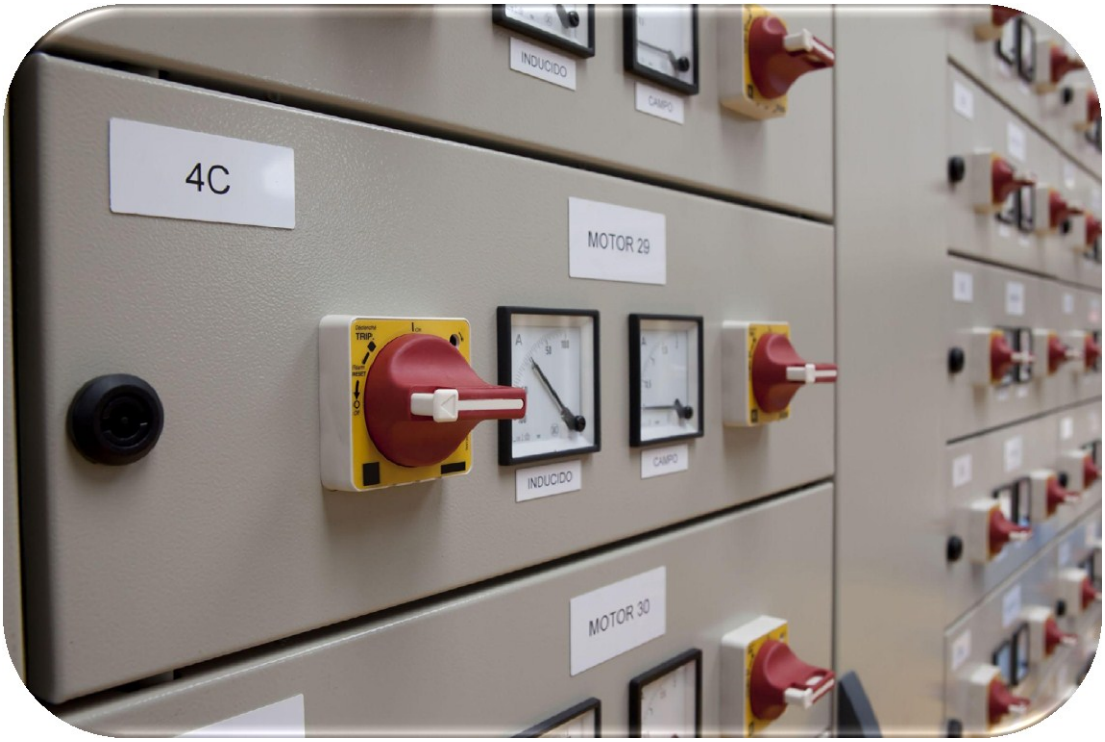
enisa
European Network and Information Security Agency



Protecting Industrial Control Systems

Recommendations for Europe and Member States

[Deliverable – 2011-12-09]

DOCUMENT HISTORY

Date	Version	Modification	Author
15/07/2011	0.1	Structure of the document defined	S21sec
29/07/2011	0.2	The following sections written: • Known standards, good practices, and policies. • Existing Initiatives • Existing solutions	S21sec
22/08/2011	0.3	Section 4 extended Sections 5, 6 completed	S21sec
26/08/2011	0.4	The following sections added: • Description of the approach • Target audience • Emerging issues • Challenges, and standards/guidelines Two annexes added: • Standards/guidelines • Initiatives	S21sec, Rafał Leszczyna
26/08/2011	0.5	Added summaries for the following sections: • Initiatives • Guidelines, standards Key Findings included into the core report Current policy context in Annex I modified	S21sec, Rafał Leszczyna
04/09/2011	0.6	Added: • Executive summary • Glossary Reviewed: • Recommendations • Survey and interviews analysis section	S21sec, Rafał Leszczyna
11/09/2011	0.7	Annex V added Bibliography and Glossary moved Minor changes in the recommendations	S21sec, Rafał Leszczyna

24/10/2011	0.8	Added: • Conclusions chapter • New figures in Annex I Workshop participant's comments incorporated	S21sec
27/10/2011	0.9	The report proof read Annex VI added Ammended: • Introduction • Approach • Executive Summary	S21sec
31/10/2011	0.10	Full draft ready	S21sec
25/11/2011	0.11	ENISA Quality Assurance review completed	Steve Purser Manel Medina

Contributors to this report

- Rafał Leszczyna, Gdansk University of Technology
- Elyoenai Egozcue, S21sec
- Luis Tarrafeta, S21sec
- Victor Fidalgo Villar, S21sec
- Ricardo Estremera, S21sec
- Jairo Alonso, S21sec

Agreements or Acknowledgements

- EuroSCSiE
- Adrian Koster, MELANI
- Alejandro Pinto, European Commission
- Ana Lozano Lima, Isdefe
- Andreu Bravo, Gas Natural
- Angelo Gino Manfredi, Enginet
- Annemarie Zielstra, CPNI NL
- Auke Huistra, CPNI NL
- Bart De Wijs, ABB
- Bela Genge. EC JRC
- Ben Kaintoch, QinetiQ
- Bence Birkas, CERT-Hungary
- Benno Scholze, Navayo
- Bernard Roussely, Infosec
- Bill Fulton, Scottish Power Energy
- Bob Lockhart, Pike Research
- Bram Reinders, Alliander
- Carmine Rizzo, ETSI
- Christos Siaterlis, EC JRC
- Claudio Brasca, RSE
- Daniela Pestonesi, ENEL
- David Barroso, S21sec
- David Willacy, UK National Grid
- Dennis Holstein, OPUS Consulting
- Dina Hadziosmanovic, University of Twente
- Dominic Storey, Sourcefire
- Eric Byres, Byres Security
- Eric Luiijf, TNO
- Eyal Adar, White Cyber Knight
- Felipe Alvarez Cuevas Figuerola, ENDESA
- Francisco Ramos, Telvent

- Frank Hyldmar, Elster
- Franky Thrasher, ESCSiE
- Gemma Deler, APPLUS
- Gitte Berknut, E.ON Sverige AB
- Guido Sanchidrian, Symantec
- Hans De Raad, PROXY Laboratories
- Hans Honecker, BSI
- Herbert Ecker, Energie AG Oberösterreich Data GmbH
- Jacek Gasiorowski, Emerson
- Jaime Andreu Servera, Endesa
- Jarkko Saarimaki, CERT FI
- Javier López, University of Málaga
- Jesus Carrillo Martinez, Gas Natural Fenosa
- Johan Rambi, Alliander
- Jorge Aguado, ISDEFE
- Jos Menting, EuroSCSIE
- Jose Fernando Carvajal Vion, Indra
- Karl Williams, QinetiQ
- Karl Rossegger, LINZ STROM GmbH
- Kris Hallaert, Elia
- Luc Van den Berghe, CEN/CENELEC
- Luca Guidi, ENEL
- Luigi Coppolino, University of Naples Parthenope - Consorzio Interuniversi
- Luigi Romano, CINI and University of Naples "Parthenope"
- Marcello Antonucci, Infosis
- Marcelo Masera, JRC
- Marcos Gómez Hidalgo, Inteco
- Marie Kerinsema, Alliander
- Marta Olivan, Indra
- Martin Euchner, ITU
- Matthias Tischlinger, Energie AG Oberösterreich Data GmbH
- Michael Freiberg, Acris
- Michael Munzert, Siemens AG
- Michal Choras, ITTI
- Michele Minichino, ENEA
- Mirabent Josep, ELECNOR DEIMOS
- Nick Reeve, RWE Npower
- Olivier Paridaens, Alcatel Lucent
- Oscar Pastor Acosta, ISDEFE
- Oscar Sancho Gasion, AGBAR
- Robert Cragie, Gridmerge

- Samuel Linares, Intermark Tecnologias
- Sandro Bologna, AIIC
- Sauli Savisalo, National Emergency Supply Agency
- Stefano Buschi, Bozz & Co.
- Stig Ole Johnsen, SINTEF and NTNU
- Tony Davies, Environment Agency UK
- Uwe Jendricke, BSI (DE)
- Walter Caputo, Elsag Datamat
- Zoltán Précsényi, Symantec

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on CIIP & Resilience, please use the following details:

- E-mail: resilience@enis.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to industrial control systems' security, please use the following details:

- E-mail: Evangelos.Ouzounis@enisa.europa.eu

Contents

Annexes

- Annex I: Desktop Research Results
- Annex II. Survey and Interview Analysis
- Annex III. ICS Security Related Standards, Guidelines and Policy Documents
- Annex IV. ICS Security Related Initiatives
- Annex V. Key Findings
- Annex VI. Minutes of the Workshop

1 Executive summary

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems. In the last few years, ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today, ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the-shelf software. All this has led to cost reductions, ease of use and enabled the remote control and monitoring from various locations. However, an important drawback derived from the connection to intranets and open communication networks, is the increased vulnerability to computer network-based attacks.

Industrial control systems constitute a strategic asset against the rising potential for catastrophic terrorist attacks affecting critical infrastructures[1]. In the last decade, these systems have been facing a notable number of incidents, including the manifestation of Stuxnet which raised a lot of concerns and discussions among all the actors involved in the field.

In April 2007, the Council adopted the conclusions of a European programme for critical infrastructure protection (EPCIP)[2]. This was the result of a series of actions driven by the European Commission, the Council and the Justice and Home Affairs Council which started in June 2004. The key element of EPCIP is the Directive[3] on the identification and designation of European Critical Infrastructures. In parallel, the information security issues for vital infrastructures in Europe are addressed by The Digital Agenda for Europe (DAE)[4] and the CIIP action plan[5].

Recognising the importance of the problem, ENISA launched a series of activities, which aim at bringing together the relevant stakeholders and engaging them into an open discussion on ICS protection. The principal goal of the open dialogue is to identify the main concerns regarding

---

[1] ***Commission of the European communities.*** *Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final. 2004.*

[2] ***Commission of the European communities.*** *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786. 2006.*

[3] ***Commission of the European communities.*** *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. 2008.*

[4] ***Commission of the European Communities.*** *Communication from the Commission: A Digital Agenda for Europe, COM(2010) 245. 2010.*

[5] ***Commission of the European Communities.*** *Communication from the Commission: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149. 2009.*

the security of ICS[6] as well as to recognize and support national, pan European and international initiatives on ICS security. The involved stakeholders include ICS security tools and services providers, ICS software/hardware manufactures and integrators, infrastructure operators, public bodies, standardisation bodies, academia and R&D.

Furthermore, in order to help the stakeholders get a deeper insight on the issue, ENISA decided to further explore this problem by delivering a research and survey-based study on this topic. The objective of the study is to obtain the current perspective of ICS protection primarily in Europe, but also in the international context. This view includes threats, risks and challenges in the area of ICS protection as well as national, pan European and international initiatives on ICS security.

This final report proposes 7 recommendations to the public and private sector involved in the area of Industrial Control Systems. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing. This guidance is based on the results of a thorough analysis of the opinions of the experts who participated in the Study. Furthermore, important information coming from an in depth desktop investigation is also taken into consideration. All this data has been analysed and has led to the derivation of almost 100 Key Findings.

What follows is a brief summary of all the recommendations.

Recommendation 1: Creation of Pan-European and National ICS Security Strategies. *The European Union should create a pan-European Strategy for European ICS Security activities and each Member State should develop a National Strategy for ICS Security. The strategies must be coherent with the European Union Council Directive 2008/114/EC for Critical Infrastructures, and leverage the existing initiatives addressing the problem of ICS Security (e.g. EuroSCSiE) as well as the national and Pan-European Public Private Partnerships (e.g. EP3Rs). The strategies have to serve as references for all state-members stakeholders, act as facilitators for sharing initiatives and foster research and education.*

Recommendation 2: Creation of a Good Practices Guide for ICS security. *The European Union should assume leadership and develop a consensus-reached document or set of documents regarding security good practices, integrating both physical and logical security aspects, to serve as reference for every type of stakeholder. This document should help all stakeholders ensure that best security practices are applied in the industry.*

Recommendation 3: Creation of ICS security plan templates. *The different National ICS Security Strategies should consider within their tasks the creation of ICS security plan templates, both for operator and infrastructures, which security experts could adapt to their particular situation. These plans should include operational and physical security, technical issues, training and awareness, security governance with roles and responsibilities, business impact measures and crisis management. These templates should severely decrease the cost*

[6] *On different levels: legal and regulatory, organisational, dissemination and awareness, economic/financial and technical.*

of developing security plans and accelerate the adoption of comprehensive security measures within the industry.

Recommendation 4: Foster awareness and training. *As part of national ICS-Security strategies, the Member States should foster dissemination and awareness activities through high quality events involving all kinds of stakeholders and with special attention to top management commitment. Training and awareness programmes and events should be created for all types of end users.*

Recommendation 5: Creation of a common test bed, or alternatively, an ICS security certification framework. *The Common ICS-Strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership in which tests could be performed in order to guarantee that different systems interaction do not cause security failures. A common test bed will help all stakeholders to detect potential problems in a controlled environment, ensuring integrity and increasing the trustfulness in certified solutions.*

Alternatively a security framework model adapted for ICS could be defined, based on existing efforts such as Common Criteria or FIPS. Member State existing certifying organisms would be responsible for the certification process based on this security framework.

Recommendation 6: Creation of national ICS-computer emergency response capabilities*. Following the national ICS Security Strategies, national ICS-computer emergency response capabilities should be established, in cooperation with an adequate number of public and private CERTs. The ICS-computer emergency response capabilities should help all stakeholders to have a reference in order to share vulnerability information, disclosure it, coordinate actions and help in effectively dealing with risk management in ICS infrastructures. In order to address the challenges which span across the borders, member states should cooperate on the Pan-European level (e.g. with the aid of an ICS-Security information sharing platform such as EuroSCSiE).*

Recommendation 7: Foster research in ICS security leveraging existing Research Programmes. *The National and Common ICS Security Strategies should foster research to address current and future ICS threats and security challenges such as ICS-ICT integration, legacy/insecure equipment, targeted attacks or Smart Grid issues. This should be done by leveraging existing European or National research programmes, such as the European Framework Programme.*

2 Introduction

This study proposes 7 recommendations to the public and private sector involved in the domain of Industrial Control Systems (ICS). These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing – relevant to the security of ICS. We consider that these recommendations are effective, achievable, and urgent.

