisio@ceris.cnr.it

ESSENCE

***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment*

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

The Essence project is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.
Networked computers reside at the heart of critical infrastructures, these are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, and expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber security of control and communication systems is now very strong worldwide. To that aim, several frameworks have been developed or are under development at present, both in the form of guidelines and proper standards, but it is difficult to evaluate costs and benefits of their adoption, although experimentation so far has shown that they may be huge.
In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts;
2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;
4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

The results of the study will be published in a series of technical reports, hosted in the “Ceris Technical reports series”. The published titles are:

1. Considerations on the implementation of SCADA standards on critical infrastructures of power grids
2. Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria

Partners of the project are:

CNR-Ceris *(Coordinator) (Italy);* Università del Piemonte Orientale Amedeo Avogadro *(Italy);*
Deloitte Advisory S.l. *(Spain);* Antonio Diu Masferrer Nueva Empresa SLNE *(Spain);*
Enel Ingegneria e Ricerca S.p.A. *(Italy);* Abb S.p.A. – Power systhems division *(Italy);*
IEN - Institute of power engineering *(Poland);* PSE – Operator SA *(Poland).*

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs

Considerations on the implementation of SCADA standards on critical infrastructures of power grids

Ugo Finardi, Elena Ragazzi*, Alberto Stefanini

CNR – CERIS
National Research Council of Italy
Institute for Economic Research on Firms and Growth
Via Real Collegio 30, 10024
Moncalieri (Torino), Italy

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

ABSTRACT**:** Many standards, frameworks or guidelines have been developed for the protection of critical infrastructures. The paper reviews the ones that can directly or indirectly concern the power systems, analyzing their matureness, wideness and specificity of scope, points of strength and weakness. Some challenges facing both policy makers/regulators and firms for their implementation are discussed in the conclusion.

JEL code: L4, L94, O38

Keywords: security, electricity, critical infrastructures, regulation

SUMMARY

1. INTRODUCTION

The Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection provides a concise definition of critical infrastructures:

> *"Critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*.

Annex I of the Directive enlists European Critical Infrastructures: electricity infrastructures and facilities for generation and transmission of electricity in respect of supply electricity stand on the top of the list.[1] The overall vulnerability of the electrical infrastructure appears to be growing due to liberalisation of national markets, growing demand, and the escalation in the transactions among local and regional systems, resulting in an infrastructure that is more complex and difficult to manage. Information & communication technologies promise means for better coping with this increased complexity, but may increase the exposure of the power infrastructure to accidental and malicious failures. Although blackouts so far do not seem to have been influenced by malicious acts, existing vulnerabilities could be exploited by malicious threats as well in the future.

Many sources (e.g. Stefanini et al. [2005], Gheorghe et al [2006], Stefanini & Masera [2008]) argue extensively that design and technology flaws within the information and processing network, may create vulnerabilities easily exploited by antagonists. Standing at the heart of the networked information and control system, Supervisory Control and Data Acquisition (SCADA) systems[2] are used to control both continuous and discrete processes taking place within such facilities. External and internal connections to the system can thus be used to channel malicious attacks to critical infrastructures. The referred works also contain an overview of the context where industrial control systems (ICS) are implemented, and specifically refer the power system. In particular they addresses the topic of how operating power infrastructures depend in a substantial way on their ICS : any (major) failures of the ICS might cause extensive disruption of the service, and massive interruption in energy supply.

The importance of standards in helping to protect process systems, supporting all processes going to specification to procurement, from operation to maintenance, is nowadays assessed as a fundamental security element [Stefanini & Masera, 2008]. Standards set for all stakeholders a common conceptual basis: operators, vendors, certifiers, authorities, can thus foster the development of a market for security products and services.

---

[1] Other examples of such infrastructures are the oil & gas infrastructure, the water supply infrastructure and some large and complex plants, e.g. power, oil and chemicals.

[2] SCADA systems encompass supervisory control, automatic control and data acquisition. According to the IEEE "All control indicating and associated with telemetering equipment at the master station and all of complementary devices at the remote station, or stations." More generally the term may refer the whole range of information systems used to control industrial processes such as manufacturing, product handling, production, and distribution, and as such is a synonym of ICS.

2. KEY CONCEPTS AND HISTORY OF RELEVANT STANDARDS

The **ISO 27002**, whose features are recapitulated in 3.1takes form in the early '90, when the British standard BS 7799 was devised. The rapid advancements in telecommunications, computing hardware and software made available smaller, more powerful and less expensive computing equipment to the small business and the home user. These computers quickly became interconnected through a network generically called the Internet. The rapid growth of electronic data processing and electronic business through the internet required better methods of protecting computers and the information they store, process and transmit. The disciplines of computer security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems. 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.

Meanwhile a set of **Common Criteria** 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. This framework ensures that computer system users can specify their security functional and assurance requirements, vendors can implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. The Common Criteria are stated by the ISO/IEC 15408, an international standard for computer security certification, currently in its version 3.1.

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 [White House, 2007] 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 [CERT 2009].

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, the North American Electricity Reliability Council, the VGB, the European association of large power utility operators, and the WIB, the International Instrument Users' Association initiated work on ICS security. 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.

In the following 3.2, we recapitulate the features of the **NIST 800-53** (now in its 3rd issue), because this was the first official standard issued to address ICS security, so that it became a reference for many industrial end users.

The **NERC CIP** (3.3), the **IEC 62351 (**3.5) and the **VGB guidelines** (4.1) are also reviewed because of the specific focus of our project on power systems protection, while the **WIB report** (4.2) is reviewed because it is agile and relatively easy to implement.
Finally, we review the **ANSI/ISA S99** (3.4) - that the ISA, the International Society of Automation, started to issue in 2007 - because it is the first attempt to provide a generic code of practice in the area of ICSs.

3. SECURITY STANDARDS

3.1 ISO 27002, 27035 and 27036

The **ISO 27002:2005** is a mature, general purpose, code of practice entitled *Information technology - Security techniques - Code of practice for information security* management. It has been developed starting from British Standard BS7799, which had been adopted as ISO/IEC 17799:2000; this standard has been revised (2005), and renumbered (unchanged) in 2007 to align with the other ISO/IEC 27000-series standards. ISO/IEC 27002 provides best practice recommendations on the management of information security to be used by those who have responsibility for initiating, implementing or maintaining information security management systems (ISMS).
Its recommendations encompass the whole life cycle of IT systems:

1. Risk assessment
2. Security policy - management direction
3. Organization of information security - governance of information security
4. Asset management - inventory and classification of information assets
5. Human resources security - security aspects for employees joining, moving and leaving an organization
6. Physical and environmental security - protection of the computer facilities
7. Communications and operations management - management of technical security controls in systems and networks
8. Access control - restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance - building security into applications
10. Information security incident management - anticipating and responding appropriately to information security breaches
11. Business continuity management - protecting, maintaining and recovering business-critical processes and systems
12. Compliance - ensuring conformance with information security policies, standards, laws and regulations

Thus ISO/IEC 27002 has general relevance concerning IT security organization.
Each section specifies and outlines information security controls and their objectives: the former are in general regarded as best practice means of achieving the latter. Nevertheless, as ISO 27002 has general relevance, the process of practical implementation is often not so clear. A Code of Practice ought to be

defined and implemented in each particular field and, moreover, how to ensure and test compliance to the code is not specified. The text anticipates the appearance of industry-specific implementation guidelines are anticipated to give tailored advice to organizations in the most important industrial sectors, e.g. telecom, process control, financial services, healthcare etc.
The topic of ISO 27002 is information security in general. This is a broad field, ramified in all areas of modern organization. Thus this standard is relevant to almost all sectors and branches of an organization (not just SCADA systems but also e.g administrative systems or engineering). This standard is concerned with the security of information assets and not just with IT/systems security per se. Information security is defined within the standard in the context of the C-I-A triad: *the preservation of* ***confidentiality*** *(ensuring that information is accessible only to those authorized to have access),* ***integrity*** *(safeguarding the accuracy and completeness of information and processing methods) and* ***availability*** *(ensuring that authorized users have access to information and associated assets when required).*
In this framework owners of the IT Department (managers who are accountable for the assets) usually charge it of securing information, as being regarded as custodian of the organization's information assets.
The use of the standard requires a common ground across the company applying it also in case when SCADA are different in each installation: ISO 27002 application to SCADA is pertinent only for companies doing so for its whole organization.

3.1.1 Strengths and weaknesses

ISO 27002 presents several critical points. They are analyzed below in some detail.
The "Risk assessment and treatment" section is particularly weak. The logic of the standard is based on a "PDCA" (Plan, Do, Check, Act) approach, but it does not emphasize risk analysis as a key element of the planning stage. Moreover the standard suggests to give the required references in the (parallel) standards ISO/IEC 27001 and 27005.
Finally, no fully accepted risk assessment methods exist for SCADA systems: this can be a further point of weakness of any 27002 application. Two dangers are envisaged: that of poor risk assessment practices by one side, and that of the development of several not fully compatible methods which could hinder any comparison or benchmarking of results.
The "Security policy" section is not always crystal clear and is instead too generic. Some terms, e.g. 'overarching security policy' can be ambiguous when there is need of more detailed policies that cover particular security requirements and controls.
This problem is particularly relevant when it is the case of industrial systems, where discussions are mostly technical. Moreover in this case control systems security policy must be integrated with the installation security policy under the supervision of the SCADA and of the general corporate security policy.
"Ownership of assets" presents a point connected to the key concepts of 'personal accountability' and 'responsibility'. Given the presence in SCADA systems of both physical and digital assets, any possible implementation of 27002 shall clarify the use of 'information assets' concept. Its application to each IT equipment and data content all along the whole network, from the field, through the control network to the corporate network, should be made clear.

"Environmental protection" of IT equipment: the (very particular) settings where SCADA are deployed (much different from typical computer rooms) should be taken in account.
Malicious attacks could be facilitated or even transmitted by environmental sources: this entails the need of specifying environmental security monitoring (electromagnetic fields, fire, water, physical intrusions, power disturbances, etc.). Presumably other standards for this area exist, thus compatibility/co-existence with the security measures should be established.
"User access" management should assess more precisely identification and especially authentication of remote users, federated identity management, etc. The SCADA system must interact with several actors (e.g. maintenance, operational, data handling, etc.) who are not always company employees (from the company owning the installation). Those are often third-parties taking part only on a temporary basis of actions onto the SCADA. This problem expands beyond the single installation to a corporation level.
Section on "Security testing of new/changed application systems": this section has been criticized as not enough comprehensive. This is because, as changes in industrial installations occur on a continuous basis: thus security management must consider this issue, which could be a main means for deploying attacks.
The "Business continuity management" section does not say much about specifying and meeting availability requirements. This is particularly true about the need of considering and when needed provide/improve resilience as well as facilitate recovery.
Problems of this type are particularly relevant in industrials settings, as continuity of operations is essential. Also, concepts such as "contingency" (that is, planning and preparing to cope with incidents that arise if/when other controls fail) present in this section require special explanation. In fact "contingencies" can mean different things for the different involved actors (e.g. manager of the installation, control engineers, etc). When events affecting data (e.g. about the environmental situation of an industrial setting like fumes from a thermal power station) present this can be particularly problematic.
"Incident management" section: this section needs to reflect legal and regulatory regimens which could be different across the EU. Thus different norms affect handling of evidence in digital assets, means and ways for managing document/data retention., etc. The impact of this point is on the discussion in court of evidence on IT equipment and digital data.
The "Information systems audit" section merely covers how to secure audit tools/data.
Auditing control equipment could instead present many difficulties, starting from physical access to equipment. IT auditing in reviewing and making improvement suggestions for the management system has a central value. So this should be discussed in any implementation, and may possibly require interactions, involve specialists in Legal, Risk, Compliance and Governance. This had direct consequences on cost and effort needed for the complete realization of the standard.

3.1.2 ISO/IEC 27032 and 27033 - Cyber security and Network security. State of advancement

ISO/IEC 27032 and 27033 are extensions to 27002 partly published and partly under development, to address cyber and network security specifically. In detail:

Published
ISO/IEC 27032:2012 - Guidelines for cybersecurity
ISO/IEC 27033-1:2009 - Network security -- Part 1: Overview and concepts
ISO/IEC 27033-2:2012 - Network security -- Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3:2010 - Network security - Part 3: Reference networking scenarios -- Threats, design techniques and control issues
Under development
ISO/IEC CD 27033-4 - Network security - Part 4: Securing communications between networks using security gateways
ISO/IEC CD 27033-5 - Network security - Part 5: Securing communications across networks using Virtual Private Network (VPNs)
ISO/IEC NP 27033-6 - Network security - Part 6: Securing IP network access using wireless

3.1.3 The Common Criteria

The **Common Criteria for Information Technology Security Evaluation** (abbreviated as **Common Criteria** or **CC**) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1. It also defines the basic criteria with which the previous standards 27032 and 27033 may be applied.
Subject of CC are:

- Target Of Evaluation **(TOE)** is the product or system that is the subject of the evaluation.
- Protection Profile **(PP)** is a document (generally created by a user or user community), which identifies security requirements for a class of security devices (such as for instance smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose.
- Security Target **(ST)** is the document identifying the security *properties* of the target of evaluation. It may refer to one or more PPs. Thus TOEs are evaluated against the SFRs (see below) established in its ST.
- Security Functional Requirements **(SFRs)**: SFR specify individual security functions which may be provided by a product; CC present a standard catalogue of such functions.
- Security Assurance Requirements **(SARs)**: these are the descriptions of the measures taken during the process of development and evaluation of the product, in order to assure compliance with the claimed security functionality.

- Evaluation Assurance Level **(EAL)** is the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to SARscovering the complete development of a product, with a given level of strictness. In CC are listed seven levels of EAL, going from 1 (the lowest) to 7 (the most strict and expensive).
- Most PPs and most evaluated STs/certified products have been for IT components (e.g., firewalls, operating systems, smart cards).

3.2 NIST 800-53

The National Institute of Standards and Technology is the US federal technology agency that develops and promotes measurement, standards, and technology. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. The overall goal of the series is to provide a unified information security framework for the US federal government and its contractors.

The Federal Information Security Management Act of 2002 (FISMA) directed federal agencies to promulgate federal standards for: (i) the security categorization of federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, mandates that agencies specify minimum security requirements for federal information and information systems. [Abrams, 2007].

NIST 800-53 implements the FISMA mandate by providing guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the US federal government. The 800-53 guidelines are well consolidated since publication of the first release, dating back to Dec. 2006. The current release 3 was issued on August 2009 [NIST 2009]. The basic plant of those guidelines resembles the one of ISO/IEC 17799 and the successor standard ISO 27002, although requirements range on a broader set of topics:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection

- Planning Management
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

What makes NIST 800-53 especially interesting is its considerable maturity, which makes it an applicable reference for industrial and business organizations, well beyond the intended scope of the standard, i.e. the US federal government agencies and their contractors.

3.2.1 Strengths and weaknesses

A remarkable feature of the 800-53 is that its Appendix D provides the security control baselines that represent the starting point in determining the security controls for *low-impact*, *moderate-impact*, and *high-impact* information systems. The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines. Respective controls are identified for each baseline in a control catalog. Control enhancements, when used to supplement security controls, are indicated by the number of the control enhancement. Some security controls and enhancements in the security control catalog are not used in any of the baselines in this appendix but are available for use by organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risk to organizational operations and organizational assets, individuals, other organizations, and the nation. Correspondingly, appendices F and G detail the controls to apply. Hence, although the NIST 800-53 in general terms is suggesting an approach to risk assessment not unlike from the one of ISO 27002, it also provides an easy way to identify controls and controls enhancements for each system, once its impact is categorised. This overcomes the difficulties related to a generic risk assessment methodology we reported in the previous section.

Furthermore the quoted NIST site also provides a well articulated guidance to assessing the Security Controls specified by SP 800-53 [NIST 2008] through a set of exemplary cases. The purpose is to present the specific actions an assessor might perform in order to obtain the evidence necessary for making the determinations identified in the assessment procedures in NIST Special Publication 800-53A. Those assessment procedures have been developed by NIST to assist organizations in determining the effectiveness of the security controls in their information systems. For each of the control areas in the range specified by 800-53, a set of specific controls can be downloaded from the site. We may conclude that, different from ISO 27002, NIST 800-53 fully specifies appropriate compliance procedures.

The third remarkable feature of NIST 800-53 is that its Appendix I provides supplemental guidance to tailor security controls to Industrial Control Systems. Tailoring guidance for ICS includes scoping guidance and the application of compensating security controls. Due to their unique features, these systems may require a greater use of compensating security controls than is the case for general-purpose information systems. In situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are

adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed. The security controls and control enhancements further listed in Appendix I are likely candidates for tailoring with the applicability of scoping guidance indicated for each control/enhancement.

3.3 NERC CIP

NERC Standards CIP-001 through CIP-009 are closely connected to the reliable operation support of bulk Electric Systems, providing a cyber security framework for the identification and protection of Critical Cyber Assets[3]. Current NERC framework recognizes the roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Electric System reliability, and the risks to which they are exposed. Standards incorporate a risk-based approach for implementation.
Appendix A contains a further description of the path leading to NERC CIP standards.
NERC CIP standards are constantly revised and implemented. Table 1 contains data on the different standards: most up-to-date version, date of issuing, title (topic) of the specific standard.