They are urgent because the ICS are an essential element in the correct operation of many European and national critical Infrastructures. Without the ICS gas distribution, water treatment, a variety of chemical processes, electricity distribution, oil refining, or railway transportation would not be possible. Furthermore, recent cyber security incidents such as Stuxnet or Night Dragon have provided real evidence of how vulnerable these systems currently are.

The implementation of these recommendations will be challenging. Many of them will require the active collaboration between the public organizations and the private sector. Additionally, European institutions will have to take the lead in a field that has been addressed only quite recently. However we believe that with the strong involvement of all engaged parties this will be an achievable task. Stakeholders attending the study workshop showed their strong support for improving the recommendations and their willingness to help in their implementation.

The recommendations were derived from almost a hundred of key findings. These key findings are the result of a thorough analysis of the opinions of the experts who participated in the study equally accompanied by a comprehensive documents-based research.

On the 16th September 2011, ENISA organised a workshop where the results of the Study on ICS security were presented. The aim of this workshop was to share and discuss the most relevant conclusions of the report, including the proposed recommendations, with the experts that participated in the Study. For this reason, an open dialog among the attendees was also planned. This dialog allowed ENISA to pulse the impression of the audience on the recommendations and to gather the different opinions on how to improve them.

This report is divided into eight chapters: introduction, purpose and scope of the study, targeted audience, approach, key findings, recommendations, and conclusions. Additionally, there are 5 annexes which contain the detailed information on the results of the study. They include the detailed output of the desktop research and the analysis of the raw data coming from the experts. Additionally, another annex is devoted to the Study Workshop.

- Annex I presents the main results coming from a desktop research phase. It provides a comprehensive overview of the current panorama of ICS security.
- Annex II provides a detailed analysis of the data gathered from the interviews and the survey in which ICS security experts participated.

- Annex III is a compilation of current security guidelines and standards for ICS.
- Annex IV includes a complete list of initiatives related with ICS security
- Annex V provides detailed descriptions of the Key Findings which make up the knowledge base on which recommendations are built upon.
- Annex VI includes the minutes of the Workshop.

2.1 The evolution of Industrial Control Systems

The first industrial control systems were simple point-to-point networks connecting a monitoring panel or command device to a remote sensor or actuator. These have since evolved into complex systems that support communication between a central control unit and multiple remote units on a local area communication bus, or spanning long distances by means of complex meshed networks. The nodes on these networks are usually special purpose embedded computing devices such as sensors, actuators, Remote Terminal Units (RTU's), and Programmable Logic Controllers (PLC's).

Through the last decade ICS systems have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today's' ICS products are mostly based on standard embedded systems platforms, applied in various devices, and they often use commercial off-the shelf software. This has resulted in less investment and operational costs, ease of use (which means less training and increased overall productivity) and enabled remote control and monitoring from various locations. However, an important drawback derived from the connection to intranets and other communication networks, is the increased vulnerability to computer network-based attacks.

2.2 Cyber security aspects of ICS

ICS communication protocols were not designed with security in mind. Many of these protocols were initially conceived as serial protocols without built in authentication, encryption or message integrity mechanisms. This exposes the communications to a variety of attacks, including eavesdropping and session hijacking and manipulation. Nowadays, many of these protocols have been integrated with the TCP/IP protocol suite, or even replaced by standard open ones with similar security problems (e.g. OPC)

Not only communication protocols have been modified or replaced by standard open ones, for similar reasons of costs and productivity, operating systems and applications in ICS have also transitioned from closed ad-hoc developments to de facto standard operating systems (e.g. MS Windows or Unix-like) and applications (e.g. MS SQL Server, MS Excel, etc.).

This in turn makes these systems susceptible to the same software attacks that affect conventional ICT systems (e.g. desktop computers).

ICS systems and other corporate IT systems are nowadays interconnected. Interconnectivity capabilities have been drastically improved, since it is quite common to have IP-based ICS communications. Now, it is quite normal to perform remote administration of control systems and associated network devices. Likewise, control engineers and support personnel can have access to supervise the ICS from points outside the control network, even making use of the Internet. As a result, attacks to ICS can originate in almost any part of the world.

On the other hand, ICS have characteristics that make them very different from traditional information processing systems. There are two main differences driving most of the others: ICS systems have different priorities and imply risks with a much broader scope and impact. ICS were designed to meet tight performance and reliability requirements which are not typical in a conventional ICT environment. All this, together with ICS technologies' specific characteristic (e.g. control protocols, real-time, etc.), results in a difficult environment for directly applying traditional security solutions and procedures.

Unfortunately, ICS and CIs are already facing problems deriving from cyber security incidents, either intentional targeted attacks or collateral damage from wrong practices, computer viruses, etc. One of the most relevant recent incidents affecting ICS is related to the malicious software Stuxnet. Stuxnet is a very advanced piece of software which was probably conceived as a cyber weapon for sabotage. The policy context

In December 2006 the COM(2006) 786 "on a European Programme for Critical Infrastructure Protection" fixed the main aspects of a European Programme for Critical Infrastructures Protection EPCIP). This communication recognized the threat from terrorism as a priority even though the protection of critical infrastructure would be based on an all-hazards approach. This Communication also defined the main guiding principles of the EPCIP and identified the necessity for creating an EU framework concerning the protection of critical infrastructures.

In the same year, the Commission also adopted the Communication COM(2006) 251, "A strategy for a Secure Information Society – Dialogue, partnership and empowerment", which stressed the importance of dialogue, partnership and empowerment of all stakeholders to properly address the threats to the security of the Information Society, complementing the activity being planned to achieve the goals of EPCIP.

In 2009, the Commission adopted COM(2009) 149 on Critical Information Infrastructure Protection. This Communication recognizes that ICT infrastructures are the underpinning platform of other CI's and defines a plan of immediate actions to strengthen the security and resilience of Critical Information Infrastructures (CII's) based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for EC infrastructures in the field of ICT. In 2011, another Communication from the Commission, COM(2011) 163, summarised the achievements of this plan and defined next steps to be taken. It also recognized that new threats have emerged, mentioning Stuxnet as an example. However, as for COM(2009) 149, none of the activities planned as next steps were specifically targeting Industrial Control Systems.

On the other hand, the USA already has a Control System Security Program, which is coordinated by the National Cyber Security Division of the Department of Homeland Security (DHS). The main goal of this programme is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments, as well as industrial control systems owners, operators and vendors.

2.3 The need for a study on ICS security

ENISA, as an EU body of expertise in Network and Information Security (NIS), is supporting the European Commission's CIIP action plan. This involves working closely with the Member States, public and private sector stakeholders' to secure Europe's Critical Information Infrastructures.

In order to help public stakeholders to develop a deeper insight into the security and resilience of ICS systems, ENISA decided, in 2011, to further explore the problem of ICS security in Europe.

3 Purpose and scope of the study

3.1 The aim of the study

The main objective of the study is to identify threats, risks and challenges in the area of ICS protection as well as to recognize national, pan European and international initiatives on ICS security. Additionally, the study investigates the increasing reliance of ICS systems on the Internet and the relationship of ICS systems to emerging areas, such as smart grids. Based on the analysis, the study proposes good practices and recommendations for all relevant stakeholders that will help them improve the security, safety and resilience of European ICS systems. Moreover, the study aims at helping the involved stakeholders in recognising the importance of security issues, engaging in international co-operation, raising awareness inside their organisations, and supporting standards. Finally, the recommendations resulting from the study will also allow ENISA to pave the way for future actions and studies on ICS systems.

3.2 The scope of the study

The two pillars of this study are:

- Identifying the current state of ICS security based on the concrete, comprehensive, and up to date 'inventory' of factual knowledge coming from the field
- Obtaining opinions on the subject from all the relevant stakeholders

Based on these pillars the recommendations for the stakeholders are derived.

Work on the factual description of the current situation has focused on the following aspects:

- Review of the concept of ICS and their role inside critical infrastructures.
- Analysis, from a security perspective, of the dependencies of ICS on third-party ICT infrastructures, considering both the underlying ICT communication infrastructure as well as interdependent ICS.
- Review of the threats that could affect these systems from a variety of perspectives.
- Description of the main differences between ICS and regular IT systems.
- Study of some emerging issues in the context of ICS security, specifically addressing targeted attacks, cloud computing and interrelationships with the smart grid.
- List of challenges to ICS security
- Summary of the current policy context under which the protection of ICS should be framed at the EU level and in the US.

- Analysis of the different technical solutions that are currently being applied for securing ICS.
- Review of the most significant standards, guidelines, regulatory documents as well as actives groups and initiatives.

Most of the content is based on highly reputable sources of information, such as official good practices, technical reports and standards of organizations such as CPNI UK, NIST, IEEE, ANSI/ISA, IEC, ISO, and others. However, it is also enriched by the contribution of several experts in the topic. These experts have contributed to this part of the study, by providing their knowledge in existing initiatives, known good practices, standards and policies, as well as other topics already addressed.

The second basic pillar of the study, obtaining the opinion on the subject of all relevant stakeholders (operators, manufacturers, policy makers, academia, etc.), is considered to be the more important part of the study. The relevant representatives of the public and the private sector have been engaged (by means of a survey and personal interviews) to provide their opinion on critical aspects of ICS security. ,

This study identifies common points and differences among stakeholders' replies and contributions to propose recommendations for these same stakeholders and ENISA itself. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing.

4 Targeted audience

This report constitutes a source of the most recent information on the topic of ICS Security which might be useful to anyone involved in the domain of Industrial Control Systems or interested in obtaining a detailed and broad overview of the current situation in ICS protection.

An important section of this document is devoted to providing an up-to-date factual description of the current security panorama of Industrial Control Systems, including existing initiatives, standards, guidelines, and regulatory documentation on ICS protection, current security challenges and emerging issues. This part of the document is presented in a technical language and it is assumed that the readers have some security and ICS background knowledge. Therefore, this section is intended for:

- Control engineers, integrators and architects
- System administrators
- Information security specialists
- Managers
- Security auditors
- Security consultants
- Business leaders with a technical background

In addition, the core sections of this document contain a number of key findings and recommendations regarding ICS security, resulting from the analysis of the opinions of multiple experts in the field. These key findings and recommendations are written in a non-technical language suitable especially for decision-makers. The key findings describe possible future strategies, devise new initiatives, and propose new research activities with the aim of improving the security of ICS at different action levels: political, organizational, technical, awareness raising, economical, etc. For this reason, this part of the report is more appropriate for:

- Business leaders
- Policy makers
- Standardisation bodies
- Public agencies
- Researchers

- Analysts

5 Approach

The study comprised two main phases. The first phase, 'stock-taking', was intended to gather all the data that will make up the work base for the study. The second phase was based on the analysis of the data in order to develop recommendations for the different types of stakeholders involved with cyber security aspects of ICS.

The activities carried out during the first phase of the study included the so called 'desktop research', which means the analysis of all available documents relevant to the topic of the study. In this part we made use of recognised existing documents (guidelines, recommendations, reports etc.) coming from organisations, companies, consortiums or research centres, as well as the most influential books in the field, and the latest news (for this we have for example subscribed to forums, discussion groups, news feeds, etc.).

The second crucial part of the 'stock taking' was the survey and interviews with the domain experts aimed at obtaining their opinion on the most important ICS security subjects. In this part we prepared six dedicated questionnaires for the following groups of stakeholders:

- ICS software/hardware manufactures and integrators
- ICS security tools and services providers
- Infrastructure operators
- Academia, R&D
- Public bodies
- Standardisation bodies

Each questionnaire comprised a mixture of around 25-27 open and closed questions which addressed the security of ICS from different points of view: political, organizational, economic/financial, dissemination/awareness, standards and guidelines, and technical. Interviews were conducted in a personal basis by means of audio conferences.. It is worth mentioning that 164 experts were contacted for the study of which 47 participated in the poll. We were able to carry out more than 20 personal interviews.

The second phase of the study was based on the qualitative analysis of the findings and the development of recommendations for different categories of stakeholders. As a result of the first stage of the study we had built up a large data source which comprised diverse information and consolidated it and normalized into a structured set of information, using dedicated, proprietary tools developed specially for this purpose. The basic element of it is a "key finding", it means the most relevant and influential observation from the desktop research, the survey and the interviews. Key findings may show an emerging issue, an

initiative taken or believed to be taken, an agreement/disagreement level between stakeholders, values or tendencies in the answers, a relevant line of opinion or any other piece of elaborated information that might have any impact in the field of ICS security. Once the key findings have been identified and treated, we can analyse them thoroughly in order to ultimately derive the recommendations.

Finally, the results of the study were presented for validation during a thematic workshop. The opinions gathered during the workshop and any other relevant issues are presented in Annex VI.

6 Key Findings

In this chapter we present the key findings discovered during the desktop research and the analysis of the results of the survey and interviews. The key findings have been grouped into various thematic categories, starting with what we consider the biggest challenges in ICS security, and continuing with a multiplicity of topics on ICS security, including:

- standards, guidelines, and regulatory documentation,
- information sharing,
- public-private partnerships and other initiatives,
- dissemination and awareness,
- technical security aspects,
- present and future of research,
- pending debates and other related issues.

To facilitate the reading, only short descriptions of the key findings are presented in this chapter. For further details of each key finding, including:

- An impact analysis
- Stakeholders involved or affected
- Areas or fields[7] in which they may have influence.

An interested reader is encouraged to refer to **Error! Reference source not found.**.

6.1 The biggest challenges in ICS security

6.1.1 Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)

At the EU level, there are policy areas addressing Critical Infrastructure Protection and Critical Information Infrastructure Protection. However, none of them are addressing ICS specifically. COM(2011) 163 recognizes that new threats have emerged mentioning Stuxnet explicitly. However, new activities proposed by this Communication on CIIP do not include any specific to ICS. In this context, ENISA has already stated that after Stuxnet, currently prevailing

[7] *Fields include: organizational and policy, standards, awareness and dissemination, economic/finance, and technical.*

philosophies on CIIP will have to be reconsidered (European Network and Informations Security Agency (ENISA), 2010). At the same time, the DHS in the USA established the Control Systems Security Program (CSSP) as a cohesive effort between government and industry to improve the security posture of control systems within the nation's critical infrastructure.

6.1.2 Challenge 2: The lack of a Common Reference in Europe (KF 1.2)

Most experts consider that there should be a European reference with regards to security standards, guidelines or regulations. This is particularly an issue when there are operators with presence in several countries (resulting from sector's fusions or mergers) with several control centres and autonomous organizational structures. These companies might have to deal with different regulations. Moreover, standards or guidelines being followed might not be the same in every division of the company. Some interviewees expressed that there is a need for a trustworthy European authority for ICS security, which would be the reference on which standards, guidelines and regulations should be followed, providing useful and practical information.