Table 1 – most up-to-date version of NERC-CIP 002/009 standards (as of October 9th, 2012)

Standard	Version	Date	Title (all listed under "Cyber Security")
CIP-001	2a	February 16th, 2011	Sabotage Reporting
CIP-002	4a	May 9th, 2012	Critical Cyber Asset Identification
CIP-003	4	January 24th, 2011	Security Management Controls
CIP-004	4a	May 24th, 2012	Personnel & Training
CIP-005	4a	January 24th, 2011	Electronic Security Perimeter(s)
CIP-006	4d	February 9th, 2012	Physical Security of Critical Cyber Assets
CIP-007	4	January 24th, 2011	Systems Security Management
CIP-008	4	January 24th, 2011	Incident Reporting and Response Planning
CIP-009	4	January 24th, 2011	Recovery Plans for Critical Cyber Assets

Reliability Standards CIP 001 to CIP 009 apply to the following entities in the sector:

- Reliability coordinators
- Balancing authorities
- Interchange authorities
- Transmission service providers
- Transmission owners
- Transmission operators

[3] NERC CIP-002/009 supersede NERC predecessor standards (1200 and 1300) first issued since 2003

- Generator owners
- Generator operators
- Load serving entities
- NERC
- Regional Reliability Organizations

The application of the standards is enforced by NERC through Responsible Entities identified by the Implementation Plan provided by the same NERC [2006] joint with the set of Standards.
Those entities are allowed to self-certify on a semi-annual basis until compliance due dates are reached; there was a three-year timeframe for compliance. According to the 2008-2010 Reliability Standards Development Plan (created by NERC in 2007) and implying the revision of the NERC CIP 001-009, standards should have been tested to meet the following ten objectives:

1. Applicability
2. Purpose
3. Performance requirements
4. Measurability
5. Technical basis in engineering and operations
6. Completeness
7. Consequence for noncompliance
8. Clear language
9. Practicality
10. Consistent terminology

Consequently the original cyber security project was delayed by one year (first target for 100% compliancy of electricity sector was the end of 2010).
This is indicative of persistent difficulties in the clarity of objectives of the NERC CIP: this, together with the exclusively North American scope of those standards, implies that a deep review should be performed before appliance in the EU. Moreover, NERC standards miss to prescribe a precise compliance method: as there is no compliance metrics, it is difficult to estimate the compliance costs; it is also argued that the estimates realized by GAO [2007a], [2008] on refurbishments gathering of information on SCADA may be largely defective.
According to Abrams [2007] many NERC CIP requirements are a subset of the Moderate Baseline set of controls in NIST SP 800-53: in his opinion this subset is inadequate for the protection of critical national infrastructures and more in general for all electric energy systems, especially considering possible impact of regional and national power outages.
Nevertheless, NERC-CIP standards are all enforced in the US and in the Canadian province of Ontario as of October 9th, 2012 according to table 2 below.

Table 2 – Enforcement of NERC-CIP 002/009 standards in the US and in Ontario

Standard	Enforcement Date (US)	Standard	Enforcement Date (Ontario)
001-2a	October 1st, 2011	001-2a	January 6th, 2012
002-3	October 1st, 2010	002-3	January 1st, 2011
003-3	October 1st, 2010	003-3	January 1st, 2011
004-3a	December 12th, 2012	004-3	January 1st, 2011
005-3a	February 2nd, 2011	005-3a	April 1st, 2011
006-3c	May 19th, 2011	006-3c	April 1st, 2011
007-3	October 1st, 2010	007-3	January 1st, 2011
008-3	October 1st, 2010	008-3	January 1st, 2011
009-3	October 1st, 2010	009-3	January 1st, 2011

3.3.1 Strengths and weaknesses

Main Criticisms to NERC CIP 001-009

- adoption cumbersome and costly, so that small companies prefer to pay fines
- practical tests have shown some inadequacy in terms of clarity and consistency of terminology
- they miss to prescribe a precise compliance method
- they would require substantial review in order to fit a European context

3.4 ANSI/ISA 99 and IEC 62443

The topic of **ANSI/ISA S99** is *Security Guidelines and User Resources for Industrial Automation and Control Systems*, being thus strongly related to the topic of this work. In this framework (originated in the US) several standards exist so far. Here below table 3 contains the list of standards that are published, approved, proposed, under development [4].

ISA 99 considers compliance metrics as an important key issue. Their use can allow the measure of the increased security. This in turn might lead to an implementation of standards of cyber security that is not cost related. in fact revenues should be increased to cover the added costs of security, or instead savings in other cost items must be realized. Both approaches result in a security cost offset: in this way security deployment is cost neutral. ISA 99 standards are also submitted to IEC to be approved as **IEC 62443** standards, elaborated by the IEC TC65/WG10, regarding *Security for industrial process measurement and control*, and which are expected to conform quite fully to ISA 99. table 1 contains also data on IEC references of the standard.

[4] This standards list has been retrieved on October 2012 from ISA website, http://www.isa.org, in the ISA 99 wiki, http://isa99.isa.org/ISA99%20Wiki/Home.aspx; a further webpage dedicated to ISA 99 is: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

3.4.1 Strengths and weaknesses

As only a part of ISA framework has been approved, it is not possible to evaluate how much it will differ from the most mature standard released so far, NIST 800-53.
An important concern regards the relatively narrow constituency behind both standards: this should be broadened in order to stimulate take up of the outcomes by the process industry at large, so as to make this set of standards a successful endeavor.

Table 3 – ISA 99 Standards

ISA Reference	IEC Reference	Title	Status	Comments
ISA-TR62443-0-3		Gap assessment of ANSI/ISA-99.02.01-2009	Approved	
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published,	
Under Revision	Current edition published as ANSI/ISA-99.00.01-2007			
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Proposed	Content is under development on the Wiki
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development	
ISA-62443-1-4	IEC/TR 62443-1-4	IACS security life cycle and use case	Proposed	
ISA-62443-2-1	IEC 62443-2-1	IACS security management system - Requirements	Published,	
Under Revision	Current edition published as ANSI/ISA-99.02.01-2009			
ISA-62443-2-2	IEC 62443-2-2	IACS security management system - Implementation guidance	Proposed	
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment	Proposed	
ISA-62443-2-4	IEC 62443-2-4	Certification of IACS supplier security policies and practices	Proposed	Proposed as a national modification to the IEC standard.
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS	Published	Current edition published as ANSI/ISA-TR99.00.01-2007
ISA-62443-3-2	IEC 62443-3-2	Security assurance levels for zones and conduits	Under Development	
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security assurance levels	Approved	Previously numbered ISA-99.01.03
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	Under Development	
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components	Under Development	

3.5 IEC 62351 Technical Specification "Data and communication security"

IEC 62351 has been developed by Work Group 15 (Data & Communication Security) of the IEC Technical Committee 57, which is responsible for developing standards for information exchange for power systems and other related systems (such as Energy Management Systems, SCADA etc.). Its scope is information security for power system control operations. Its primary objective is to undertake the development of standards for security of the communication protocols defined by IEC TC 57. Specifically such protocols are: the IEC 60870-5 series; the IEC 60870-6 series; the IEC 61850 series; the IEC 61970 series; the IEC 61968 series.

Specifications of the standard are the following ones, all listed under "Power systems management and associated information exchange - Data and communications security:

IEC 62351-1 - Part 1: Communication network and system security - Introduction to security issues

IEC 62351-2 - Part 2: Glossary of terms

IEC 62351-3 - Part 3: Communication network and system security - Profiles including TCP/IP

IEC 62351-4 - Part 4: Profiles including MMS

IEC 62351-5 - Part 5: Security for IEC 60870-5 and derivatives

IEC 62351-6 - Part 6: Security for IEC 61850

IEC 62351-7 - Part 7: Network and system management (NSM) data object models

Besides these parts another one is still a work in progress:

IEC/TS 62351-8 - Part 8: Role-based access control

According to the abstracts (source: IEC website, page http://www.iec.ch/smartgrid/standards/ and herein, accessed October 2012) the purposes of the parts are the following:

Part 1: introduces the reader to information security as applied to power system operations.

Part 2: covers the key terms used in the IEC 62351 series. This list is not meant to be definitive. It also must be noted that most cyber security terms are formally defined by other standards organizations, thus reference is provided here.

Part 3: specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols making use of TCP/IP as a message transport layer.

Part 4: specifies procedures, protocol extensions, and algorithms to facilitate securing ISO 9506 - Manufacturing Message Specification (MMS) based applications. This technical specification should be referenced as a normative part of other IEC TC 57 standards that have the need for using MMS in a secure manner.

Part 5: specifies messages, procedures and algorithms for securing the operation of protocols based on/derived from the IEC 60870-5 standard: Telecontrol equipment and systems - Part 5: Transmission protocols. More specifically it applies to IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104

Part 6: specifies messages, procedures, and algorithms for securing the operation of all protocols based on/derived from IEC 61850 standard. This part applies to at least the protocols of IEC 61850-8-1, IEC 61850-9-2 and IEC 61850-6.

Part 7: defines those network and system management (NSM) data object models that are specific to power system operations. These NSM data objects are used to: monitor the health of networks and systems; detect possible security intrusions; manage the performance and reliability of the information infrastructure.

3.5.1 Strengths and weaknesses

The IEC 62351 are a set of standards for information exchange among power systems and other related systems (such as Energy Management Systems, SCADA etc.). Their scope is information security for power system control operations. Several IEC 62351 guidelines are still under development.

4. SECURITY GUIDELINES

Several guidelines were developed in the early 2000 by either standard organisations or sector associations, like the:

- ISO/PAS 22399:2007 [ISO/PAS 2007] presenting the general principles and elements for incident preparedness and operational continuity of an organization,
- the API 1402 [API 2005], issued by the American Petroleum Institute to provide operators with a description of industry practices in SCADA Security, and provide a framework for developing sound security practices within the operators individual companies,
- the Guidance for Addressing Cyber Security in the Chemical Industry – V. 3-0 [AGA, 2006 , issued by AGA, the American Gas Association.

Most of these guidelines appear irrelevant to the scope of our project, or issued by American associations, or both. Thus we limit ourselves to quote here two guidelines only, the VGB R 175 [VGB, 2006] and the WIB Report M2784-X-10, because they were issued by European or international organisations, and appear fully relevant to the scope of ESSENCE. They appear to have a more limited scope of the previously quoted standards, however, within this application scope, they appear reasonably complete and applicable.

4.1 VGB R175

This guideline - guideline R175 – was issued in 2006 by **VGB -** Vereinigung der Großkraftwerks-Betreiber**,** the European association of large power utility operators. It concerns *IT security for power plants* and its aim is providing power plants operators with recommendations and hints on how they could improve IT security [VGB, 2006].

VGB R175 is focused on the functionality of those instrumentation and systems of control that are necessary to control power plants, with the aim of protecting against IT systems threats; this is one of the few European attempts to tackle this issue. This guideline also provides hints on how IT administration and IT systems should be organized themselves.

It is expected that VGB is requiring to implement the guideline to instrumentation and control systems manufacturers and suppliers, in order to offer solutions for the specific power plants requirements, and that it is going to realize them together with the operators.

4.2 WIB Report M2784-X-10

Report M2784-X-10 was produced by the Plant security working group of WIB, an international instrument users' association collaborating in sponsoring, planning and organization of instrument evaluation programs. It was first issued in march 2010 [WIB 2010].
Scope of the report is to specify requirements and to give recommendations for IT security that have to be fulfilled by vendors of systems for process control and automation.
It covers both policy (addressing vendor's organization, IT security processes, technological solutions and IT security governance) and commissioning and maintenance.
It is divided into several section, each addressing a specific topic. In order to explore its topics it is useful to consult its detailed table of contents:

1. INTRODUCTION
    - 1.1 Scope
    - 1.2 Distribution, intended use and regulatory consideration
    - 1.3 Definitions
    - 1.4 Cross-references
    - 1.5 Process safety requirements
2. GENERAL SECURITY POLICY
    - 2.1 Demonstrating compatibility via independent certification
    - 2.2 Security application
3. PROCESS CONTROL SECURITY FOCAL POINT
4. CONTROLS AGAINST MALICIOUS CODE
5. SOFTWARE PATCH MANAGEMENT
6. SYSTEM HARDENING
7. PROTECTION OF PCD DOCUMENTATION
8. ACCOUNT MANAGEMENT
9. BACKUP, RESTORE AND DISASTER RECOVERY
10. REMOTE ACCESS AND TRANSFER OF DATA FILES
11. WIRELESS CONNECTIVITY
12. SECURE CONNECTIONS TO SIS (SAFETY INSTRUMENTED SYSTEMS)
13. STANDARDS AND CERTIFICATION
14. SECURITY MONITORING
15. PROCESS CONTROL DOMAIN NETWORK ARCHITECTURE

16. HANDLING OF REMOTE AND ADVISORY SETPOINTS

17. DATA HISTORIANS

18. COMMISSIONING AND MAINTENANCE

5. SUMMARY

In summary, we compared seven standards or guidelines:

- ISO 27002: it is a general purpose code of practice for *information security management*. Pros: it is a very general and mature standard. Cons: there are reserves on its risk management approach making it rather un-applicable to real-time applications and to SCADA systems in particular; it needs to be adapted to a specific industry sector to envisage appropriate compliance mechanisms.
- The NIST 800-53 provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the US federal government. Contrary to the other guidelines and standards considered hereinafter, the NIST 800-53 does not stem out from the collective effort of a panel of experts in view of the needs of an industrial sector, it was elaborated to meet the requests of the US federal government. The 800-53 guidelines are well consolidated since publication of the first release, dating back to Dec. 2006. They include an elaborated framework where specific controls are provided for a broad number of areas, in view of the impact of the information system considered. A compliance assessment methodology is clearly specified. Moreover the NIST 800-53 include an Appendix where their controls framework is adapted to the requirements of ICS, and additional controls are suggested. Although it is the only mature reference available, there are reserves about the adequacy of the standard, especially as far as ICSs are considered
- NERC guidelines: such guidelines were originated by sector associations in the power industry; they focus on Bulk Power System Members of the originating organization, which are mainly from the US. Pros: NERC guidelines are already compulsory in the US, and are thus Standards in a proper sense (their implementation is enforced by the NERC itself through Responsible Entities[5]). Cons: NERC guidelines implementation has shown some inadequacy in terms of clarity and consistency of terminology; they miss to prescribe a precise compliance method; finally, they are exclusively North American and would require substantial review in order to fit a European context.

[5] This fact did involve a change of status from a consulting body (the North American Electricity Reliability Council) to an Electricity Reliability Organization (the North American Electricity Reliability Corporation). NERC now plays an official role about issuing and ensuring compliance of security related standards.

- IEC 62351 Technical Specification "Data and communication security": the IEC 62351 guidelines have been specifically devised for the security of information exchange of power systems. They are thus rather specific for the purpose. Being still under development they have not been adopted as far as now.
- ANSI/ISA S99 and IEC 62443: they are about *Security for Industrial Automation and Control*; thus they will probably provide a generic code of practice in this area. Pros: at this stage they look the most appropriate attempt to provide a standard ensuring SCADA security. Cons: they are rather immature in their development; constituency of the standards appears quite limited.
- VGB guidelines: such guidelines were originated by sector associations in the power industry, predominantly German, and focus on Power Plant controls. Although considerable because they fill an existing niche, VGB R175 are thus quite clearly a very limited framework, both in terms of constituency and in terms of scope.
- WIB Report M2784-X-10: "Process Control Domain Security Requirements for Vendors" are a general set of guidelines for IT security to be fulfilled by vendors of such systems only.

To make the comparison between standards easier, the Table 4 below gives a review of their main features.

Table 4 – summary of Standards

Standard	**ISO 27002**	**NIST 800-53**	**NERC CIP**	**ANSI/ISA 99 and IEC 62443**	**IEC 62351**
Summary	The ISO/IEC 27002 is a general purpose code of practice for the security of information technologies. It is not specific for power grid security, but it's being adopted by IEC. It is thus useful for those who are entitled of the security management of information systems. As far as now it has not been adopted or made compulsive.	NIST 800-53 is a set of general guidelines on information system security, and resembles ISO 27002 in its basic plant. It is not specific for power systems. It is thus useful for the general It is thus useful for those who are entitled of the security management of information systems. As far as now it has not been made compulsive, but being rather assessed could have been adopted by enterprises/bodies managing power grids.	NERC-CIP standards are a set of standards specifically studied for the cyber security of power grids. They are thus useful for the owner/manager of such infrastructure. They have been made compulsive – and thus adopted – in the US and in the Canadian province of Ontario.	ANSI/ISA 99/IEC 62443A are a set of guidelines for the security of automation and control system. They are thus of very general use, but encompass also SCADA systems and are thus of utility for power grid cyber security. Being still under development they are not to our knowledge in use or adopted.	IEC 62351 guidelines have been specifically devised for the security of information exchange of power systems. They are thus rather specific for the purpose. Being still under development they have not been adopted as far as now.
Used by	Applied through national regulations	Compulsory for US Govt. contractors.	USA and Ontario	Not yet defined	Applied by the power equipment manufacturers on a voluntary basis.
Applicability	Mature	Rev. 4 published februarry 5th, 2013 as draft.	First Issued in 2003 and subsequently revised	Under development. ISA 99.00.01 issued late in 2007. ISA 99.00.02 issued late in 2008	Set of standards managed by IEC TC 57. Several issues until present date.
Application range	Generic for any IT system	Specific to ICSs	Specific to North American power systems	opp. Specific to ICSs	Specific to power system equipment