6.1.3 Challenge 3: The lack of integrated management of ICS security (KF 1.3)

It has been found, both during the desktop research and the questionnaire analysis, that one of the biggest issues that ICS operators have to face is to build security programmes that integrate all aspects of cyber security, incorporating desktop and business computing systems with industrial automation and control systems. Many organizations have fairly detailed and complete information security programmes for their business computer systems, but information security management practices are not as fully developed for ICS. Additionally, these companies normally have physical security programmes focused on preventing unauthorised access to facilities accommodating critical machinery which is part of the process being controlled or of the ICS itself. However, nowadays many cyber attacks can be combined with physical attacks to ICT systems to which access is not restricted. These systems might not have been considered critical for the process but they might be logically interconnected with critical systems. In fact, boundaries are fading as some attacks (and risks) that needed physical action years ago may be perpetrated in the cyber space nowadays.

6.1.4 Challenge 4: Lack of involvement of Top management (KF 1.4)

Operator's top Management is not considered to be involved enough in ICS logical security. Experts expressed that Top management usually consider cyber security a cost more than an investment, and that they have the wrong impression that they are already doing enough. It is essential to make Top Management realise that securing ICS is a key aspect that they should consider, also from an economical point of view (i.e. security as a business driver).

6.1.5 Challenge 5: Amortization of ICS investments (KF 1.5)

ICS systems technology has been developed in many cases for a very specific purpose and its implementation is different for each use case. This in turn has implied high investments from operators that are normally amortized during the next 15-20 years, or even longer. Most of these components do not include appropriate security mechanisms to protect them from today's threats and even less from tomorrows'. As a result, security staff will have to deal with ICS with little or no security capabilities for the next 10 – 15 years, and this will have to be taken into account when designing security plans.

6.1.6 Challenge 6: A long path for ICT security tools and services providers (KF 1.6)

Traditional ICT security companies have tried to penetrate the control and automation market in recent years. However, the ICS world is different from classic ICT systems and there are challenges that force them to adapt existing (or even create new) solutions and services. A fundamental difference is in the very basic guiding principles. The ruling security paradigm in classic ICT systems is based on the CIA model (Confidentiality, Integrity, Availability), but in the ICS environment what rules is the SRA model (Safety, Reliability, Availability). As a result, even though many security strategies, technologies and services may be exported from one world to the other, a much deeper reflection and ICS-oriented training in the ICT security industry is required.

6.1.7 Challenge 7: Adaptive Persistent Adversaries as the threat of the future (KF 1.7)

As ICS systems are often behind Critical Infrastructures, many self-organized, well supported and technically skilled adversaries may see ICS as the perfect target to sabotage for many possible reasons (e.g. terrorist attack, unfair competition, etc.). Terrorists, criminal organizations, rival companies, foreign states or independent groups can make use of different means (e.g. ad-hoc malware, highly qualified hackers, etc.) to attack these systems thanks to the increasing integration with ICT technology and other corporate systems. This is an increasing phenomenon (e.g. Stuxnet, Night Dragon) and many experts think it will grow during the following years.

6.1.8 Challenge 8: The security technical challenges of the Smart Grid: size, third party networks and customer privacy (KF 1.8)

The most challenging security factors of the adoption of the Smart Grid have been identified as: the overwhelming size of the networks, the trustfulness of third party networks for data transmission, and how to guarantee end customer privacy. Additionally, security challenges were commonly related to the deployment of secure smart meters. The remote control of these devices, together with a higher number of interdependencies and a distribution of control are considered factors that might increase the probability of weak points and cascade effects.

6.2 Standards, guidelines and regulations

6.2.1 Not all sectors are being targeted by EU policies (KF 2.1)

The Council Directive 2008/114 defined the procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure. This directive articulated the pillars of the EU framework for the protection of critical infrastructures that were defined in COM(2006) 768. However, this Directive only concentrates on the Energy (excluding also Nuclear Power plants) and Transport sectors, leaving place for a future review to include other sectors within its scope.

6.2.2 Current documents, usually generic (KF 2.2)

During the desktop research phase, 38 different documents were studied: 26 guidelines, 9 standards and 3 regulatory documents (enlisted in Annex III). Most of them can be considered as "generic", in the sense that they focus on security aspects affecting ICS from a general perspective.

6.2.3 Standards and guidelines target: ICS communications, ISMS and the definition of security profiles (KF 2.3)

Several guidelines provide advice based on industrial security good practices for relevant issues specific to ICS security and important efforts regarding the improvement and standardisation of the security of SCADA and DCS communications. A very important aspect of cyber security is to establish, within the company an Information Security Management System (ISMS). With regards to this there are several documents that have been studied which guide operators on how to include industrial control systems into their ISMS. Finally, there is a very useful set of documentation which addresses the security requirements/profiles and characteristics that new ICS components should include to comply with critical infrastructure protection programmes.

6.2.4 Energy, the sector with a greater number of specific guidelines (KF 2.4)

Some of the documents studied during the Desktop Research phase focus on specific sectors, with the Energy sector (including here oil, gas and electricity subsectors) being the most active one. Moreover, inside the Energy sector, it is the electricity subsector the one which presents, by far, the largest number of specific guidelines, standards and regulatory documents.

6.2.5 Transportation, Water Supply or Agriculture within the less active sectors (KF 2.5)

Sectors like transportation (e.g. railway transportation or airports), water supply (e.g. water distribution and waste water), or agriculture (e.g. food production) were not seen as being as active as the Energy sector with regard to the creation of security guidelines and standards for ICS protection.

6.2.6 Guidelines are "fresh" and "final" (KF 2.6)

Many new publications and updates have arrived in the last three years, from 2009 onwards. Actually, 18 of the 35 identified documents were published during that period. Additionally, most documents are in a final state, even though there are important initiatives that are yet in draft version such as the ANSI/ISA 99 and the IEC 62443 standards.

6.2.7 Lack of coordination among European countries (KF 2.7)

Many documents come from the United States of America or from international organizations such as IEEE, ISO, etc. At the same time, there are some countries in Europe that have defined on their own guidelines or even industrial mandates themselves. Some of the most active ones have been the United Kingdom, Germany, and Norway.

6.3 Acceptance and use of standards, guidelines and regulations

6.3.1 Good Practices and Standards are considered to be the most effective measures (KF 3.1)

Most survey respondents agree that the most effective mechanisms to secure ICS are Good Practices and Standards. A significant part of them stated that securing ICS must always be addressed as a combination of standards and guidelines together with awareness raising initiatives.

6.3.2 The most valued characteristics of security standards: a holistic approach, risk management guidance and business-orientation (KF 3.2)

Standards that had a holistic approach, that helped in risk management, and which have a business orientation were more appealing for the experts since they consider that their implementation tended to be more successful.

6.3.3 Too technical standards less valued (KF 3.3)

Too comprehensive or technical standards are normally not taken into consideration so much. Some respondents even warn about the danger of providing too much useful information for potential attackers.

6.3.4 On the costs of implementing guidelines: they are considered acceptable (KF 3.4)

Most of the interviewed stakeholders considered that implementing the "minimum" security measures proposed by the security guidelines is not very expensive. Operators are the ones that consider them assumable (probably due to the tender offer strategy they use to follow for product acquisition) while Security Tools and Services Providers and Manufacturers tend to consider them more expensive.

6.3.5 Low level of adoption of security guidelines and standards (KF 3.5)

Survey respondents showed that their current level of adoption of ICS security good practices was between low and medium, with Operators being the best positioned. Most of them are in the early stages of implementing security good practices, since they declared that they are currently developing a security plan or even performing the initial risk analysis. Among the problems they are facing they highlight the low level of involvement of Top Management or the lack of a common framework to follow.

6.3.6 Implementation of non European regulations, standards or good practices in industrial environments (KF 3.6)

International standards such as ISO 27002 or United States' guidelines are being followed widely. Moreover, companies are starting to comply with different aspects considered in regulations that are not to be applied in Europe, probably as a result of a lack of leadership in European authorities.

Some sectors are already starting projects to improve the security of their ICS due to the fact that there are specific regulations in place in the USA, such as the NERC CIP standards for the bulk electricity transportation or the NRG 5.71 for nuclear power plants (North American Electric Reliability Corporation (NERC), 2004-2010). However, there are other sectors that seem to be waiting for a specific mandate from public organisations before accomplishing such tasks.

6.3.7 Mistrust of guidelines causing heterogeneity (KF 3.7)

A wide variety of ways to deal with security threats, risks and challenges has been observed within the different participants of the survey and interviews. The most relevant reason for this heterogeneity is the lack of confidence in existing guidelines. This lack of confidence stems from various reasons that range from not being included into the "addressed audience" to not trusting the organisations, companies or groups behind those guidelines.

6.3.8 Disagreement between stakeholders on the effectiveness of regulations (KF 3.8)

Opinions are divided regarding the effectiveness of regulations, especially in Europe. Most Manufacturers and Operators' experts believe that this is not the best way to address security issues. Some others emphasize that there is a big difference between being compliant with a

regulation and being really secure. Only Security Tools and Service Providers and Academia have expressed direct support for it.

6.3.9 Manufacturers' negative attitude towards good practices and standards (KF 3.9)

Manufacturers participating in the survey and interviews have very little interest or even show a negative attitude towards most security standards of the industry. Some experts stated that since vendors are global companies, they are not strongly influenced by unilateral efforts and suggested that a joint European approach could be useful. ENISA was seen as an appropriate organisation to do so.

6.3.10 Compliance is not a market driver in ICS security (KF 3.10)

As there are no specific regulations to be compliant within the European ICS environment, it is not a driving factor for operators to invest in security technology even if most Security Tools and Service Providers think that it could help them foster the adoption of their solutions and the selling of their services.

6.3.11 No need for a specific law to prosecute cyber criminal targeting ICS (KF 3.11)

Stakeholders do not think that a specific law to prosecute ICS attacks is necessary as this is mostly covered by general regulation on cyber crime. Some of them state that some kind of amendment could be made to include aggravating factors. Some experts state that, in this respect, the USA is more advanced than European countries, but not all of them consider this to be better as they might have done it too fast.

6.3.12 The need for a European ICS security good practices documents (KF 3.12)

A majority of respondents consider that it is important, even urgent, to have a European collection of documents on ICS security good practices. Most respondents spontaneously said that it not necessary to “reinvent the wheel” and it would be desirable to cooperate with European Member States, the US, Asia or Oceania to quickly put together a collection of European ICS security good practices. However, there are some experts that do not feel comfortable with cooperating with USA organisations. Furthermore, cooperation within European affected stakeholders will be much appreciated. Several respondents pointed to ENISA and Euro-SCSIE as catalyst organisations to create/compile a collection of ICS security good practices.

6.4 The need for an Operators / Infrastructure level Security Plan

6.4.1 Need for an Operator/Infrastructure level security plan template (KF 4.1)

There is high consensus about the need for creating a reference security plan for each operator and/or infrastructure. Most believe a general template could be useful as a first step.

6.4.2 Sections to be included in the Operator/Infrastructure level security plan (KF 4.2)

Most respondents believe that the plan should include:

- operational and physical security,
- technical issues,
- training and awareness,
- security governance (roles and responsibilities),
- business impact measures, and
- crisis management.

6.4.3 Risk Management to be included in the ICS security plan (KF 4.3)

ICS on-field stakeholders should establish a process for assessing the current security posture of industrial control systems and for conducting risk analysis. It is important to understand what the information flows and system dependencies are, based on the consequences that a fault or disrupted function could have, both for the physical process being controlled and the organization itself.

6.4.4 Awareness topic to be included in the ICS security plan (KF 4.4)

On-field staff should have guidance regarding:

a) proper understanding of the current information technology and cyber security issues;

b) differences between ICT and ICS technologies, along with the process safety and associated management processes and methods;

c) developing practices that link the skill sets of all the organizations to deal with cyber security collaboratively.

6.4.5 Security plans need to be adapted for every operator (KF 4.5)

ICS usually consist of highly specialised deployments, designed for very specific purposes and to fulfil very precise requirements. Security projects deriving from the security plan normally include the implementation of technical, operational and management security controls. These controls should be tailored for each ICS since their applicability widely differ widely from their classic IT counterparts. Some examples of security controls that need some tailoring are: account management, separation of duties, least privilege principle, concurrent session control, remote access, auditable events, configuration change control, contingency plan testing and exercises, maintenance tools, remote maintenance, malicious code protection, security functionality verification, etc.

6.4.6 Developing security programs, too costly for operators (KF 4.6)

Developing and Implementing complete security programmes that incorporate ICS can be very costly. Many large operators are making use of compensatory controls to avoid investing lots of money in renewing old insecure devices, operating systems and software applications. However, smaller end users might find even this approach unaffordable.

6.5 Attitude towards information sharing and other collaborative Initiatives

6.5.1 Interest in sharing initiatives (KF 5.1)

Most stakeholders have expressed their interest in the creation or promotion of information sharing and mutual collaboration initiatives. They referred to the benefits coming from information sharing and collaboration between partners, such as the exchange of specific expertise and tools, the possibility of creating integrated solutions and promoting awareness. The information exchange may benefit from the participation of Academia and Public bodies as this provides a desirable, more objective point of view.

6.5.2 Excessive size, constraints or private interests are the main disadvantages and risks of sharing initiatives (KF 5.2)

Although the attitude is usually positive, several experts warned about negative aspects of this kinds of initiatives, such as:

- Loss of efficiency if they become too big
- Potential undesired constraints introduced by states
- Private companies' participation focusing only on defending their own interests instead of acting for the common good

6.5.3 Unbalanced interest in cooperation between each group of stakeholders (KF 5.3)

There are big differences regarding the interest that each kind of stakeholder has in cooperating with the others. Operators are the stakeholder group that is the most sought after, and they maintain an interest in others too. Academia is the stakeholder type with more interest in cooperating with others, but at the same time they do not receive much attention from other stakeholders. Manufacturers seem to be very focused on cooperation with Operators even though all other stakeholder types would like to cooperate more with them.

6.5.4 Active collaboration between the ICT security sector and ICS Manufacturers, essential to improve ICS security (KF 5.4)

The ICT security sector and ICS manufacturers' organizations should work collaboratively and bring their knowledge and skills together to tackle security issues. This is important since, in some cases, security practices are in opposition to normal production practices designed to maximize safety and continuity of production. Vendors might need to consider differentiating their ICS products based on the security functionalities they include.

6.5.5 Bilateral cooperation preferred to multilateral (KF 5.5)

A few experts stated that bilateral cooperation is usually more effective and efficient than multilateral initiatives.

6.6 Public Private Partnerships

6.6.1 PPP sharing initiatives demanded by most stakeholders (KF 6.1)

The majority of experts believe that public-private information sharing and collaboration initiatives are useful and necessary, as eventually they will lead to the improvement of the situation in the ICS security domain, even if they show different, sometimes contradictory, interests. Some experts even consider that without a facilitator (i.e. public sector), it is unlikely that private companies will get together. It is interesting however to highlight that both Manufacturers and Security Tools and Services Providers prefer other mechanisms to address ICS security challenges. In addition to usual sharing initiatives, public support can help long term funding, which is not always evident for companies, usually looking for short-term results and where true costs can be initially underestimated.

6.6.2 Not involving all stakeholder types and slowness- main critics regarding Public-Private Partnerships (KF 6.2)

Experts signalled several negative points of PPP's:

- Public entities do not always take all stakeholder types into account.

- Public guidelines that arrived late.

6.6.3 National or European funded security programs to be improved (KF 6.3)

A slight majority of stakeholders is participating in public programs to improve security in ICS. Participation is high particularly in research activities and also in Smart Grid issues, but more practical, better articulated, longer and more ICS oriented programs are demanded by interviewees.

6.6.4 Trust is an essential ingredient for the success of sharing initiatives (KF 6.4)

Several respondents had a good impression of some successful ICS security PPP initiatives. They consider them as a facilitator for cooperation and they particularly highlighted the importance of classifying information based on confidentiality levels. Privacy is of paramount importance for the success of these kinds of sharing initiatives.

6.7 Common test bed

6.7.1 Need for independent evaluations and tests of ICS security products (KF 7.1)

According to the operators, there is no difficulty in finding technical information on particular ICS security technologies or products. The problem is that the information comes from various sources, which are not necessarily considered as trusted sources. Operators indicate that independent evaluations and tests are missing.

6.7.2 Interest in creating a common test bed (KF 7.2)

A vast majority of participants were interested in the creation of a common test bed to certify technologies regarding ICS Security and interoperability.

6.7.3 PPP, a European scope and supported by Academia the desired characteristics of the common test bed (KF 7.3)

Respondents supporting the creation of a test bed believe that funding should come from public and private organisations and that the test bed should operate on a European level. A minority of respondents even think that technology certification by this test bed should be mandatory. Academia is willing to participate, as they have experience in creating minor test beds and have knowledge about methodologies.

6.7.4 Concerns regarding a European common test bed (KF 7.4)

Some respondents, and in particular ICS Manufacturers, are reluctant to see the creation of a European test bed. They do not think that Public Bodies should be very overly involved in the

technological aspects and that they do not like the kind of conclusions that are derived from such participation. Others think that it is unlikely that such an organisation could work fast enough to be useful.

6.7.5 A security reference model as an alternative to a European common test bed (KF 7.5)

A few experts signalled a different option that could have more support than a common European test bed. It would be the definition of a security model, such as Common Criteria or FIPS, adapted for ICS and the already existent certifying organisations in each Member State would be responsible for the certifying process. The reference standard would be used for this purpose and facilities should be available and configured and appropriate detailed test procedures should be defined.

ICS Operators, Manufacturers, certifying companies, etc. would need to verify and validate security configuration aspects, capabilities and interoperability of ICS including security features.

6.8 Dissemination and Awareness Initiatives

6.8.1 Space for improvement in Dissemination and Awareness Forums (KF 8.1)

Only two thirds of participants were aware of the current dissemination and awareness initiatives.

6.8.2 High interest in participating in Dissemination and Awareness Forums (KF 8.2)

A large number of stakeholders who were aware of dissemination and awareness forums were actively participating on them, due to their high interest in such initiatives.

6.8.3 Quality of “ICS security events” low-rated (KF 8.3)

Participants stated that the quality of “ICS security events” could be improved. They consider that they are too commercial (so too general) or too academic (without the presence of Manufacturers, Operators or Security Tools and Services Providers). Moreover, some interviewees stated that there are far too many conferences where it is too easy to get a paper published, in all domains not only in the security domain. Many experts think that there is a need for events addressing specific problems, existing standards or focused at Senior Management audiences.

6.8.4 Top Management awareness to be fostered (KF 8.4)

Many experts agreed that one of the main difficulties in improving ICS security is to defend security costs to the Top Management. There is a current of opinion that states that it has to

be presented as a business driver, providing economic reasons such as that, if considered during the PDCA cycle, it can be good for efficiency purposes. Incidents in industrial control systems should serve as a basis for risk assessment updates and to lead corrective measures and reprioritizing resource allocation. Organisations should address the challenge of establishing a group that meets regularly to discuss incidents and risks. This group should evaluate how these risks could impact security in the organisation's control systems. It should be composed by representatives from Management as well as from process control and IT.

6.8.5 Discussion on technology-centric forums (KF 8.5)

A few experts stated that Dissemination and Awareness Forums focus too much on security technologies or generic security aspects, not giving enough attention to the business aspects, such as the specific ICS implementations used in different activity sectors. Moreover, technologies may be adapted for several functionalities, but specific issues come from productivity and business objectives. Therefore, there is a need for dissemination and awareness initiatives focusing on specific activity sectors and which consider technology as a horizontal subject.

6.9 The usefulness of an ICS-computer emergency response capabilities or equivalent alternatives

6.9.1 Creation of an ICS-computer emergency response capability (KF 9.1)

According to a large number of experts an ICS-computer emergency response capability should be developed or in place.

6.9.2 PPP and cross-border as desired characteristics of an ICS-computer emergency response capability (KF 9.2)

Most respondents think that the ICS-computer emergency response capability should be operational on the cross-border level as well as on the national. It should be connected to the national/governmental CERT baseline capabilities and able in to cooperate on the Pan-European level, in order to address the challenges which span across the borders.

It should be promoted by ENISA. Respondents proposed that some of the activities of the ICS-computer emergency response capability could be providing guidelines and a vulnerability model.

6.9.3 Characteristics of the an ICS-computer emergency response capability (KF 9.3)

Some of the experts believe that this an ICS-computer emergency response capability should address ICS security issues by sector. This means that there should be specialised divisions for Energy, Transportation, Water, etc. The divisions should work in a coordinated manner.

6.10 Current situation of Technologic Threats and Solutions

6.10.1 Technical threats identified by experts (KF 10.1)

According to the respondents, the biggest technical challenges regarding ICS security are: legacy issues, ICS and ICT convergence issues (including common viruses, Stuxnet-like malware and increasing interest in hacking), practical difficulties in patching/vulnerability management, and unintentional human errors due to a lack of interest or understanding of ICS security issues.

6.10.2 ICS security "taken in their own hands" (KF 10.2)

Operators normally rely on third parties on issues that are not considered their core business for efficiency reasons. However, this is not the case as far as the ICS security is concerned.

6.10.3 IDS/IPS, DPI, VPN and NAC, the most recommended security technologies (KF10.3)

Intrusion Detection/Prevention Systems (IDS/IPS), Deep Packet Inspection (DPI), Virtual Private Network (VPN) and Network Access Control (NAC) technologies are the most popular security technologies for Operators, Academia and Security Tools and Service Providers. The next on the list of most applied solutions are: conventional firewalls, application white listing, host bastioning, wireless security and multi-factor authentication.

6.10.4 Discrepancies among stakeholders on the most appropriate security technologies (KF10.4)

Operators usually use IDS/IPS, VPN, Firewalls or Host bastioning technologies, while other tools pointed out by Security Tools and Service Providers and Academia (such as NAC, Wireless Security or DPI) are not widely adopted.

6.10.5 Discrepancies within most demanded/acquired security services (KF 10.5)

According to the survey, developing cyber security plans, performing penetration tests and risk analysis are the most recommended security services for the Operators. At the same time, Operators declare that they are only demanding security network (re)design and penetration tests. On the contrary, ICS Security Services Providers are providing risk analysis, security products deployment, compliance audits and host bastioning.

6.11 Legacy Related Risks

6.11.1 Untrusted and legacy devices and protocols - current biggest threat (KF 11.1)

According to the survey, the biggest threat to the security of ICS is the existence of untrusted devices. This is usually related to the use of legacy or proprietary technologies that often include security breaches (e.g. backdoors).

6.11.2 Legacy devices working under invalid assumptions and the long lifecycle of ICS (KF 11.2)

Obsolete technologies were designed with invalid assumptions such as that "devices are isolated", or "these systems are only understood by a small number of experts". These assumptions are no longer true. Built-in security is the best approach for protecting these systems, but for economical reasons a compensating, multi-layer approach is being implemented in most networks. The situation is worsened by the fact that ICS technologies lifecycle is much longer than the usual ICT lifecycles. As a result, many current ICS systems may remain vulnerable for longer.

6.11.3 Built-in security needed (KF 11.3)

Security requirements should be included in system specifications from the beginning. It is always much more difficult and expensive to implement compensating controls that solve the security deficiencies of these products designed and developed with no security requirements in their specifications. Often this is impossible, since many of the 'old' solutions do not have enough computing resources available to accommodate current security mechanisms. Additionally, third-party security solutions are not allowed due to ICS vendor license and service agreements.

6.11.4 Most Manufacturers already produce built-in security functionalities (KF 11.4)

During the interviews the majority of Manufacturers stated that their products were currently providing built-in security functionalities such as communication or password storage encryption.

6.11.5 Modular approach to built-in security requested by most on-field stakeholders (KF 11.5)

Most experts agree that for economic end reusability reasons it is more reasonable to design devices in a modular way. So, if a module needs to be updated or replaced, it can be done at a lower cost. This is also the recommended approach to be able to cope with the evolving threat panorama in the long life-cycles of ICS components.

6.12 ICT and ICS convergence problems

6.12.1 ICS importing the ICT solutions and the ICT problems (KF 12.1)

During the last few years ICT solutions have been becoming more and more common in ICS environments. Field devices have evolved from mechanical to electronic, relays have been replaced with microprocessors, computer operating systems and high level programming languages have been introduced to ICS. Control systems used to be built up on proprietary software but now many of them utilise standard applications or OS, or use IT systems such as TCP/IP networks. With this adoption of ICT solutions, ICS have also inherited their vulnerabilities. Additionally the increased complexity of software raises the likelihood of implementation flaws (such as software bugs).

6.12.2 Regular ICT solutions need to be adapted further to the ICS scenario (KF 12.2)

ICS tool providers still need to make an effort in adapting some of their technologies to the ICS world. For instance, Deep Packet Inspection in industrial firewalls is limited to a small subset of control protocols. Professional IDS/IPS solutions should start to commit to ICS protection, developing professional signatures and including new integral techniques. Data Loss Prevention is another technology with little acceptance in the ICS domain but which might become useful in the data exploitation process from historical and other business information processing applications and servers. Finally, only a small number of commercial available data diodes are compatible with industrial protocols (and only with a subset of all available industrial protocols) while they are still focusing on traditional ICT protocols such as FTP, SMTP, CIFS, etc.

6.12.3 ICT staff does correctly understand ICS requirements (KF 12.3)

A common problem mentioned by the ICS Security respondents was to make the ICT personnel (often in their own companies) properly understand the real needs and requirements of ICS environments. Some approaches regularly used in the ICT context can have catastrophic consequences if applied to ICS environments. Proper education must be given.

6.12.4 ICS providers are not aware of security good practices of the ICT world (KF 12.4)

Many ICS software and hardware vendors are not aware of programming good practices and methodologies. Penetration tests and white box audits, in controlled laboratories, have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included in the development cycle.

6.12.5 Warnings about ICT security vendors into ICS (KF 12.5)

Many respondents expressed their concern about the appearance during the last few years of conventional ICT security vendors, trying to sell their technologies to ICS operators without sufficiently understanding their requirements.

6.12.6 Potential role in ICS-ICT security integration (KF 12.6)

To correctly adapt security requirements and functionalities into the ICS environments, stakeholders from Academia may play an important role as they have the necessary resources. Developing theoretical frameworks to help both vendors and customers to understand what is needed and how to address it.

6.13 Other Technology Issues

6.13.1 Hardening often requires support from vendors and security tools and services providers (KF 13.1)

Hardening (e.g. restricting the permissions of running ICS applications) of computer solutions implies reducing the attack surface and therefore risks. ICS components cannot normally be hardened without a strong support from vendors and often requires Security Tools and Service Providers.

6.13.2 Difficulties with vulnerability management in the Operators side and in the commitment of Manufacturers (KF 13.2)

New vulnerabilities in ICS software and devices are discovered every day. Operators are often not prepared to address this issue in their systems. At the same time, ICS vendors don't provide an effective response to this demand quickly enough. Sometimes there are tensions between security researchers (who disclose vulnerabilities) and Manufacturers.

6.13.3 ICS security dependence of the ICT QoS (KF 13.3)

Quality of Service (QoS) parameters of the underlying ICT communication infrastructure are of paramount importance since many of the ICS need real-time performance, where delay and jitter are not acceptable.

6.13.4 Security in remote accesses (KF 13.4)

Enabling remote accesses to a control system by vendors, maintenance contractors, management staff accessing from their homes, etc. increases the exposure of the system to external threats. Therefore, it becomes necessary to introduce security for remote access. The introduced security measures must not impede or degrade the normal operational processes

that are critical for the control system to function normally. This may sometimes constitute a challenge.

6.13.5 Cloud computing not to be adopted in core ICS technologies (KF 13.5)

Cloud Computing is perceived by respondents as promising from some points of view, (for instance, for computational needs). But the majority stated that it is yet too immature or even, by its nature, not valid for the Control System itself, considering uses of QoS or real time functionalities. Even for valid use cases, some experts warned that every detail must be very clearly stated in Contract Agreements. One of the respondents indicated that standardized requirements at a European level would foster the adoption of this paradigm.

6.14 Present and Future Research

6.14.1 Current research lines (KF 14.1)

Currently and during the last few years, ICS security research has been focused on: testing methodologies and tools for system interdependencies, security and functionality metrics, access controls for devices, security in wireless networks, vulnerability analysis, Intrusion Detection Systems, study and test performance of current Smart Grid installations, Smart Grid standards and measures of effectiveness.