Standard	ISO 27002	NIST 800-53	NERC CIP	ANSI/ISA 99 and IEC 62443	IEC 62351
Strenghts/ Weaknesses	**Weaknesses**: "Risk assessment and treatment" section is particularly weak: it does not emphasize risk analysis as a key element. "Security policy" section is too generic. Some terms can be ambiguous. "Ownership of assets" presents a point connected to the key concepts of 'personal accountability' and 'responsibility'. “Environmental protection” of IT equipment: the (very particular) settings where SCADA are deployed (much different from typical computer rooms) should be taken in account; malicious attacks could be facilitated or even transmitted by environmental sources. "User access" management should assess more precisely identification and especially authentication of remote users, federated identity management, etc. “Security testing of new/changed application systems”: this section has been criticized as not enough comprehensive. The "Business continuity management" section does not say much about specifying and meeting availability requirements. The "Information systems audit" section merely covers how to secure audit tools/data.	**Strenghts:** Appendix D provides the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems. Correspondingly, appendices F and G detail the controls to apply. Hence, although the NIST 800-53 in general terms is suggesting an approach to risk assessment not unlike from the one of ISO 27002, it also provides an easy way to identify controls and controls enhancements for each system, once its impact is categorised. This overcomes the difficulties related to a generic risk assessment methodology we reported in the previous section. Furthermore the quoted NIST site also provides a well articulated guidance to assessing the Security Controls specified by SP 800-53 [NIST 2008] through a set of exemplary cases. We may conclude that, different from ISO 27002, NIST 800-53 fully specifies appropriate compliance procedures. The third remarkable feature of NIST 800-53 is that its Appendix I provides supplemental guidance to tailor security controls to Industrial Control Systems.	**Main Criticisms:** adoption cumbersome and costly, so that small companies prefer to pay fines; practical tests have shown some inadequacy in terms of clarity and consistency of terminology; they miss to prescribe a precise compliance method; they would require substantial review in order to fit a European context.	As only a part of ISA framework has been approved, it is not possible to evaluate how much it will differ from the most mature standard released so far, NIST 800-53. An important concern regards the relatively narrow constituency behind both standards: this should be broadened in order to stimulate take up of the outcomes by the process industry at large, so as to make this set of standards a successful endeavor.	The IEC 62351 are a set of standards for information exchange among power systems and other related systems (such as Energy Management Systems, SCADA etc.). Their scope is information security for power system control operations. Several IEC 62351 guidelines are still under development.

6. CONSIDERATIONS ON THE IMPLEMENTATION OF SCADA SECURITY STANDARDS IN EUROPE

There are two issues to be tackled when considering for implementation the security standards overviewed in chapter 3 and 4:

- The socio-economic impact of the application of those standards
- The implementation mechanisms that could be put in place.

On the first issue, the implementation process of the NERC standards overviewed in chapter 9 is quite telling:

The implementation of security standards comes at a considerable cost for private enterprises. The GAO cost report on the Mandatory Reliability Standards for Critical Infrastructure Protection estimates the cost for information gathering requirements to amount to more than $100 million [GAO, 2008]. This does not even take into account the cost of actual implementation expenses associated with compliance.

About 1,000 entities within the US electricity sector need to comply with Mandatory Reliability Standards for Critical Infrastructure Protection. 85% of those companies are private enterprises. If information gathering costs is 10% of total compliance cost, then each entity is looking at a cost of 1 million dollars or more. About 60% of these entities are classified as small businesses and a security expense of 1 million dollars or more might not be economically feasible.

The resistance to complying with voluntary standards created by NERC was probably due to the high price of compliance. For the second quarter of 2007, 3,412 violations were self-reported [NERC, 2007a]. To counteract this scenario the penalty fees set by FERC amount to a maximum of 1 million dollars per day [GAO, 2007a].

Although the financial risks of sharing critical infrastructure information can be determined, the benefits are not easy to determine for the private sector [GAO, 2004a]. According to the report *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*, attacks on control systems (i.e., SCADA) are increasing [Byres & Lowe, 2004]. According to this report 70% of cyber attacks originate from an exterior source. This report also stated cyber attacks were under reported by a ratio of 1 to 10. The consequences of successful cyber attacks reported by Byres & Lowe [2004] are monetary losses of over a million dollars (50% of the cases) and loss of control of the physical facilities (29% of cases). However, those data are regarded with skepticism by other sources. This is confirmed by the E-Crime Survey conducted in 2007 [CSO Magazine, U.S. Secret Service, CERT Program, & Microsoft Corporation, 2007]. The E-Crime Survey shows a 12% increase in electronic crime was experienced along with a 5% decrease in information technology security spending. This survey also noted that many electronic crimes were not reported due to negative publicity (22%) and due to the fear that competitors would use that information to their advantage (13%). A more complete and updated review of attack scenarios to the electrical critical infrastructures will be the object of the second Essence Technical Report: "Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria", by Fernando García, Andrés Cortes, Hanna Bartoszewicz-Burczy, Daniela Pestonesi, Tadeusz Włodarczyk and Marco Alessi.

The US experience, the only existing experience of generalised adoption of a security framework up to now, highlights then the fact that implementation of security standards implies affording huge costs, which are hardly quantifiable before the adoption.

The resistance practiced by many firms shows that the implementation process has to be designed, to ensure a correct sharing of costs, corresponding to benefits. Benefits are difficult to assess as well and are, above-all, for a large part public collective benefits.

The EU power system is likely less fragmented that the US one. A large majority of the players in the sector - power producers, transmission system operators and distribution utilities - are large companies. This is likely to make implementation of cyber security measures less awkward than it proved in the USA. Application of any of the mentioned standards in the power sector at large would involve a small number of SMEs. Of course the structure of the electricity system in Europe is progressively evolving, due to the increase of competition in many countries, to the diffusion of dispersed small and micro plants by renewable sources, and to the new challenges linked to the smart grid scenario[6], but it remains true that critical infrastructures remain concentrated in the hands of a few big operators. This is even more true in the case of critical infrastructures as defined by the Directive 2008/114/EC of 8 December 2008 (they must concern at least two European countries to be so defined) which would definitely involve only a few SMEs, if any. Moreover, although with the introduction of competition in the generation and trading phases many private operators have appeared[7], the networked phases of the utility (transmission and distribution) are still publicly controlled and public actors have still a dominant role in many countries. This implies that the problem of the sharing of the cost of implementation facing a mix of private and public benefits is less difficult to afford. Finally, since some big operators have already adopted on a voluntary basis a security policy, the actual situation is a little bit different than in the USA. In a sense, some advances have already been made, but there are also negative implications of this unregulated and uneven investment on security standards. Firstly it is clearly more difficult to reach an agreement on a common framework for all European operators, since different choices could have been made; secondly to upgrade a security system is often very costly, and not always possible, with respect to the investment necessary to build a brand new system for a new electricity facility.

It is difficult to forecast whether the adoption of S99/IEC 62443 should involve similar costs as the NERC guidelines, because not all the normative technical controls those standards shall specify are defined by now. The ISO 27000, having a substantially broader scope, may involve a broader cost. It must be remarked that regarding ISO 27000, a self assessment tool to estimate such costs is provided by *http://17799.cryptovb.com/iso17799-ImpactAnalysis.htm*). Concerning the NIST 800-53, the cost basically depends on the impact associated to the considered system. According to some experience made by EU organisations that voluntarily complied to NIST 800-53, however, implementation costs for an organisation in charge of high impact systems exceeded by almost an order of magnitude those estimated by GAO relevant to NERC guidelines (i.e, costs over 5 M€ vs. 1 M$)

[6] It is nevertheless true that the change from a vertically controller unidirectional electrical system, to a smart system, with aleatory flows and dispersed control increases also the complexity of security controls.

[7] The level of real competition and the structure of the market may vary a lot among countries.

It is likely that the impact analysis on the EU power sector ESSENCE shall perform may confirm figures in the order of those mentioned in Appendix A (Control systems cost 3-4 billion dollars for the electric grid. Remote field devices cost 1.5-2.5 billion dollars to replace [GAO, 2007a]. Retrofitting an existing SCADA system is also probably an expensive expenditure (estimated 1/2 – 1 million dollars). Nevertheless, such an impact analysis may lack an objective basis to forecast such costs in the absence of a precise compliance metrics to refer.

Concerning the implementation process in the EU, different implementation processes could be envisaged in principle ranging from voluntary to completely mandatory. Concerning totally voluntary mechanisms, their limitation were shown by the earlier US experience with CIP NERC. It is unlikely that sector specific guidelines may have a broad take up in Europe, where the power sector (for instance) is quite totally privatised, although the share of small & medium enterprises on the total should substantially differ from the US one. On specific sectors like the power system, voluntary application of standards needs to be ascertained in view of its impact on reliability: auditing processes under responsibility of national regulators appears to be a sensible way to proceed.