6.14.2 Future research lines (KF 14.2)

During the next few years, research lines are planned to focus on: more robust and flexible architectures, early anomaly detection by Network Behaviour Analysis (NBA) and Security Information and Event Management (SIEM) systems, patching and updating equipment without disruption to service and tools, methodologies to manage and integrate logic and physical threats, and improve forensic techniques for supporting criminal law enforcement.

6.14.3 Future threats a research topic (KF 14.3)

Experts considered that in the future their biggest technical challenges will be to deal with external targeted attacks, internal threats (both intentional and unintentional) as well as increased difficulties in the vulnerability management and privacy issues, due to the growth of Smart Grids.

6.15 Pending debates on ICS security and other related issues

6.15.1 The security by obscurity debate (KF 15.1)

There is a strong debate about the suitability of the "security by obscurity" approach. Many manufacturers and some other experts in different fields believe that this security philosophy is correct and even necessary. On the other hand, most ICT specialists and academia consider this is not an acceptable practice. For example, Standardization groups consider that the Industry should adopt a single cryptographic system rather than a diverse mix of systems that have not undergone public expert review. The system should be flexible to permit the introduction of new algorithms (ciphers) and new technologies after they are validated to be cryptographically secure.

6.15.2 The debate about regulation enforcement by penalties (KF 15.2)

A slight majority of respondents think that the regulation enforcement in Europe should not follow the NERC-CIP approach of the US.

6.15.3 Reasons against regulation enforcement by penalties (KF 15.3)

Several experts stated that it is not in the European culture to apply a regulatory approach, and that Good Practices and Standards should be used instead. Some pointed out that being compliant does not always mean being secure, with the former often being the only objective of Senior Management. They brought up the example of US companies trying to bypass the regulation and, hence, compromising security.

6.15.4 Reasons for regulation enforcement by penalties (KF 15.4)

Some experts believe that introducing penalties for not implementing regulations is an effective way to proceed at least to make the Senior Management aware, because the lack of compliance with the regulations will have a direct economic impact (and will be visible in the accounting reports). Others state that if Operators were more aware of the cascading effects that other Operators' security failures may have, they would prefer this type of enforcement for their own confidence.

6.15.5 Debate regarding Smart Grid dependency on third party telecomm Operators (KF 15.5)

A majority of stakeholders perceive as negative the dependency on third parties when providing Smart Grid services. However, there are a number of voices, especially from Academia, that consider it could provide benefits for Operators.

6.15.6 Concerns regarding Smart Grid dependency on third party telecomm Operators (KF 15.6)

Respondents are concerned because Operators don't have control or knowledge on the status of the network. Operators cannot identify, neither solve any problem independently of the telecommunication operator. Many agree to require encryption and signatures to prevent information leaks.

6.15.7 Positive points regarding Smart Grid dependency on third party telecomm Operators (KF 15.7)

A few respondents consider a benefit for operators to rely on specialized telecommunication companies, as this allows to Smart Grid Operators' to focus on their core business. At the same time there is a need for IT security monitoring technologies that allow maintenance personnel to quickly solve the problem or even to trigger automated actions that can minimize the impact. Relying on third party telecommunication operators might permit them to ask for this service.

7 Recommendations

This chapter presents 7 recommendations to improve the protection of ICS in Europe. They focus on national and pan-European initiatives that should be implemented as soon as possible. These recommendations are intended primarily for public bodies and authorities and specifically to the national and European ones. However, they also target other stakeholders such as ICS manufacturers, integrators and operators, security tools and services providers, academia and R&D, and standardisation bodies.

The seven recommendations are related to each other. Recommendation 1 presents the framework under which the subsequent seven recommendations should be included and interpreted. The remaining six recommendations should be coherent among them and with the common reference of Recommendation 1. These six recommendations address different ICS security topics and can be considered as equally important.

The detailed descriptions of the recommendations contain the following sections:

- Background: where the different motives that support the recommendation are briefly described. It can be considered as the “why” part of the recommendation.
- Related Key Findings: provides references to the Key Findings in which the Recommendation is based.
- Description: where the core content of the recommendation is presented. It can be considered as the “what” and the “how” parts of the recommendation.
- Objective: provides a more detailed description of what would be the benefits of this recommendation.
- Alternative: this subsection presents possible alternatives to the core proposal described in the “Description” section.
- Steps: suggests a number of possible phases to successfully implement the recommendation.
- Measures of success: suggests a number of metrics to evaluate the achievements of the recommendation.
- Stakeholders affected: lists those stakeholders that are affected by the recommendation and provides the level of involvement by assigning one of the following categories: leading, cooperating, consulting, none. This section can be considered the “who” part of the recommendation.

7.1 Recommendation 1: Creation of Pan-European and National ICS Security Strategies

7.1.1 Background:

Industrial Control Systems have been used for several decades. However, in the last few years ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. This has helped reducing costs and increasing efficiency while at the same time has resulted in making ICS vulnerable to computer network-based attacks. Even though there are multiple available good practices, technical reports, standards, etc. many security staff feels that they lack guidance coming from a trustworthy and objective reference authority. It seems that it is the moment to identify and unify existing efforts involving all different stakeholders and consider different perspectives in a coherent manner.

7.1.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Interest in sharing initiatives (KF 5.1)
- Excessive size, constraints or private interests are the main disadvantages and risks of sharing initiatives (KF 5.2)
- Unbalanced interest in cooperation between each group of stakeholders (KF 5.3)
- Active collaboration between the ICT security sector and ICS Manufacturers, essential to improve ICS security (KF 5.4)
- Bilateral cooperation preferred to multilateral (KF 5.5)
- PPP sharing initiatives demanded by most stakeholders (KF 6.1)
- Not involving all stakeholder types and slowness- main critics regarding Public-Private Partnerships (KF 6.2)
- National or European funded security programs to be improved (KF 6.3)
- Trust is an essential ingredient for the success of sharing initiatives (KF 6.4)

7.1.3 Description:

The European Union should create a pan-European Strategy for European ICS Security activities and each Member State should develop a National Strategy for ICS Security. The strategies must be coherent with the European Union Council Directive 2008/114/EC for Critical Infrastructures, and leverage the existing initiatives addressing the problem of ICS Security (e.g. EuroSCSiE) as well as the national and Pan-European Public Private Partnerships (e.g. EP3Rs). The strategies have to serve as references for all state-members stakeholders, act as facilitators for sharing initiatives and foster research and education.

7.1.4 Objective:

The strategies have to serve as a reference for all state-members' stakeholders, act as a facilitator for sharing initiatives and foster research and education. Taking advantage of such a structure, already existent efforts could converge, increasing their effectiveness and efficiency and enabling strategic long-term activities. Among the initiatives to be considered by such strategies, at least the following should be considered:

- Creation of good practices guides for ICS security
- Creation of ICS security plan templates
- Foster awareness and training through events and programmes
- Creation of a common test bed, or alternatively, an ICS security certification framework
- Creation of ICS-computer emergency response capability
- Foster ICS security research

These initiatives are fully detailed in the following six recommendations.

7.1.5 Steps:

- At the EU level, recommend Member States to create a National Security Strategy on ICS security.
- Current Member States' procedures to establish national strategies on ICS security should be followed.
- The most relevant stakeholders, both public and private, should be invited to take part on a Working Group (WG).

- Define a process to incorporate in the WG any other actor willing to participate once the WG is operative.
- Define the process of cooperation in the WG, with regular meetings and defining short-medium and long term objectives as well as developing a network of trust.
- Define the National ICS security strategy: scope, objectives, guiding principles, etc.
- Develop the Pan-European ICS security strategy. .

7.1.6 Measures of Success:

- Degree of involvement: All types of stakeholders, from public bodies -including the EU- to private actors should demonstrate their support by valuable contributions in both quantity and quality.
- Measure of satisfaction: The results of the different activities, from documentation to education must be useful for all involved members.
- Level of agreement: Regarding the activities and statements specified in the strategies.
- Tracking the validity of their long-term strategies: Accepting that they need to be flexible and adaptable, they must be coherent, with clearly defined, long term objectives.

7.1.7 Stakeholders affected:

- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: *consulting*
- Public bodies: **leading**
- Standardisation bodies: *consulting*

7.2 Recommendation 2: Creation of a Good Practices Guide for ICS Security

7.2.1 Background:

One of the clearest ideas that came up during the study is that most ICS security professionals are lacking guidance in how to implement their security solutions. Many have started to follow international guidelines, standards or local regulations in an attempt to improve the security of their ICS. However, they are still not confident enough about the suitability of these documents. Very often, they find themselves facing problems regarding the integration of physical and logical security. Moreover, companies operating in different EU member states, have to deal with different regulations (which in most cases are in an initial phase) that are not always easy to conciliate.

On the other hand, Industrial Control Systems are highly complex environments that depend heavily on the specific process and in the expertise of control and automation professionals. It is complicated to provide external guidance without understanding the deeper implications and cause-and-effect relationships that exist in a specific setup. For this reason, even if there is a debate regarding its effectiveness, most professionals do not feel comfortable regarding regulatory mandates and prefer good practices or voluntary standards as expert guidance.

7.2.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Challenge 2: The lack of a Common Reference in Europe (KF 1.2)
- Not all sectors are being targeted by EU policies (KF 2.1)
- Current documents, usually generic (KF 2.2)
- Energy, the sector with a greater number of specific guidelines (KF 2.4)
- Transportation, Water Supply or Agriculture within the less active sectors (KF 2.5)
- Lack of coordination among European countries (KF 2.7)
- Good Practices and Standards are considered to be the most effective measures (KF 3.1)
- The most valued characteristics of security standards: a holistic approach, risk management guidance and business-orientation (KF 3.2)
- Too technical standards less valued (KF 3.3)

- Implementation of non European regulations, standards or good practices in industrial environments (KF 3.6)
- Mistrust of guidelines causing heterogeneity (KF 3.7)

7.2.3 Description:

The European Union should assume leadership and develop a consensus-reached guide or set of guides regarding security good practices, integrating both physical and logical security aspects, to serve as a reference for all stakeholder types. This guide or set of guides should help every stakeholder to ensure that good security practices are applied in the industry. There are already international and member-state efforts, so it is not necessary to build this kind of documentation from scratch, but in a cooperative manner. Moreover, this Good Practice document should make clear reference to existing international standards supported by CEN/CENELEC.

7.2.4 Objective:

These documents or set of documents should help to make sure that good security practices are applied within the industry. Considering the results from the study, this sort of documentation could be better accepted and applied if it takes into account the following objectives:

- Unified reference: This set of documents should be an ICS security unified reference for every European stakeholder. For this reason, a holistic approach, including risk management guidance and business related issues would be more appreciated. On the other hand, excessive technical depth may make the document less helpful, as it could be too specific for most of the audience.
- Targeting every sector where ICS are used in CI's: The number of ICS security guidelines is dissimilar between the different industry sectors. Standards and good practices of reference for different sectors must be included, even if some of them have not been considered so critical up to now (e.g. water, transportation, etc.).

7.2.5 Steps:

In order to make these guidelines useful over time it is necessary to:

- Contact international and national peers that already have experience in developing these kinds of guidelines to speed things up and make the most of previous experiences. ENISA, or any other competent organisms, could be in charge of this.

- Establish a working group including all stakeholders, to receive cooperation from both Public and Private sector expertise.
- Publish the Good Practices document but providing mechanisms to receive future inputs and subsequently updating it.

7.2.6 Measures of Success:

To consider the set of documents or guidance documentation a success, the following metrics should be taken into account:

- The degree of adoption in the industry.
- The degree of satisfaction of the different stakeholders regarding the effectiveness of the solutions provided.
- How much experts are engaged with the creation of these set of documents, providing their knowledge and participating on the evolution of the document.

7.2.7 Stakeholders affected:

- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: cooperating
- Public bodies: **leading**
- Standardisation bodies: cooperating

7.3 Recommendation 3: Creation of ICS security plan templates

7.3.1 Background:

ICS are highly specialised infrastructures, designed and customised for very specific purposes and to fulfil very precise requirements. Each activity sector has a number of ICS that are used for different purposes. Moreover, inside the same sector each operator has their own particular implementation of these ICS. At the same time, security projects deriving from the

security plan[8] normally include the implementation of technical, operational and management security controls. These controls should be tailored for each ICS since their applicability widely differ from their classic IT counterparts. Some examples of security controls that need some tailoring are configuration change control, maintenance procedures, security functionality verification, and contingency plan testing. Moreover, the integration of physical and logical security and the educational factor are sometimes disregarded or not a priority. Due to the current European policy context, most operators have developed (or are in the process of developing) their own Operator or Infrastructure security plans with great effort and economic costs, and probably not in the most efficient manner. Besides, they are not always comfortable with the results, as system dependencies are often extremely complex making it difficult to do risk analyses well, which is the first and basic step for any security plan. This results in an insecure top management not trusting the effectiveness of such plans.

7.3.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Challenge 2: The lack of a Common Reference in Europe (KF 1.2)
- Need for an Operator/Infrastructure level security plan template (KF 4.1)
- Sections to be included in the Operator/Infrastructure level security plan (KF 4.2)
- Risk Management to be included in the ICS security plan (KF 4.3)
- Awareness topic to be included in the ICS security plan (KF 4.4)
- Security plans need to be adapted for every operator (KF 4.5)
- Developing security programs, too costly for operators (KF 4.6)

7.3.3 Description:

The different National ICS Security Strategies introduced in Recommendation 1 should consider within their tasks the creation of ICS security plan templates, both for Operator and Infrastructures, which security experts could adapt to their particular situation. These plans should include operational and physical security, technical issues, training and awareness, security governance with roles and responsibilities, business impact measures and crisis

[8] *A security plan details how the rules defined in a security policy will be implemented. A security policy identifies the rules that will be followed to maintain security in a system. A security policy is generally included within a security plan. (Theriault & Heney, 1998)*

management. Furthermore, these templates should be coherent with the set of good practices documents defined in Recommendation 2.

7.3.4 Objective:

These templates should guide operators in the classification of their ICS systems and networks, helping them to prioritise the most critical ones as well as to define the different security projects. For instance, they will define how operators should accomplish the risk analysis (e.g. methodology that should be used, assets to include, etc.) and how the information should be exchanged with the public authorities. Moreover, it would be very much appreciated if for each sector and subsector concrete examples are also included as a reference. These examples should also focus on how to tailor specific security controls for hypothetical but realistic reference scenarios, or use cases. It is considered that such templates will severely decrease the cost of developing security plans and accelerate the adoption of comprehensive security measures within the industry. Furthermore, these templates, since they will have a standard format, will make it easier to evaluate the security plans of each operator and CI by the competent public authority.