7. CONCLUSIONS

In conclusion, the following issues appear to withstand:

- No mature framework for a coordinated industry-wide implementation of ICSs securityexists as of yet; the closer to attain such goal appears to be the convergent product by ISA SG 99 and IEC TC65/WG10. However this would not come before 2014; and the constituency of such working groups appears too restricted yet to ensure a broad take up.
- The NIST 800-53 appears the only mature and fully specified framework available so far. It is an adaption of a broader scope standardto ICSs, and initially doubts were raised about the adequacy and the completeness of this adaption. However so far it was applied (in a compulsory way) to US government contractors withouth many complains. Moreover, some large EU stakeholders have adopted it on a voluntary basis because it is fairly clear and straightforward to apply.
- The NERC CIP standards only fit the bulk power system. They appear anyway defective because their terminology still is to some extent unclear; moreover they lack a precise compliance metrics, and their US origin may redder any attempt to fit them to the European landscape quite awkward.
- In the absence of such a compliance metrics, it is difficult to predict whether the costs for cyber security implementation forecast by GAO [2007a], [2008] may be confirmed for Europe. Any impact analysis (whether restricted to European critical infrastructures or to the power sector at large) may lack precision. More generally, this issue needs to be solved prior that proper implementation mechanisms can be prescribed.

In those conditions, the following recommendations can be made:

- Concerning the bulk power system, the ESSENCE case studies will reveal:
  a) to which extent that framework is applicable to EU power systems, and
  b) whether the lack of compliance metrics seriously hampers its application.
- In case our reply to question a) is positive, and negative to question b), a serious attempt should be made to develop in the EU a NERC-like approach to SCADA security. An issue deserves special attention: envisaging an appropriate implementation mechanism. Such attempt needs to involve European stakeholders (power generation and distribution companies, transmission system operators and national energy authorities). The role of ENTSOE, the European Association of Transmission Systems Operators, might be substantial concerning the first issue, which involves identifying who should comply and which way compliance should be assessed and enforced. A panel of experts from the current working groups involved in the discussion of the other standards mentioned in chapter 3 should also be involved.
- Concerning the ICSs security sector in general, there is a need to foster a convergence process in between industry and decision/policy makers, where ENTSOE, other industrial associations and European standard organizations like the CEN may play an important role. Promoting a CEN workshop on the subject is a practical way to initiate a public-private partnership initiative aimed at this objective, and at tackling meanwhile the pending issues that hamper deployment of those standards. On a technical standpoint, the most promising approach may come from a joint work of the working groups in charge of ISA 99 and IEC 62443. To this aim, we recommend to find incentives so as to:
  - increase participation in ISA-99 and IEC 62443 and add to the critical mass needed to develop the base material for each standard;
  - harmonize the administrative/editorial differences between ISA99 and IEC so that ballots for are executed in parallel, and not sequentially. If funds are available to facilitate this harmonization, it will have significant pay-off in terms of shortening the time to release the standards.

8. OPEN ISSUES IN VIEW OF THE CASE STUDY DESIGN AND EVALUATION

It is important to summarize here all the question marks and key points gathered in the report, that must be considered when fixing an agenda for the case study implementation, but also more in general when evaluating which standard to implement and how. These key points concern the feasibility taking in consideration of the actual situation of national systems, the implementation process and the regulatory aspect.

8.1 How to decide which standard suits more?

Technical feasibility in the European context must take into account the different technical features of European systems (size, reliability, endowment) and the heterogeneity in these systems.
The difference in the physical characteristics of systems is accompanied by some heterogeneity in regulation and market asset. In particular these concern:

- Different national market structure
- Different role of public firms
- Different national regulation although in a common framework established by the UE.

Finally it must be considered the public attitude towards risk:
In EU less stress is given to risk related to terrorism, respect to the US, even though this attitude is now changing.
Even apart from terrorism related risks, the electricity system felt as more reliable but, on the other hand, lot of stress put on environment protection and on safety for citizens.

8.2 Which implementation process in the EU?

The different standards and guidelines reviewed imply different levels of tightness in the application, and of invasive control. For this reason the implementation process must be designed together with the choice of the standard. The following options may be considered:

- Voluntary
- Voluntary with auditing mechanism by country and sector: e.g. national regulators follow the companies that declare the application of standards
- Voluntary with economic incentives given to actors which are going to invest and/or experiment (with public feedback)
- Mandatory at national level in sectors/installations recognized as critical infrastructures. Responsibility can be given to government or to industrial associations;
- Mandatory to entire sectors, e.g. power
- Mandatory at European level

The more the enforcement is mandatory, the more it will be difficult to converge to a single common European standard, because of the lack of a single transnational authority empowered to impose the choice of the standard on all agents involved. On the other hand organisms charged to find a common path agreed by all operators will hardly succeed in their task, at least in a short term, because of diverging interests. One different solution to assess would be to allow or multiple national experimentations, respecting some minimum and common requirements, and converging (maybe) in the long term to a common technological path.

8.3 Who should pay for standard implementation?

The cost of standard implementation holds on facility owners, while benefits are shared between owners (less insurance costs, lower fee probability for service interruption, improvement of company image) and the public at the large (electricity being a pervasive input, a black-out can hamper firm activity and private style of life in an heavy way).

From an economic point of view this is related to the theory of public goods (goods whose benefits cannot be denied to consumers not paying for them) and to that of standards (it is not sure that the prevailing standard in case of *laissez-faire* is the best one, but it depends on the first comer, or on who is the firm, generally the one with more market power, keen to invest more in being the first comer or more in general the one able to impose its own standard). Both elements are indications for public policy. In particular confirm that a voluntary implementation could lead to unsatisfactory results, and that the public regulator must afford the problem of the financing of this investment.

The regulator can choose in a mix of instruments based on incentives (direct grants or mark-ups on the market tariff) and on penalties in case of default.

The amount of incentive necessary is linked also to a point touched in 8.1, that is public perception of risk. Apart the fear of terroristic attacks, there is also the problem of the low perceived relevance of future risks. Individuals are generally insufficiently keen to pay today to cover uncertain future needs or costs. A long past experience of reliability in electricity supply will reinforce this under-evaluation of the cost of a possible future black-out.

The decision will also be linked to the total real cost of implementation (which is the object of the Essence project) and with the type of risk and of risk prevention (which will be considered in the report on the attack scenarios). Moreover also the completeness of the standard coverage is important too: only transmission, dispatchment and big plant management or all remote control devices?

9. APPENDIX A - NERC CIP STANDARDS: DEVELOPMENT AND IMPLEMENTATION IN THE UNITED STATES

A vivid review of what happened related to security of the Bulk electric system in the US is depicted by Marianne Hoebich [2008][8]. This thesis provides an 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 lessons coming from that experience give many highlights on the implementation path and on the choice of standards to be applied, so it is useful to quickly review them.

The Hoebich survey makes a 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 respective roles are presented as such:

- *NERC provides direction to the electricity sector in regards to improving the reliability of the bulk-power grid system. NERC encouraged the adoption of reliability measures by providing plans, guidelines, standards, training, and education. NERC's reliability measures were voluntary until 2005. A major blackout in 2003 resulted in FERC empowering NERC to develop and enforce reliability standards (North American Electric Reliability Corporation [NERC], 2008f).*
- *DHS, DOE, FERC, and GAO, the Government Accounting Office represent the public sector. DHS' role is to supervise critical infrastructure protection efforts. DOE's role is a coordinating function between DHS and the private sector. FERC's role is regulatory, creating legislation when it is required. In general, regulations are the last option pursued in critical infrastructure protection efforts. The GAO provides progress and evaluation reports on governmental activities.*

The survey recapitulates the main developments by DHS, NERC and FERC in three separated chapters.

DHS Developments

The developments under DHS consist mostly of plans for securing critical infrastructure. All the plans address issues and vulnerabilities created by the utilization of information technology used in critical infrastructure in an interconnected, networked environment. *These environments in the electricity sector commonly employ SCADA systems.* They are vulnerable to cyber attacks that accompany the networked environment of information technology products. *Since 85% of the electricity sector's critical infrastructure is privately owned* [OHS, 2002], *all plans emphasize the* ***public-private partnership*** *efforts to share information so vulnerabilities can be identified, threats can be assessed, and mitigation plans and solutions can be developed and implemented. Each plan builds upon the previous plans.* We quote here the main developments reported, by stressing only key issues discussed by Hoebich [2008]:

[8] *Italics* denotes textual excerpts from Hoebich [2008]