7.3.5 Steps:

Security plans can be reached by the following steps:

- Establish a working group comprised especially of industry experts to identify all generic needs, understand the problems that operators are facing when preparing such plans, study success stories in other Member States and select the most appropriate ones as a reference model.
- Prepare a set of templates for each activity sector including examples of security projects. These templates should be coherent with the set of good practice documentation defined in Recommendation 2.
- Publish the Template, with proper documentation to adapt to current situations.
- Consider the possibility of preparing a web-based support tool as guidance for the first steps: classification, prioritising, definition of the different security projects, etc.
- Provide mechanisms to collect experiences and update the document.

7.3.6 Measures of Success:

To evaluate the success of the templates, at least the following aspects should be considered:

- How much and in which way are they used by operators.

- The degree of satisfaction regarding the cost decrease and the effectiveness of the solutions provided.
- The implication of companies regarding contributions and feedback.

7.3.7 Stakeholders affected:

- Manufacturers and integrators: *consulting*
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: *consulting*
- Public bodies: **leading**
- Standardisation bodies: none

7.4 Recommendation 4: Foster Awareness and Training

7.4.1 Background:

Awareness of the risks and available safeguards is the first line of defence for security of information systems and networks.

Awareness raising is not only about being aware of the risks involved in using the electronic communication systems, but far more about making the users aware of how to protect themselves online and how to use their information systems and products in a secure manner. The OECD guidelines towards a culture of security, state that “awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks”. The fact that security aware users are a prime requisite for increased trust in the online services as well as for the wide-spread information society has been recognised in all Member States.

At the same time, there is still a strong debate about the suitability of the “security by obscurity” approach. Again, awareness and training is a the most useful security measure to overcome false myths and understand how threats are changing and what is the best way to fight against them.

The organizational maturity required for fostering awareness and training among manufacturers, integrators and operators can only be achieved if serious commitment comes from an organisation’s top management. During the study, many security experts signalled that one of their most challenging tasks was to make their superiors aware of actual risks and

threats, and to get them involved in order to successfully define and implement operator/infrastructure security plans or to take into account security requirements in product design, manufacture and commission. Experts expressed that Top management usually consider cyber security a cost more than an investment, and that they mistakenly believe that they are already doing enough.

It has been detected that there already exist dissemination and awareness raising events calling for attention. However, the quality is poorly rated by the attendants, considering them too commercial or academic, without providing real answers, and not targeting Top Management.

7.4.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Challenge 4: Lack of involvement of Top management (KF 1.4)
- PPP sharing initiatives demanded by most stakeholders (KF 6.1)
- Space for improvement in Dissemination and Awareness Forums (KF 8.1)
- High interest in participating in Dissemination and Awareness Forums (KF 8.2)
- Quality of “ICS security events” low-rated (KF 8.3)
- Top Management awareness to be fostered (KF 8.4)
- ICS providers are not aware of security good practices of the ICT world (KF 12.4)
- The security by obscurity debate (KF 15.1)

7.4.3 Description:

As part of national ICS-Security strategies, the Member States should foster dissemination and awareness activities through high quality events involving all types of stakeholders and with special attention to top management commitment. Training and awareness programmes and events should be created for all end user types and other stakeholders such as manufacturers and integrators. These initiatives can focus among other things on existing standards and good practices on ICS security, to disseminate their content and raise end user awareness. Other possible topics can be the discussion about the suitability of the “security by obscurity” paradigm and other pending debates affecting the security of ICS.

Several events could be created, targeting real security problems in each sector. These initiatives should be mainly vertical (i.e. sector-based) with some others focusing on horizontal aspects: technology, security solutions, etc., but with the common guiding principle

of differentiating different activity sectors. Special attention should be given to the quality of these initiatives, avoiding duplicated work programmes, and assuring the quality of the speakers.

7.4.4 Objective:

If top management is engaged then this could be expected to make real security improvements. With top management as the main target of security awareness and training initiatives, the whole organisation will be reached and a security culture will be easily built. All the staff will acquire proper understanding of current information technology and cyber security issues and their relation with physical, environmental and safety aspects of process control and automation.

7.4.5 Steps:

- Member States should create or get actively involved in the organisation of existing forums and events regarding ICS security. This could be leaded by the competent National authority.
- Identify experts among each stakeholder type that are able to differentiate myths from realities and to provide reliable arguments and expose them in an understandable manner for any kind of stakeholder.
- Focus on top management by showing real security problems that could affect their business.
- Look for cooperation from ICS leading-companies' managers and show how security gestures may (positively) affect business results.

7.4.6 Stakeholders affected:

- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: **leading**
- Academia and R&D: cooperating
- Public bodies: **leading**
- Standardisation bodies: none

7.5 Recommendation 5: Creation of a common test bed, or alternatively, an ICS security certification framework

7.5.1 Background:

Interoperability has always been critical in ICS infrastructures for system reliability and availability. On the other hand, many ICT security vendors are now trying to sell their technologies (e.g. antivirus, whitelisting technology, etc.) and services (e.g. security assessments) to ICS operators without deeply understanding their impact in the operation of real ICS.

Additionally, ICS manufacturers are starting to (or will have to) include security requirements in the design phase of ICS components and applications. However, operators indicate that independent evaluations and tests are missing to effectively guarantee that those devices are in fact secure and that interoperability has also been considered when the new security features/capabilities are included.

Furthermore, penetration tests and white box audits in controlled laboratories have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included into the development cycle.

In any case, manufacturers, ICS security tools and services providers, as well as operators cannot be completely aware of the implications a modification may have with respect to their own systems or third party ones. Moreover, it is important to certify that ICS do comply with minimum quality requirements with respect to cyber security programming bugs.

7.5.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Need for independent evaluations and tests of ICS security products (KF 7.1)
- Interest in creating a common test bed (KF 7.2)
- PPP, a European scope and supported by Academia the desired characteristics of the common test bed (KF 7.3)
- Concerns regarding a European common test bed (KF 7.4)
- A security reference model as an alternative to a European common test bed (KF 7.5)
- Warnings about ICT security vendors into ICS (KF 12.5)
- ICS providers are not aware of security good practices of the ICT world (KF 12.4)

7.5.3 Description:

The Common ICS security strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership that leverages existing initiatives (e.g. EuroSCSiE). This test bed would make use of realistic environments with the appropriate resources for conducting independent verification and validation tests. These tests should include, at least:

- Check the compliance of applications and systems with specific security profiles.
- Verify and validate that programming good practices and methodologies are being applied.
- Certify that ICT security tools and services are compatible with specific ICS systems, applications and specific setups.

Product/services certification would not be mandatory but should also be considered as an option.

7.5.4 Objective:

A common test bed will help all stakeholders to detect potential problems in a controlled environment, ensuring integrity and increasing the trustfulness on certified/tested solutions. Moreover it will provide operators with independent security evaluations and a common security reference so that they are supported when deciding which products/services to buy.

Alternatively a security framework model adapted for ICS could be defined, based on existing efforts such as Common Criteria or FIPS. Member State existing certifying organisms would be responsible for the certification process based on this security framework.

7.5.5 Steps:

- Coordinate a group to clearly define the purpose of such a test bed.
- Identify the requirements and design the organisation of such a test bed.
- Get involved the main actors: ICS manufacturers, security tools and services providers.
- Develop the test bed: infrastructures, procedures, metrics, etc. Academia may be particularly helpful as they have experience in such kind of environments. Moreover, standardisation bodies could help standardising such procedures, metrics, etc.

7.5.6 Measures of Success:

The test bed could be considered successful if:

- ICS Manufacturers and Integrators, ICS Security Tools and Services Providers accept the results as trustful.
- The speed of security measures adoption is increased.
- The battery of tests is demonstrated to be comprehensive.

7.5.7 Alternative:

Al alternative option to a European common test bed is the definition of a security framework model, such as Common Criteria or FIPS, adapted for ICS. In each Member State a national certifying authority exists which, based on a certification framework (e.g. Common Criteria or FIPS), is in charge of checking the compliance of applications and systems with specific security profiles.

Therefore, Member State existing certifying organisms would be responsible for the certification process: verify and validate security configuration aspects, capabilities and interoperability of ICS devices and security tools. Moreover, a European coordination group could be defined to avoid duplicated work. For instance, once a product is certified in a Member State's national laboratories, it wouldn't be necessary to certify it once again.

7.5.8 Stakeholders affected:

- Manufacturers and integrators: cooperating or *consulting*
- ICS Security tools and services providers: *consulting*
- Operators: *consulting*
- Academia and R&D: cooperating
- Public bodies: **leading**
- Standardisation bodies: cooperating

7.6 Recommendation 6: Creation of national ICS-computer emergency response capabilities

7.6.1 Background:

A Computer Emergency Response Team (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The team provides the necessary

services to handle them and support their constituents to recover from computer security breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency. The constituency (an established term for the customer base) of a CERT usually belongs to a specific sector, like academia, companies, governments or military. The term CSIRT (Computer Security Incident Response Team) is a more modern synonym and should reflect the fact that CERTs developed over time from being mere reaction forces towards more universal providers of security services[9].

There are many CERTs in the European Union, both public and private, but very few of them are specifically prepared for ICS security issues. On the other hand, the idea of creating a Euro-CERT[10] is not currently considered as an attractive option by Member States.

ICS are behind many CI's. These CI's are part of strategic sectors such as Energy, Transportation, Water, or Food. Interdependencies among CI's make it possible to have cascading effects that can span multiple Member State countries if a security incident affects a critical component of a CI (e.g. a key ICS). Therefore, it would be necessary to coordinate and respond, in an effective and efficient manner, to possible risks, events, incidents, or any other type of security information related to ICS systems behind European Critical Infrastructures (ECI's).

Finally, there is a need for a specific organization to host, maintain and foster some of the initiatives previously presented: European ICS security documents, security plan templates, awareness and training events and programmes.

7.6.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Creation of an ICS-computer emergency response capability (KF 9.1)
- PPP and cross-border as desired characteristics of an ICS-computer emergency response capability (KF 9.2)
- Characteristics of the an ICS-computer emergency response capability (KF 9.3)

7.6.3 Description:

Following the national ICS Security Strategies, national ICS-computer emergency response capabilities should be established, in cooperation with an adequate number of public and

[9] *http://www.enisa.europa.eu/act/cert/support/baseline-capabilities*

[10] *It is worth to mention that in the past, an initiative aiming at establishing European Coordination Centre for CERTs, called EuroCERT, failed. More information can be found in: https://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders (p. 23-24).*

private CERTs. The capabilities should leverage on the initiatives deriving from previous recommendations being the visible reference for ICS stakeholders.

They should structure their activity by business/sector rather than by technologies. This means that there should be specialised divisions for Energy, Transportation, Water, etc. Some experts consider that, usually, problems are more related to production functionalities than with the technology itself. Especially, in cases such as ICS environments in which systems based on the same solutions can vary heavily on the functionality they are designed for. An advantage of this division is that top management would be more likely to become involved if they can see business orientation in the initiative.

Reasoning on the previous ideas, the ICS-computer emergency response capabilities should be focused on the following services:

- Centralising ICS security good practice set of guides
- Centralising security plan templates
- Fostering of awareness and training events and programmes
- ICS components and applications vulnerability disclosure coordination
- Coordinate ICS security incidents: information sharing, crisis management, etc.

7.6.4 Objective:

The ICS-computer emergency response capabilits should help all stakeholders to have a reference in order to share vulnerability information, disclose it, coordinate actions and help in effectively dealing with risk management by providing reference security documentation, security plan templates, and by fostering awareness and training initiatives in the context of ICS security. In order to address the challenges which span across the borders, member states should cooperate on the Pan-European level (e.g. with the aid of an ICS-Security information sharing platform such as EuroSCSiE).

7.6.5 Steps:

In order to create such a structure it would be necessary to:

- Consider other initiatives to find synergies and avoid duplicated efforts.
- Contact Member State authorities to coordinate the collaboration with national public and private CERTs. The contributions from every public and private actor involved should be clearly defined.
- Define the ICS-computer emergency response capability functional and operational duties.

- Create the ICS-computer emergency response capability, providing budget.

7.6.6 Measures of Success:

The ICS-computer emergency response capability could be considered successful depending on:

- The effectiveness on providing solutions to emerging vulnerabilities.
- The degree of implication of every sharing-actor.
- The acceptance of all stakeholder of its authority regarding vulnerability disclosure information.
- The coordination effectiveness and efficiency of ICS-related security incidents.

7.6.7 Stakeholders affected:

- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: *consulting*
- Public bodies: **leading**
- Standardisation bodies: *consulting*

7.7 Recommendation 7: Foster research in ICS security leveraging existing Research Programmes

7.7.1 Background:

The expertise of Academic and Security professionals is very much needed in the field of ICS security. For a long time control systems were so isolated and have been managed, developed, and installed by professionals who didn't consider cyber security as a priority.

Now the situation has changed dramatically. Standard ICT technologies are very present, even if the philosophical approach to security is radically different (Confidentiality-Integrity-Availability versus Safety-Reliability-Availability). Many proprietary and legacy solutions that are currently in production (and will certainly stay there for at least the next ten years) were

designed under assumptions that would not be valid today. There is still also a fierce debate regarding the suitability of concepts such as “security through obscurity” that must be resolved. On top of all this, there are new technical challenges to address, such as targeted attacks and Adaptive Persistent Adversaries or Smart Grid related issues.

Research efforts have proven to be effective in the past as it has been verified during the study. However it is also clear that such programmes could be improved.

7.7.2 Related Key Findings:

- Challenge 1: The lack of specific initiatives on ICS security (KF 1.1)
- Challenge 7: Adaptive Persistent Adversaries as the threat of the future (KF 1.7)
- Challenge 6: A long path for ICT security tools and services providers (KF 1.6)
- ICS importing the ICT solutions and the ICT problems (KF 12.1)
- Regular ICT solutions need to be adapted further to the ICS scenario (KF 12.2)
- Current research lines (KF 14.1)
- Future research lines (KF 14.2)
- Future threats a research topic (KF 14.3)
- Regular ICT solutions need to be adapted further to the ICS scenario (KF 12.2)
- Modular approach to built-in security requested by most on-field stakeholders (KF 11.5)

7.7.3 Description:

The National and Common ICS Security Strategies should foster research to address current and future threats and challenges such as ICS-ICT integration, legacy/insecure equipment, targeted attacks or Smart Grid issues. This should be done by leveraging existing European or National research programmes, such as the European Framework Programme.