- **National Strategy for Homeland Security** and **Homeland Security Act** of 2002. The Act created the DHS in 2003, with the goal to *Build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors.*
- **The National Strategy to Secure Cyberspace**, 2003. This strategy also addresses the security issues with *SCADA systems in the electricity sector. SCADA systems are increasing using the Internet to transmit data rather than closed, proprietary networks. DHS works with private sector and DOE to raise awareness of the security issues affecting the commonly used SCADA systems and to promote SCADA security.* Some goals for SCADA include: work on intrusion detection, internet security, application security and transmission security (encryption and authentication). *These goals all need to be implemented in an environment that requires real-time responses.*
- **Homeland Security Presidential Directive 7**, 2003 replacing PDD-63
- **Protected Critical Infrastructure Information Program**, 2004. *This Program enables the private sector to voluntarily submit vulnerabilities and threat information to the DHS on critical infrastructure. DHS in return will analyze the submitted information and determines if it qualifies for protective status from the Freedom of Information Act, civil lawsuits and public viewing (…) This program is not being used that much due to concerns over DHS' implementation of it. The electric sector reported in 2005 that they had not used the program since it required paper submission, but probably would when the process went electronic. In March 2008, the PCII Program did have electronic submission capabilities, however, the digital certificate on the Web site had expired in 2007. This implies that DHS is experiencing organizational and implementation difficulties.*
- **National Infrastructure Protection Plan (NIPP),** 2006
- **Roadmap to Secure Control Systems in the Energy Sector,** 2006. *The Roadmap Report was a collaborative effort between DOE, DHS, NERC, and private entities within the electricity sector (…) Over half of the 3,200 power utilities are estimated to have some form of SCADA system employed (…) Legacy SCADA systems were designed without secure password policies and with limited to no data protections mechanisms. Also applying security to legacy SCADA systems is expensive and without a well known example of a cyber attack to a SCADA system in the electricity sector, the business case is difficult to justify.*
- **Energy Critical Infrastructure and Key Resources Sector-Specific Plan,** 2007. The Sector-Specific Plan implements the NIPP in the electricity sector. To reach the goal of cyber critical infrastructure protection the application of a risk management methodology is employed in this plan: *use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency* (...) *The performance metrics used to track critical infrastructure progress are qualitative and quantitative in nature and are still being developed by DHS and the electricity sector (…) One of the most valuable outcomes from this plan is the increased communication and the development of trusted relationships between the government and the private electricity sector entities.* The Sector-Specific Plan built off the Roadmap Report, and was a collaborative effort between DHS, DOE, and NERC.

- In summary, *DHS was created as a response to the Sept. 11, 2001 attacks.* One of its main responsibilities *is to be the focal point of critical infrastructure protection efforts (…) DHS is tasked with developing and implementing strategies and plans on critical infrastructure protection.* These appear to be consequential – they *build off each other; however on closer examination there is a lot of repetition.* DHS has identified and brought attention to the vulnerabilities of SCADA systems, however it *falls short in implementing the plans, due dates have been missed and effective processes for information sharing with the private sector are still not in place.*

NERC Developments

These developments consist mostly of creating guidelines and standards to achieve a level of sustained reliability in the bulk power system. *Due to the threats to SCADA systems in the electricity sector, specific attention is paid to cyber critical infrastructure standards development.* Moreover, since the government put considerable emphasis on information sharing NERC did put some effort into this area. In the following we report the main developments quoted by Hoebich [2008]:

- The **Critical Foundations** report *was produced by the President's Commission on Critical Infrastructure Protection in 1997 and it reports on the perceived threats to critical infrastructure and the proposed solutions (…) The Critical Foundations report also identified NERC as a model for partnership success,* in that NERC had a long history of collaboration with the FBI and the DOE in information sharing *(…) Building on this concept of information sharing, the report recommended the development of repositories where information could be stored, accessed, and shared by the private sector and the public sector (ISACs - Information Sharing and Analysis Centers)… In 1998 the DOE asked the NERC to take the role of Coordinator for Critical Infrastructure Protection for the electricity sector and also to set up the ISAC.*
- The NERC became **CIP Coordinator for the Electricity sector** in 1998 and set up the Energy Sector Information Sharing and Analysis Center **(ES-ISAC**) in 2000.
- In 2002, NERC produced the **Security Guidelines for the Energy Sector**. *These are general guidelines for protecting electric critical infrastructure systems and are advisory in nature.* As a result, NERC took on the responsibility of developing reliability standards for electricity generation and transmission. The guidelines provided a foundation that other developments built upon. They were applied in the Reliability Standards on Critical Infrastructure Protection, like the **Urgent Action 1200 Cyber Security Standard** (2003) and the Reliability Standards **CIP 002-1** to **CIP 002-9** which replaced the UA-1200 in 2006. In 2003 the NERC also created the **Reliability Standards Process Manual**, a step-by-step process for creating, changing, and deleting standards. The process is accredited by the ANSI since 2003 and involves, among other, a field testing phase after which the standard is either adopted or rejected. The Process Manual later developed in the Reliability Standards Development procedures (2006). This development is also somewhat related with the **FERC order certifying NERC as the ERO**.

The **Reliability Standards Development Plan: 2008-2010** was created by NERC in 2007. This plan is a management tool to guide development in reliability standards. This plan is dynamic; it changes over time based on priorities and what has been accomplished. *Standards are tested to meet the following ten objectives:*

1. Applicability
2. Purpose
3. Performance requirements
4. Measurability
5. Technical basis in engineering and operations
6. Completeness
7. Consequence for noncompliance
8. Clear language
9. Practicality
10. Consistent terminology

However, as a result, the cyber security project was delayed by one year. Originally the electricity sector was supposed to be 100% audit compliant by the end of 2010.
In summary, the NERC appears engaged in *continuous work on creating comprehensive guidelines and standards. The establishment of official manuals and procedures for designing and approving standards for cyber critical infrastructure insure that specific requirements are met before the standard is passed.* The standards development process is approved by the ANSI. It creates a collaborative environment and promotes industry take up. *For example, the draft of the UA-1200 cyber security standard was posted for comment and got around 700 responses. However, obstacles still persisted in the adoption of these voluntary standards by the electricity sector. This became clear after the 2003 Northeast Blackout. The investigation showed that voluntary standards were not being adopted (…)* This resulted in the FERC regulations to force entities in the electricity sector to implement standards to achieve reliability in the bulk-power grid system.

FERC developments

FERC is an independent regulatory agency within the DOE. *FERC issues the regulations needed to establish reliability in the bulk-power grid system (…) the public-private partnership efforts between FERC and NERC are present in all these resulting rules. NERC submits a proposed standard and FERC gives the standard its seal of approval or sends it back to NERC for revisions. NERC in turn can make comments on revisions and FERC considers those comments in its final rule making process.* Hoebich [2008] quotes three major developments where FERC played a key role:

- The **Critical Energy Infrastructure Information Final Rule** was issued by FERC in 2003 to clarify the process for gaining access to protected information that was voluntarily submitted to DHS from the energy sector. This Rule is a response to the lack of cyber critical infrastructure information sharing with the government. The electricity sector was concerned *about sharing information on power system vulnerabilities, cyber security incidents, and other sensitive information that could be detrimental*

if that information was to be released into the public realm. FERC took measures to alleviate concern over this issue *by incorporating specific language as to what information is considered protected and who is authorized to access this protected information*. NERC responded to the notice of this impending rule by providing comments to FERC to be considered. *A 30 day window was requested to respond to information that was submitted as critical infrastructure information, but did not qualify as it (so submitting entity could take back the information and still retain control over its dispersal). The use of non-disclosure agreements was requested for the released protected information. NERC also wanted relationship interdependencies information on SCADA and Energy Management Systems to be deemed protected information.*

- The Northeast Blackout of 2003 brought attention *to the lack of voluntary compliance to guidelines and standards meant to secure the power grid.* The joint US-Canada Power System Outage Task Force found that many entities involved did not implement the voluntary standards. This was the main reason behind the development of regulations to enforce compliance in 2005. The **Energy Policy Act** of 2005 empowered FERC to certify an Electric Reliability Organisation (ERO). The ERO can make compulsory standards for the bulk power system reliability with the full force of law (it can enforce monetary penalties for non-compliance). In 2006 NERC was certified as the ERO thus becoming able to enforce the reliability standards it developed.
- FERC approved NERC's cyber security standards in 2008 as the **Mandatory Reliability Standards on Critical Infrastructure Protection.** *Entities in the electricity sector must comply with the standards or face monetary fines of up to one-million dollars per day* (...) *There are 3,284 electric utility companies in the United States in 2005 and 3,029 are considered small utilities under the definitions of the Small Business Administration. Under the requirements of NERC there are 1,000 entities that will be required to comply with the Mandatory Reliability Standards on Critical Infrastructure Protection. Of these – 632 are small entities.*

In summary, *regulations come after all voluntary methods have been attempted, but have failed. When an event such as a major power outage makes it clear that voluntary measures to secure the bulk-power grid system are unsuccessful, then FERC creates legislation to solve the problem. FERC has also tried to improve information sharing by creating more specific rules protecting the access and availability of critical infrastructure information submitted to the government. However, resistance to sharing sensitive, potentially damaging information with the government still exists.*

Key issues

According to Hoebich [2008] there are three main recurrent themes that appear in each group of developments:

Power outages

Major power outages bring attention to the vulnerabilities of the power system and the fact that reliability standards are not being implemented. The lack of adoption of voluntary reliability standards points to the need for regulation. Cyber critical infrastructure protection efforts appear to intensify after a major power

outage. Power outages are reported to NERC and the DOE through *electricity disturbance reports*. An examination of the data in these reports show that when the number of outages per year increases, the likelihood for a major power outage also appears to increase. Both NERC and the DOE *show larger numbers of power outages occurring per year during 2003 through 2006 (numbering from 60-90 per year). One to three major power outages per year also occurred during this timeframe. Looking at the developments that occurred from 2003-2007, there was a plethora of activity, including regulations, standards, and plans.* The economic impact is the main motivation to protection efforts. The cost of the Northeast blackout was estimated to range in between $7-10 billion. The response to the Northeast blackout was an intensification of the efforts to achieve higher reliability of the power system. The Energy Policy Act of 2005, the NERC becoming ERO in 2006 and submitting CIP standards to FERC for approval, the approval of those standards by FERC as Mandatory Reliability Standards in 2008 are to be seen in that light.

Economic Considerations

Since the majority of the cyber critical infrastructure is owned by the private sector it is important for the public sector to understand the role of economics in business decisions. *The concept of return on investment and cost benefit analysis are used when considering new business expenditures.* If the financial analysis shows poor returns businesses will avoid investing in additional security. *If an entity within the electricity sector experiences a cyber attack that is significantly financially damaging then they will take measures to prevent this from happening in the future. However, if the risk is low for a successful, damaging cyber attack, and it is cheaper to clean up after an attack than install preventive measures, the organization will take the route that makes better business sense* [CSO et al., 2007]. The cost of securing control systems and SCADA system from cyber attacks is difficult to determine. *Control systems according to DOE cost 3-4 billion dollars for the electric grid. Remote field devices cost 1.5-2.5 billion dollars to replace* [GAO, 2007a]. Retrofitting an existing SCADA system is also probably an expensive expenditure (estimated 1/2 – 1 million dollars). The GAO cost report on the Mandatory Reliability Standards for Critical Infrastructure Protection estimates the cost for information gathering requirements to amount to more than $100 million [GAO, 2008]. This does not even take into account the cost of actual implementation expenses associated with compliance. If the investment is so high, some electricity entities might decide not to comply. To counteract this scenario the penalty fees are set to a maximum of 1 million dollars per day [GAO, 2007a]. *Since 1,000 entities within the electricity sector need to comply with Mandatory Reliability Standards for Critical Infrastructure Protection and if information gathering costs is 10% of total compliance cost, then each entity is looking at a cost of 1 million dollars or more. 632 of these entities are classified as small businesses and a security expense of 1 million dollars or more might not be economically feasible.*
The resistance to complying with voluntary standards created by NERC was probably due to the high price of compliance. *There were several compliance reports by NERC on voluntary reliability standards.* For the second quarter of 2007, 3,412 violations were self-reported [NERC, 2007a]. The resistance to sharing potentially damaging information with the DHS can also be tied to economics. *GAO confirms that the financial risks of sharing critical infrastructure information can be determined, but the benefits are not easy to determine for the private sector* [GAO, 2004a]. Risks encompass customers losing confidence, lawsuits, loss of business, and decreases in stock prices.

Public-Private Partnership

The overall governmental strategy who led to establishing the DHS put emphasis on developing effective public-private partnerships. We have seen that partnerships efforts between NERC and FERC in the development of standards for critical infrastructure protection were successful. On the contrary, partnership efforts between NERC and DHS seem to be tenuous at best. The relationship between DHS and the private entities that NERC represents is not that successful since the responsibilities and benefits are not clearly recognized.

The concept of DHS as a focal point for disseminating information is a good idea. *This ensures that all participants get the information in a timely manner* [GAO 2006] . *It is important to get key information into the hands of people who can mitigate the damage, and those people are in the private sector, not the public sector. But DHS needs to make it clear why it needs cyber critical infrastructure information from the private sector. DHS needs to convey how this information is used, how this information is protected (...) and show the benefits to the private sector of sharing information.* GAO [2006] also reports that *DHS has not said if it needs specific vulnerability information or interdependencies and this drives the question if DHS knows what it needs.* The report shows that DHS has received a total of 290 submissions from the private sector, but *DHS has not used the information submitted by the private sector to issue any warnings or advisories, which makes the private sector wonder what the information is used for. Additionally, there has been no court case to uphold protection of submitted information from the Freedom of Information Act*.

GAO [2007a,b] maintain that there still was no standard governmental implemented process for sharing information with the private sector. From 2003 to June, 2006, *DHS has only issued nine notices on control system vulnerabilities to the private sector. This small number of notices does not encourage the private sector to reciprocate information sharing with the DHS.* DHS information sharing capabilities are further restricted by organization issues within DHS. DHS has lost many of its key positions during 2004 and 2005. *The turnover in DHS leadership positions has produced an unstable environment, which results in the private sector wondering if the DHS is capable.*

REFERENCES

Abrams [2007] *Addressing Industrial Control Systems in NIST Special Publication 800-53,* MITRE Technical Report MTR070050, Marshall D. Abrams, March 2007 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf

AGA [2006] *AGA 12 recommends how to protect SCADA communications from cyber attack*. Rush, William F.,Kinast, John A.,Shah, Aakash B., Pipeline & Gas Journal, Nov. 2006. Press release on: http://www.allbusiness.com/agriculture-forestry-fishing-hunting/support-activities/3974400-1.html

API [2005] *Security Guidelines for the Petroleum Industry, Third Edition,* The American Petroleum Industries Association, April 2005. http://www.api.org/aboutoilgas/sectors/pipeline/securitypreparedness.cfm?renderforprint=1

Byres, E. & Lowe, J. [2004]. *The myths and facts behind cyber security risks for industrial control systems.* http://tswg.gov/subgroups/ps/infrastructure-protection/documents/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

CSO et al. [2007] CSO Magazine, U.S. Secret Service, CERT Program, and Microsoft Corporation, *2007 e-crime watch survey.* http://www.cert.org/archive/pdf/ecrimesummary07.pdf.

CERT [2009] *ICS CERT Incident Summary Report 2009-2011*, http://ics-cert.us-cert.gov/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

EC [2008] European Commission, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection Text with EEA relevance*, Official Journal L 345 , 23/12/2008 P. 0075 – 0082, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:HTML:NOT

GAO [2006] Government Accountability Office, *Information sharing: DHS should take steps to encourage more widespread use of its program to protect and share critical infrastructure information.* Retrieved July 20, 2009, from http://www.gao.gov/new.items/d06383.pdf.

GAO [2007a] Government Accountability Office, *Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain*. Retrieved July 28, 2009, from http://www.gao.gov/new.items/d071036.pdf.

GAO [2007b] Government Accountability Office, *Department of homeland security: progress report on implementation of mission and management functions*. Retrieved July 28, 2009, from http://www.gao.gov/new.items/d071240t.pdf.

GAO [2008] Government Accountability Office, *Report under 5 U.S.C. § 801(a)(2)(a) on a major rule issued by the department of energy, federal energy regulatory commission entitled "mandatory reliability standards for critical infrastructure protection"* (Docket No. RM06-22-000). Retrieved July 28, 2009, from http://www.gao.gov/decisions/majrule/d08493r.pdf.

Hoebich [2008] CSO Magazine, U.S. SCERIAS Tech Report 2008-16 *Status Report on Cyber Critical Infrastructure Protection Involving the Bulk-Power Grid System* by Marianne Hoebich, Center for Education and Research - Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086, May 2008

Gheorghe et al [2006] Gheorghe A.V., M. Masera, M. Weijnen, L.J. De Vries, *Critical Infrastructures at Risk: Securing the European Electric Power System* , Springer Verlag, 2006

ISO/PAS 22399 [2007] *Societal security - Guideline for incident preparedness and operational continuity management,* ISO, the international Standard Organisation, 2007, http://www.iso.org/iso/catalogue_detail?csnumber=50295

NERC [2006] *(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1*, NERC, the North American Reliability Council, May 2006, http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf

NIST [2009] *Recommended Security Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53 Revision 3, August 2009, http://csrc.nist.gov/publications/PubsSPs.html
Office of Homeland Security. (2002). *National strategy for homeland security.* http://www.oe.energy.gov/DocumentsandMedia/National_Strategy_for_Homeland_Security.pdf.

Stefanini et al [2005] Stefanini, A., S. Puppin e A. Servida, *Electric System Vulnerabilities: the Crucial Role of Information & Communication Technologies in Recent Blackouts,* Electra no. 223 p. 6-17

Stefanini & Masera [2008] *The security of power systems and the role of information and communication technologies: lessons from the recent blackouts*, Int. J. of Critical Infrastructures, 2008 Vol.4, No.1/2, pp.32 – 45

VGB [2006] *VGB Guideline IT Security for Power Plants.* VGB PowerTech e.V, October 2006, http://www.vgb.org/en/nl_september_2006_en.html
White House [2007] The White House PRESIDENTIAL DECISION DIRECTIVE/NSC-63, Washington, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

WIB [2010] Process control domain-security requirements for vendors, Report: M 2784-X-10, Published by WIB, first issue march 2010, available at http://www.wib.nl/download.html