A future work programme for research in ICS security should include the following topics at least:

- Robust and flexible architectures (e.g. modular approach for security)
- Early anomaly detection by Network Behaviour Analysis (NBA) and Security Information and Event Management (SIEM) systems

- Patching and updating equipment without disruption of service and tools
- Methodologies to manage and integrate logic and physic threats
- Improved forensic techniques for supporting criminal law enforcement
- Adaptation of current ICT security solutions to ICS environments

7.7.4 Objective:

The general objective is to improve the security and reliability of ICS systems. Some of the most urgent topics are:

- Establish a transposition framework to adequate conveniently ICT security technologies into ICS requirements. There is a key philosophical challenge in this field, as it is the culture of security that has to be adapted. An academic approach on this topic might be an extremely valuable contribution.
- Define the best ways to address legacy challenges as well as built-in security needs.
- Measure the effectiveness, identify the advantages and disadvantages, and obtain objective conclusions to resolve the “security through obscurity” debate and disseminate the results.
- Study new techniques to address the targeted attacks made by organized Adaptive Persistent Adversaries such as Network Behaviour Analysis or Security Information and Event Management systems.
- Identify and proceed with Smart Grid related issues such as the high amount of data, end-user privacy or measure the suitability of using third party telecoms networks.

7.7.5 Steps:

It would be necessary to:

- Establish priorities for the different research objectives in accordance with the National and Common ICS Security Strategies.
- Make contact with existing security programmes at EU and National levels, such as the European Framework Programme.

- Work together with appropriate organisations and bodies (e.g. Framework Programme Committee and Advisory Groups, Technology Platforms, etc.) to define an appropriate Work Programme.
- Emphasize results dissemination, especially those that can help to shed light on pending debates.

7.7.6 Measures of Success:

This recommendation could be considered a success if:

- Both public and private actors are implicated.
- Problems are resolved before they become urgent.
- Efforts are coordinated and offer additional or synergic solutions between them.

7.7.7 Stakeholders affected:

- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: **leading**
- Public bodies: **leading**
- Standardisation bodies: none

8 Conclusions

Recent cyber security incidents such as Stuxnet or Night Dragon provided the real evidence of how vulnerable Industrial Control Systems are. These systems are responsible for monitoring and controlling processes in infrastructures, which are very often vital for critical services in Europe. The EU has acknowledged the importance of the fact and since 2004 the European Commission and the Council of Justice and Home Affairs has been carrying a series of actions that resulted in the European Programme for Critical Infrastructure Protection (EPCIP). In parallel, the information security issues for vital infrastructures in Europe have been addressed by The Digital Agenda for Europe (DAE) and the Critical Information Infrastructure Protection (CIIP) action plan. Specifically, the last Communication on CIIP, CIIP COM(2011)163, targets ICS security by explicitly mentioning Stuxnet as the spearhead of new threats looking for disruption and destruction purposes.

In order to define European-wide actions on ICS security, the first step is to understand the current situation of ICS protection. Therefore it is essential to take stock of the on-going activities, policy contexts, existing standards, guidelines and regulations in the national (Member-States) and pan-European level but also in the international context. Moreover, the current situation cannot be fully described without an overview on the challenges, emerging issues, threats and solutions in place. For instance, the relationship between ICS and the new Smart Grid or underlying Telecommunication infrastructures could be considered relevant for the future actions on ICS security.

Additionally, the most appropriate way to recognise the current situation of ICS security is to facilitate the open dialogue among the stakeholders, by actively involving the private and the public sectors. ENISA facilitates this dialogue by identifying the relevant parties, getting them together and providing the basis for discussions. Moreover, ENISA, as an EU body of expertise in Network and Information Security (NIS), is supporting the European Commission's CIIP action plan.

As a result, in 2011, ENISA conducted the study on the ICS Security and identified threats, risks and challenges in the area as well as took stock of national, pan European and international initiatives on ICS security. Moreover, based on the active collaboration of experts belonging to ICS-related sectors, the study proposed good practices and recommendations that aim at helping to improve the security, safety and resilience of European ICS systems. Seven areas have been identified as of priority: development of ICS strategies, good practices, security plan templates, awareness raising, test beds/maturity frameworks, ICS-computer emergency response capabilities, and research.

ENISA considers that these recommendations are effective, achievable, and urgent. This opinion is also shared by the experts who attended the ICS security workshop in which these recommendations were presented. Furthermore, these experts suggested a close follow-up of this report and proposed the European Public-Private Partnership for resilience (EP3R), the European Union's Public-Private Partnership, as the umbrella to discuss further the

recommendations provided. However, ENISA believes that the real state of security of Industrial Control Systems can be only achieved with a common effort of all stakeholders.

9 References

American Gas Association (AGA). (2006). *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 1 Background, policies and test plan.* American Gas Association.

American Gas Association (AGA). (2006). *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 2 Performance Test Plan.* American Gas Association.

American National Standard (ANSI). (2007). *ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models.* International Society of Automation (ISA).

American National Standard (ANSI). (2007). *ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems.* International Society of Automation (ISA).

American National Standard (ANSI). (2009). *ANSI/ISA–99.02.01–2009 Security for Industrial Automation and Control Systems. Part 2: Establishing an Industrial Automation and Control Systems Security Program.* International Society of Automation (ISA).

American Petroleum Institute (API) energy. (2005). *Security Guidelines for the Petroleum Industry.* American Petroleum Institute.

American Petroleum Institute (API) energy. (2009). *API Standard 1164. Pipeline SCADA Security.* American Petroleum Institute.

Amin, S., Sastry, S., & Cárdenas, A. A. (2008). *Research Challenges for the Security of Control Systems.*

Asad, M. (n.d.). *Challenges of SCADA.* Retrieved 2011, from http://www.ceia.seecs.nust.edu.pk/pdfs/Challenges_of_SCADA.pdf

Bailey, D., & Wright, E. (2003). *Practical SCADA for Industry.* Newnes.

Berkeley III, A. R., & Wallace, M. (2010). *A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council.* National Infrastructure Advisory Council.

Boyer, S. A. (2004). *SCADA Supervisory and Data Acquisition.* Retrieved 2011, from http://www.fer.unizg.hr/_download/repository/SCADA-Supervisory_And_Data_Acquisition.pdf

Boyer, S. A. (2010). *SCADA: Supervisory Control and Data Acquisition.* Iliad Development Inc., ISA.

Centre for the Protection of Critial Infrastructure (CPNI). (n.d.). *Meridian Process Control Security Information Exchange (MPCSIE).* Retrieved 2011, from http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie

Centre for the Protection of Critical Infrastructure (CPNI). (n.d.). *CPNI*. Retrieved 2011, from http://www.cpni.gov.uk/advice/infosec/business-systems/scada

Centre for the Protection of National Infrastructure (CPNI). (2005). *Firewall deployment for scada and process control networks.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (2011). *Configuring & managing remote access for industrial control systems.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (2011). *Cyber security assessments of industrial control systems.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 1. Understand the business risk.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 2. Implement secure architecture.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 3. Establish response capabilities.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 4. Improve awareness and skills.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 5. Manage third party risk.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 6. Engage projects.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 7. Establish ongoing governance.* Centre for the Protection of National Infrastructure.

CI2RCO Project. (2008). *Critical information infrastructure research coordination*. Retrieved 2011, from http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=79305

Commission of the European communities. (2004). *Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final.*

Commission of the European communities. (2004). *Communication from the commission to the council and the European parliament. Prevention, preparedness and response to terrorist attacks COM(2004) 698 final.*

Commission of the European communities. (2005). *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.*

Commission of the European communities. (2006). *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.*

Commission of the European communities. (2006). *Communication from the commission to the council, the European parliament, the European economic and social commitee and the commitee of the regions. A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment' COM(2006) 251.*

Commission of the European communities. (2008). Council decision on a Critical Infrastructure Warning Information Network (CIWIN) COM(2008) 676».

Commission of the European communities. (2008). *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.*

Commission of the European communities. (2009). *Communication from the commission to the European parliament. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.*

Commission of the European communities. (2011). *Communication from the commission to the European parliament, the European economic and social commitee and the commitee of the regions. Achievements and next steps: towards global cyber-security.*

CRUTIAL Project. (2006). *CRitical Utility InfrastructurAL resilience*. Retrieved 2011, from http://crutial.rse-web.it

Department of Energy (DoE). (2002). *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities.* Department of Energy.

Department of Energy (DoE). (2008). *Hands-on Control Systems Cyber Security Training of National SCADA Test Bed.* Retrieved 2011, from http://www.inl.gov/scada/training/d/8hr_intermediate_handson_hstb.pdf

Department of Energy (DoE). (2010). *Cybersecurity for Energy Delivery Systems Peer Review.* Retrieved 2011, from http://events.energetics.com/CSEDSPeerReview2010

Department of Energy (DoE). (n.d.). *21 Steps to Improve Cyber Security of SCADA Networks.* Department of Energy.

Department of Energy (DoE). (n.d.). *Control Systems Security Publications Library*. Retrieved 2011, from http://energy.gov/oe/control-systems-security-publications-library

Department of Homeland Security (DHS). (2003). *Homeland Security Presidential Directive-7.* Retrieved 2011, from http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

Department of Homeland Security (DHS). (2009). *Catalog of Control Systems Security: Recommendations for Standards Developers.*

Department of Homeland Security (DHS). (2009). *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Department of Homeland Security.

Department of Homeland Security (DHS). (2009). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies.

Department of Homeland Security (DHS). (2011). *Cyber storm III Final Report.* Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division.

Department of Homeland Security (DHS). (2011). *DHS officials: Stuxnet can morph into new threat.* Retrieved 2011, from http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat

DigitalBond. (n.d.). *DigitalBond.* Retrieved 2011, from ICS Security Tool Mail List: http://www.digitalbond.com/tools/ics-security-tool-mail-list

Energiened. (n.d.). *Energiened Documentation*. Retrieved 2011, from http://www.energiened.nl/Content/Publications/Publications.aspx

Ericsson, G. (n.d.). *Managing Information Security in an Electric Utility.* Cigré Joint Working Group (JWG) D2/B3/C2-01.

ESCoRTS Project. (2008). *Security of Control and Real Time Systems*. Retrieved 2011, from http://www.escortsproject.eu

ESCoRTS Project. (2009). *Survey on existing methods, guidelines and procedures.*

eSEC. (n.d.). *eSEC*. Retrieved from Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza: http://www.idi.aetic.es/esec

European Network and Informations Security Agency (ENISA). (2010). Retrieved 2011, from EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection: http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier.* Symantec.

Gartner. (2008). *Assessing the Security Risks of Cloud Computing.* Retrieved 2011, from Gartner: http://www.gartner.com/DisplayDocument?id=685308

Ginter, A. (2010). *An Analysis of Whitelisting Security Solutions and Their Applicability in Control Systems.* Retrieved 2011

Glöckler, O. (2011). *IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in NPPs.* Retrieved 2011, from http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/Day-3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf

Goméz, J. A. (2011). *III Curso de verano AMETIC-UPM 2011 hacia un mundo digital: las e-TIC motor de los cambios sociales, económicos y culturales.*

Holstein, D. C., Li, H. L., & Meneses, A. (2010). *The Impact of Implementing Cyber Security Requirements using IEC 61850.*

Holstein, D. K. (2008). *P1711 "The state of closure".* PES/PSSC Working Group C6.

Huntington, G. (2009). *NERC CIP's and identity management.* Huntington Ventures Ltd.

IBM Global Services. (2007). *A Strategic Approach to Protecting SCADA and Process Control Systems.*

Iinternational Atomic Energy Agency (IAEA). (2011). *IAEA Technical Meeting on Newly Arising Threats in Cybersecurity of Nuclear Facilities.* Retrieved 2011, from http://www.iaea.org/NuclearPower/Downloads/Engineering/files/InfoSheet-CybersecurityTM-May-2011.pdf

INSPIRE Project. (2008). *INcreasing Security and Protection through Infrastructure REsilience*. Retrieved 2011, from http://www.inspire-strep.eu

Institute of Electrical and Electronics Engineers (IEEE). (1994). *IEEE Standard C37.1-1994: Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.* Institute of Electrical and Electronics Engineers.

Institute of Electrical and Electronics Engineers (IEEE). (2000). *IEEE PES Computer and Analytical Methods SubCommittee*. Retrieved 2011, from http://ewh.ieee.org/cmte/psace/CAMS_taskforce.html

Institute of Electrical and Electronics Engineers (IEEE). (2007). *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.*

Institute of Electrical and Electronics Engineers (IEEE). (2008). *Transmission & Distribution Exposition & Conference 2008 IEEE PES : powering toward the future.* Institute of Electrical and Electronics Engineers.

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *IEEE Power & Energy Society*. Retrieved 2011, from http://www.ieee-pes.org

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *WGC1 - Application of Computer-Based Systems.* http://standards.ieee.org/develop/wg/WGC1.html.

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

International Electrotechnical Commission (IEC). (2007). *IEC TS 62351-1: Power systems management and associated information exchange – Data and communications security. Part 1: Communication network and system security – Introduction to security issues.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2007). *IEC TS 62351-3: Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2007). *IEC TS 62351-4: Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2007). *IEC TS 62351-6: Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2008). *IEC TS 62351-2: Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2009). *IEC TS 62351-5: Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives.* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2010). *IEC 61850-7-2: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI).* International Electrotechnical Commission.

International Electrotechnical Commission (IEC). (2010). *IEC TS 62351-7: Power systems management and associated information exchange – Data and communications security. Part 7: Network and system management (NSM) data object models.* International Electrotechnical Commission.

International Federation for Information Processing (IFIP). (n.d.). *IFIP TC 8 International Workshop on Information Systems Security Research*. Retrieved 2011, from http://ifip.byu.edu

International Federation for Information Processing (IFIP). (n.d.). *IFIP Technical Committees*. Retrieved 2011, from http://ifiptc.org/?tc=tc11

International Federation for Information Processing (IFIP). (n.d.). *IFIP WG 1.7 Home Page*. Retrieved 2011, from http://www.dsi.unive.it/~focardi/IFIPWG1_7

International Federation of Automatic Control (IFAC). (n.d.). *TC 3.1. Computers for Control — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/3/1

International Federation of Automatic Control (IFAC). (n.d.). *TC 6.3. Power Plants and Power Systems — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/6/3

International Federation of Automatic Control (IFAC). (n.d.). *Working Group 3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/5/4/working-groups/copy2_of_working-group-1-decentralized-control-of-large-scale-systems

International Instruments Users' Association (WIB). (2010). *Process control domain - Security requirements for vendors.* EWE (EI, WIB, EXERA).

International Organization for Standardization (ISO), I. E. (2005). *Information technology — Security techniques — Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission.

International Society of Automation (ISA). (n.d.). *ISA99 Committee - Home*. Retrieved 2011, from http://isa99.isa.org/ISA99 Wiki/Home.aspx

International Society of Automation (ISA). (n.d.). *LISTSERV 15.5 - ISA67-16WG5.* Retrieved 2011, from http://www.isa-online.org/cgi-bin/wa.exe?A0=ISA67-16WG5

INTERSECTION Project. (2008). *INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks (INTERSECTION)*. Retrieved 2011, from http://www.intersection-project.eu

Interstate Natural Gas Association of America (INGAA). (2011). *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry.* Interstate Natural Gas Association of America.

IRRIIS Project. (2006). *Homepage of the IRRIIS project*. Retrieved 2011, from http://www.irriis.org

Jeff Trandahl, C. (2001). *USA Patriot Act (H.R. 3162).* Retrieved 2011, from http://epic.org/privacy/terrorism/hr3162.html

Masica, K. (2007). *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.*

Masica, K. (2007). *Securing WLANs using 802.11i. Draft. Recommended Practice.*

McAfee. (2011). *Global Energy Cyberattacks: "Night Dragon".* Retrieved 2011, from http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Meridian. (n.d.). *Meridian*. Retrieved 2011, from http://www.meridian2007.org

National Infrastructure Security Coordination Centre (NISCC). (2005). *Firewall deployment for scada and process control networks. good practice guide.* National Infrastructure Security Coordination Centre.

National Infrastructure Security Coordination Centre (NISCC). (2005). *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* British Columbia Institute of Technology (BCIT).

National Infrastructure Security Coordination Centre (NISCC). (2006). *Good Practice Guide Process Control and SCADA Security.* PA Consulting Group.

National Institute of Standards and Technology (NIST). (2004). *NISTIR 7176: System Protection Profile - Industrial Control Systems.* Decisive Analytics.

National Institute of Standards and Technology (NIST). (2009). *NIST SP 800-53: Information Security.* National Institute of Standards and Technology.

National Institute of Standards and Technology (NIST). (2010). *NISTIR 7628: Guidelines for Smart Grid Cyber Security.* Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG).

National Institute of Standards and Technology (NIST). (2011). *NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology.

North American Electric Reliability Corporation (NERC). (2009). *Categorizing Cyber Systems. An Approach Based on BES Reliability Functions. Cyber Security Standards Drafting Team for Project 2008-06 Cyber Security Order 706.*

North American Electric Reliability Corporation (NERC). (2010). *CIP-001-1a: Sabotage Reporting.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-002-4: Cyber Security — Critical Cyber Asset Identification.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-003-4: Cyber Security — Security Management Controls.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-004-4: Cyber Security — Personnel and Training.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-005-4: Cyber Security — Electronic Security Perimeter(s).* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-006-4: Cyber Security — Physical Security.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-007-4: Cyber Security — Systems Security Management.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-008-4: Cyber Security — Incident Reporting and Response Planning.* North American Electric Reliability Corporation.

North American Electric Reliability Corporation (NERC). (2011). *CIP-009-4: Cyber Security — Recovery Plans for Critical Cyber Assets.* North American Electric Reliability Corporation (NERC).

Norwegian Oil Industry Association (OLF). (2006). *OLF Guideline No. 104: Information Security Baseline Requirements for Process.* Norwegian Oil Industry Association.

Norwegian Oil Industry Association (OLF). (2006). *OLF Guideline No.110: Implementation of information security in PCSS/ICT systems during the engineering, procurement and commissioning phases.* Norwegian Oil Industry Association.

Norwegian Oil Industry Association (OLF). (2009). *Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems.* Norwegian Oil Industry Association.

Open Smart Grid. (n.d.). *Open Smart Grid*. Retrieved 2011, from http://osgug.ucaiug.org/default.aspx

Rijksoverheid. (2009). *Scenario's Nationale Risicobeoordeling 2008/2009.* Retrieved 2011, from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/21/scenario-s-nationale-risicobeoordeling-2008-2009.html

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*.

SANS. (1989). *SCADA Security Advanced Training*. Retrieved 2011, from http://www.sans.org/security-training/scada-security-advanced-training-1457-mid

SANS. (2011). *The 2011 Asia Pacific SCADA and Process Control Summit - Event-At-A-Glance*. Retrieved 2011, from http://www.sans.org/sydney-scada-2011

Smart Grid Interoperability Panel (SGIP). (n.d.). *SGIP Cyber Security Working Group (SGIP CSWG)*. Retrieved 2011, from http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Smith, S. S. (2006). *The SCADA Security Challenge: The Race Is On.*

Stouffer, K. A., Falco, J. A., & Scarfone, K. A. (2011). *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed*

Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology.

Suter, M., & Brunner, E. M. (2008). *International CIIP Handbook 2008 / 2009.*

Swedish Civil Contingencies Agency (MSB). (2010). *Guide to Increased Security in Industrial Control Systems.* Swedish Civil Contingencies Agency.

Technical Support Working Group (TSWG). (2005). *Securing Your SCADA and Industrial Control Systems.* Departmet of Homeland Security.

The 451 Group. (2010). *The adversary: APTs and adaptive persistent adversaries.*

The White House. (2001). *Executive Order 13231.* Retrieved 2011, from http://www.fas.org/irp/offdocs/eo/eo-13231.htm

The White House. (2007). *National Strategy for Information Sharing.* Retrieved 2011, from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html

Theriault, M., & Heney, W. (1998). *Oracle Security* (First Edition ed.). O'Reilly.

Tsang, R. (2009). *Cyberthreats, Vulnerabilities and Attacks on SCADA networks.*

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *Control Systems Security Program: Industrial Control Systems Cyber Emergency Response Team.* Retrieved 2011, from http://www.us-cert.gov/control_systems/ics-cert/

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *Control Systems Security Program: Industrial Control Systems Joint Working Group.* Retrieved 2011, from http://www.us-cert.gov/control_systems/icsjwg/index.html

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *US-CERT: United States Compueter Emergency readiness Team*. Retrieved 2011, from http://www.us-cert.gov

United States General Accounting Office (GAO). (2004). *Critical infrastructure protection. Challenges and Efforts to Secure Control Systems.* United States General Accounting Office.

United States Nuclear Regulatory Commission. (2010). *Regulatory Guide 5.71: Cyber security programs for nuclear facilities.*

VIKING Project. (2008). *Vital Infrastructure, Networks, Information and Control Systems Management*. Retrieved 2011, from http://www.vikingproject.eu

Water Sector Coordinating Council Cyber Security Working Group. (2008). Roadmap to Secure Control Systems in the Water Sector.

Web application Security Consortium. (2009). *Web Application Firewall Evaluation Criteria*. Retrieved 2011, from http://projects.webappsec.org/w/page/13246985/Web Application Firewall Evaluation Criteria

Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats.* Momentum Press.

West, A. (n.d.). *SCADA Communication protocols.* Retrieved 2011, from http://www.powertrans.com.au/articles/new pdfs/SCADA PROTOCOLS.pdf

ZigBee. (n.d.). *ZigBee Home Automation Overview*. Retrieved 2011, from http://www.zigbee.org/Standards/ZigBeeHomeAutomation/Overview.aspx

Zwan, E. v. (2010). Security of Industrial Control Systems, What to Look For. *ISACA Journal Online*.

10 Abbreviations

ACC	American Chemistry Council
AD	Active Directory
AGA	American Gas Association
AMETIC	Multi-Sector Partnership Of Companies In The Electronics, Information And Communications Technology, Telecommunications And Digital Content
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programming Interface
API	American Petroleum Institute
ARECI	Availability And Robustness Of Electronic Communication Infrastructures
ARP	Address Resolution Protocol
AV	Anti-Virus
BDEW	Bundesverband Der Energie Und Wasserwirtschaft
BGW	Bundesverband Der Deutschen Gas Und Wasserwirtschaft
BW	Band Width
CA	Certified Authority
CC	Common Criteria
CCTV	Closed-Circuit Television
CEN	European Committee For Standardization
CENELEC	European Committee For Electrotechnical Standardization
CERT	Computer Emergency Response Team
CFR	Code Of Federal Regulations
CI	Critical Infrastructure
CI2RCO	Critical Information Infrastructure Research Coordination
CIFS	Common Internet File System
CIGRE	Conseil International Des Grands Réseaux Électriques
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructures Protection
CIKR	Critical Infrastructure And Key Resources
CIP	Critical Infrastructures Protection
CIWIN	Critical Infrastructure Warning Information Network
CNPIC	Centro Nacional Para La Protección De Infraestructuras Críticas
COTS	Commercial Off-The-Shelf
CPNI	Centre For The Protection Of National Infrastructures
CRP	Coordinated Research Project
CRUTIAL	Critical Utility Infrastructural Resilience
CSSP	Control Systems Security Program
DCS	Distributed Control Systems
DD	Data Diode
DDOS	Distributed Denial-Of-Service Attack
DHS	Department Of Homeland Security

DLP	Data Loss (Or Leak) Prevention (Or Protection)
DLP	Data-Leakage Prevention
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DNS	Domain Name Server
DOE	Department Of Energy
DOS	Denial Of Service
DPI	Deep Packet Inspection
DSO	Distribution System Operator
EC	European Commission
ECI	European Critical Infrastructure
ELECTRA	Electrical, Electronics And Communications Trade Association.
ENISA	European Network And Information Security Agency
EO	Executive Orders
EPA	Environmental Protection Agency
EPCIP	European Programme For Critical Infrastructures Protection
ERA	European Research Area
ESCORTS	Security Of Control And Real Time Systems
E-SCSIE	European Scada And Control Systems Information Exchange
EU	European Union
EXERA	Association Des Exploitants D'equipements De Mesure, De Régulation Et D'automatisme
FDAD	Full Digital Arts Display
FIPS	Federal Information Processing Standard
FP	Framework Programme
FTP	File Transfer Protocol
GIPIC	Grupo De Trabajo Informal Sobre Protección De Infraestructuras Críticas
GP	Good Practices
GPS	Global Position System
GUI	Graphical User Interface
HIPS	Host Intrusion Prevention System
HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
HW	Hardware
I&C	Instrumentation And Control
IAEA	International Atomic Energy Agency
IAM	Identity And Access Management
IAONA	Industrial Automation Open Networking Association
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control Systems
ICSJWG	Industrial Control Systems Joint Working Group
ICT	Information And Communications Technology
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation Of Automatic Control.
IFIP	International Federation For Information Processing
IMG-S	Integrated Management Group For Security
INL	Idaho National Laboratory
INSPIRE	Increasing Security And Protection Through Infrastructure Resilience
INTER-SECTION	Infrastructure For Heterogeneous, Resilient, Secure, Complex, Tightly Inter-Operating Networks
IO	Input/Output
IPS	Intrusion Protection System
IPSEC	Internet Protocol Security
IRBC	Ict Readiness For Business Continuity Program
IRIIS	Integrated Risk Reduction Of Information-Based Infrastructure Systems
ISA	Instrumentation, Systems And Automation Society
ISACA	Information Systems Audit And Control Association
ISBR	Information Security Baseline Requirements
ISMS	Information Security Management System
ISO	International Organization For Standardization
IST	Information Society Technologies
IT	Information Technologies
JHA	Justice And Home Affairs
KF	Key Finding
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPDE	Low Density Polyethyl
MAC	Media Access Control
MCM	Maintenance Cryptographic Modules
MIT	Middleware Improved Technology
MSB	Swedish Civil Contingencies Agency
MTU	Master Terminal Unit
NAC	Network Access Control
NBA	Network Behaviour Analysis
NBA	Network Behaviour Analysis
NCI	National Critical Infrastructure
NCS	Norwegian Continental Shelf
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NHO	Norwegian Business And Industry
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan

NIS	Network And Information Security
NISCC	National Infrastructure Security Co-Ordination Centre
NIST	National Institute For Standard And Technologies
NISTIR	National Institute Of Standards And Technology Interagency Report
NRC	Nuclear Regulatory Commission
NRG	Nuclear Regulatory Guide
NSAC	National Security Advice Centre
OLF	Norwegian Oil Industry Association
OPC	Ole For Process Control
OS	Operating System
OSG	Open Smart Grid
OSI	Open System Interconnection
OTP	One Time Password
PCCIP	Presidential Commission On Critical Infrastructure Protection
PCD	Process Control Domains
PCN	Process Control Networks
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PDCA	Plan, Do, Check, Act
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PP	Protection Profiles
PPP	Public Private Partnerships
QOS	Quality Of Service
R&D	Research And Development
RAT	Remote Administration Tools
RF	Radio Frequency
RSS	Really Simple Syndication
RTU	Remote Terminal Units
SANS	System Administration, Networking, And Security Institute
SCADA	Supervisory Control And Data Acquisition
SEM	Security Event Manager
SEMA	Swedish Emergency Management Agency
SIEM	Security Information And Event Management
SIM	Security Information Management
SIMCIP	Simulation For Critical Infrastructure Protection
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier

SSL	Secure Sockets Lay
SSP	Sector-Specific Plan
ST	Security Targets
SW	Software
TCG	Trusted Computing Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TISP	The Infrastructure Security Partnership
TKIP	Temporal Key Integrity Protocol
TOE	Target Of Evaluation
TR	Technical Report
TSWG	Technical Support Working Group
UDP	User Datagram Protocol
UK	United Kingdom
USA	United States Of America
VDI	The Association Of German Engineers
VDN	Verband Der Netzbetreiber
VIKING	Vital Infrastructure, Networks, Information And Control Systems Management
VPN	Virtual Private Network
VRE	Verband Der Verbundunternehmen Und Regionalen Energieversorger In Deutschland
WAF	Web Application Firewall
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIB	International Instruments Users' Association
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu