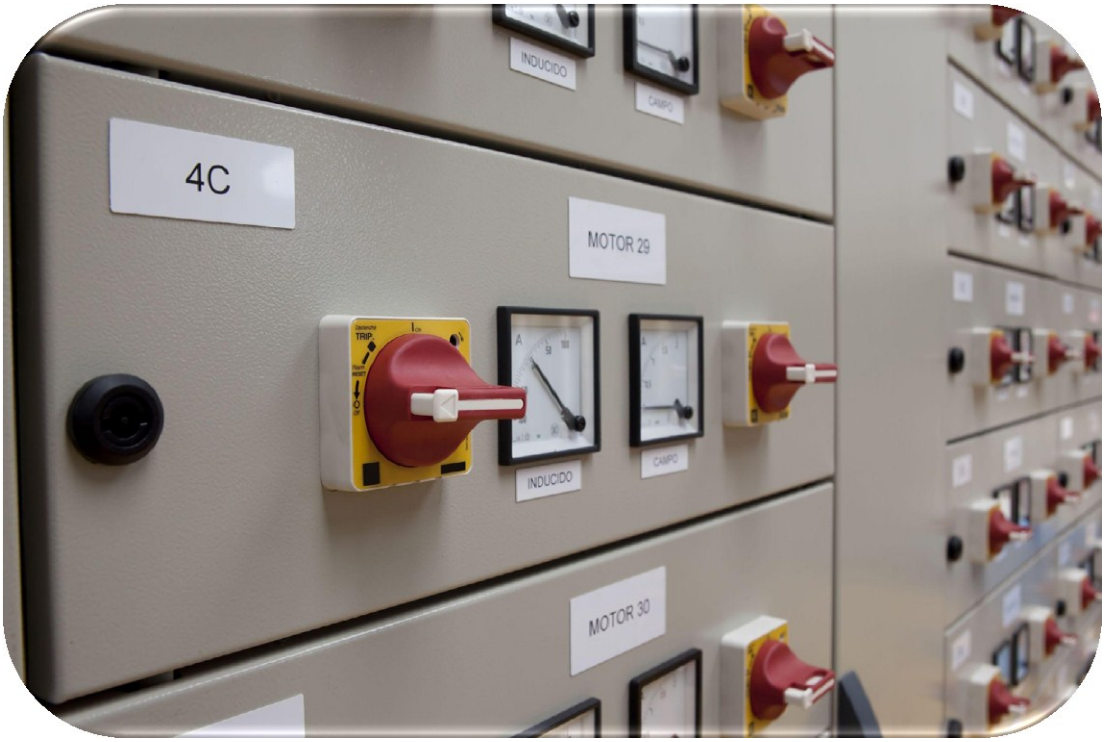
enisa
European Network and Information Security Agency



Protecting Industrial Control Systems

Annex V. Key Findings

[Deliverable – 2011-12-09]

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

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

Contents

1 Key Findings

This chapter presents a more detailed view on the Key Findings presented in chapter **Error! Reference source not found.** of the main report. The following tables provide a comprehensive description including details such as:

- An impact analysis
- Stakeholders involved or affected
- Areas or fields[1] in which they may have influence.

1.1 The biggest challenges in ICS security

Title	**Number**
Challenge 1: The lack of specific initiatives on ICS security	**1.1**
Description	
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. Likewise, ENISA has formally declared that after Stuxnet, currently prevailing philosophies on CIIP will have to be reconsidered. 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.	
Impact	
It seems that ICS security is not a key topic in CIP and CIIP plans at the EU level. Related stakeholders might not give them the necessary level of attention.	

Level			**Stakeholder Type**			**References**
Org&Pol.		Aware.	Man&Int	ICS Sec.	Operator	Desktop Research
			Acad&R	Public B.	Stand. B.	

Title	**Number**
Challenge 2: The lack of a Common Reference in Europe	**1.2**
Description	
Most experts consider that there should be a European reference with regards to security standards, guidelines or regulations. This is paricularly 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.	
Impact	

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

As there is not such a reference, most Stakeholders are starting to make their own decisions which may not always be appropriate and increases ICS security heterogeneity.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (23)
	Technic.		Acad&R	Public B.	Stand. B.	

Title	**Number**
Challenge 3: The lack of an integrated management of ICS security	**1.3**
Description	
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 cyber security programmes for their business computer systems, but cyber 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.	
Impact	
Not having an integral security management approach that integrates the different security flavours (i.e. physical, logical, environmental, and safety) can result in some risks being overlooked.	

Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
	Technic.		Acad&R	Public B.	Stand. B.	

Title	**Number**
Challenge 4: Lack of involvement of the Top management	**1.4**
Description	
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 them see 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).	
Impact	
Without a clear commitment from Top Management, the security of ICS will not be appropriately managed, and in turn, the overall security of the company will result weakened.	

Level			**Stakeholder Type**			**References**
Org&Pol.		Aware.		ICS Sec.	Operator	Survey&Interview
Econom.				Public B.	Stand. B.	

Title	Number
Challenge 5: Amortization of ICS investments	**1.5**
Description	
ICS systems technology has been developed, in many cases, for a very specific purpose use 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.	
Impact	
The ICS market would have to deal with this issue at least for the following decade. Compensatory security controls will have to be developed.	

Level			Stakeholder Type			References
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Challenge 6: A long path for ICT security tools and services providers	**1.6**
Description	
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.	
Impact	
There is a need to further reconsider classic ICT security solutions and services, so that they can really help securing ICS.	

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Challenge 7: Adaptive Persistent Adversaries as the threat of the future.	**1.7**
Description	
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 most experts think it will grow during the following years.						
Impact						
Adaptive Persistent Adversaries are a formidable threat that can make much harm and require intelligent security measures to be implemented.						
Level			**Stakeholder Type**			**References**
Org&Pol.		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (65)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
Challenge 8: The security technical challenges of the SmartGrid: size, third party networks and customer privacy.						**1.8**
Description						
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.						
Impact						
All involved stakeholders (manufacturers, telecommunication companies, operators, and end-users) will have to deal with security problems.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.2 Current standards, guidelines and regulations

Title						**Number**
Not all sectors are being targeted by EU policies.						**2.1**
Description						
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.						
Impact						
This might be the reason why sectors such as water and food/agriculture are not active on defining guidelines and standards for ICS protection.						
Level			**Stakeholder Type**			**References**

Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Desktop Research
				Public B.	Stand. B.	

Title	**Number**
Current documents usually generic.	**2.2**
Description	
During the desktop research phase, 38 different documents were studied: 26 guidelines, 9 standards and 3 regulatory documents. Most of them can be considered as "generic", in the sense that they focus on security aspects affecting ICS from a general perspective.	
Impact	
Security documentation is usually for a general purpose. Guidelines providing examples for addressing security of ICS in a specific sector could help to better design security plans.	

Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Desktop Research
				Public B.	Stand. B.	

Title	**Number**
Standards and guidelines target: ICS communications, ISMS and the definition of security profiles	**2.3**
Description	
Several guidelines provide advice based on industrial security best 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, wihtin 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	
Impact	
ICS security specific documentation targeting ICS communications, ISMS and security profies already exists.	

Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Desktop Research
				Public B.	Stand. B.	

Title	**Number**
Energy, the sector with a larger number of specific guidelines	**2.4**
Description	
Some of the documents studied during the Desktop Research phase focus on specific sectors, with the	

Energy sector (including 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.						
Impact						
Comparing to other sectors, the Energy sector counts with a good number of reference ICS security standards and guidelines.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Desktop Research
Econom.	Technic.			Public B.	Stand. B.	

Title						**Number**
Transportation, Water Supply or Agriculture within the less active sectors						**2.5**
Description						
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 proteciton.						
Impact						
The aforementioned sectors may need especial attention to address ICS logical security issues.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Desktop Research
Econom.	Technic.			Public B.	Stand. B.	

Title						**Number**
Guidelines are "fresh" and "final"						**2.6**
Description						
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 a draft version such as the ANSI/ISA 99 and the of IEC 62443 standards.						
Impact						
Most guidelines are in a final status what makes them fully useful.						
Level			**Stakeholder Type**			**References**
	Stand.		Man&Int	ICS Sec.	Operator	Desktop Research
				Public B.	Stand. B.	

Title						**Number**
Lack of coordination among European countries						**2.7**
Description						
Many documents do 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.						
Impact						
Many European countries are developping their own guidelines while others will adapt existing ones.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Desktop Research
				Public B.	Stand. B.	

1.3 Acceptance and use of standards, guidelines and regulations

Title						**Number**
Good Practices and Standards are considered to be the most effective measures.						**3.1**
Description						
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.						
Impact						
The degree of acceptance of Good Practices and Standards is good.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.	Stand. B.	

Title						**Number**
The most valued characteristics of security standards : a holistic approach, risk management guidance and business-orientation						**3.2**
Description						
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.						
Impact						
Security in ICS is still at is early stages and therefore high-level holistic standards are more welcome						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview
				Public B.	Stand. B.	

Title	**Number**
Too technical standards less valued	**3.3**
Description	
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.	

Impact						
There are still organizational and management aspects to be considered first when securing ICS.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview
	Technic.			Public B.	Stand. B.	

Title						Number
On the costs of implementing guidelines: they are considered acceptable.						**3.4**
Description						
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.						
Impact						
Operators are transfering security costs to manufacturers and might not be yet considering appropriate compensatory measures for their current ICS.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.				Public B.	Stand. B.	

Title						Number
Low level of adoption of security guidelines and standards.						**3.5**
Description						
Survey respondents showed that their current level of adoptation of ICS security good practices was between low and medium, Operators being the best positioned. Most of them are in the early stages of implementing security best practices, since they declared that they are currently developping 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.						
Impact						
There is still work to do in the implementation of good practices, guidelines or standards.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
				Public B.	Stand. B.	

Title	Number
Implementation of non European regulations, standards or best practices in industrial environments.	**3.6**
Description	
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 by 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, like the NERC CIP standards for the bulk electricity transportation or the NRG 5.71 for nuclear power plants. However, there are other sectors that seem to be waiting for a specific mandate from public organisations before proceeding with these tasks.

Impact

The lack of reference guidelines and trying to comply with non-European regulations might result in not optimal investments.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Mistrust of guidelines causing heterogeneity.	**3.7**

Description

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 heterogenity 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.

Impact

From a security point of view, ICS environments are very heterogeneous on needs, activities and reference frameworks.

Level			Stakeholder Type			References
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.	Stand. B.	

Title	Number
Disagreement between stakeholders on the effectiveness of regulations	**3.8**

Description

Opinions are divided regarding the efectiveness of regulations, especially in Europe. Most Manufacturers and Operator 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.

Impact

The regulation of ICS security in Europe will probably have to overcome ressistance.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
				Public B.		

Title						Number
Manufacturers' negative attitude towards best practices and standards						**3.9**
Description						
Manufacturers participating in the survey and interviews have very little interested 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.						
Impact						
Manufactures seem to work independently, driven by market conditions. If the reasons behind are not understood and taken into consideration the whole community may lack the contribution of a very important stakeholder.						
Level			**Stakeholder Type**			**References**
	Stand.	Aware.	Man&Int			Survey&Interview

Title						Number
Compliance is not a market driver in ICS security						**3.10**
Description						
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.						
Impact						
In Europe, compliance is not a driving factor of ICS security as it has happenned in other regions and technological environments.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.				Public B.		

Title						Number
No need for a specific law to prosecute cyber criminal targeting ICS						**3.11**
Description						
Stakeholders do not think that an 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 kinkd of ammendment 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.						
Impact						
There is no need for specific legislation on attacks to ICS, but an ammendment to incorporate aggravating factors/circumstances.						
Level			**Stakeholder Type**			**References**

Org&Pol.						Survey&Interview
				Public B.		

Title						Number
The need for a European ICS security good practices documents						**3.12**
Description						
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 is not necessary to "reinvent the wheel" and it would be desireble 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 Eruopean 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.						
Impact						
All stakeholders could have a common reference to follow in Europe. Such a reference could also be a method to call Manufacturers attention and increase their willingness to cooperate.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.				Survey&Interview
				Public B.	Stand. B.	

1.4 The need for an Operators / Infrastructure level Security Plan

Title						Number
Need for an Operator/Infrastructure level security plan template						**4.1**
Description						
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.						
Impact						
The creation of such a templates could facilitate the adoption of complete and comprehensive security plans within ICS infrastructures.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.				Operator	Survey&Interview
				Public B.	Stand. B.	

Title	Number
Sections to be included in the Operator/Infrastructure level security plan	**4.2**
Description	
Most respondents believe that the plan should include operational and physical security, technical issues, training and awareness, security governance (roles and responsabilities), bussiness impact measures, and crisis management.	

Impact						
A hollistic approach could help operators and other stakeholders to unify their security situation.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.			Operator	Survey&Interview
Econom.	Technic.			Public B.	Stand. B.	

Title						Number
Risk Management to be included in the ICS security plan						**4.3**
Description						
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.						
Impact						
Risk Management, one of the most critical and complex steps in security plans, could be addressed easierly with this approach.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview (23)
	Technic.			Public B.	Stand. B.	

Title						Number
Awareness topic to be included in the ICS security plan						**4.4**
Description						
On-field staff should have guidence 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						
Impact						
Education and awareness issues should not be overlooked in a comprehensive security plan.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (11)
				Public B.	Stand. B.	

Title						Number
Security plans need to be adapted for every operator						**4.5**
Description						
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 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						
Impact						
The creation of such a template could facilitate the adoption of complete and comprehensive security plans within ICS infrastructures.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview (29)
					Stand. B.	

Title						**Number**
Developping security programs, too costly for operators						**4.6**
Description						
Developping 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						
Impact						
This somehow contradicts KF3.4 which might be related to the fact that ICS security is in its early stages, as stated in KF3.5. However, if this turns to be true, the objective of securing ICS might not be accomplished.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research
Econom.	Technic.			Public B.	Stand. B.	

1.5 Attitude towards information sharing and other collaborative Initiatives

Title						**Number**
Interest in sharing initiatives						**5.1**
Description						
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 desireable, more objective point of view.						
Impact						
There is a possitive attitude towards sharing initiatives.						
Level			**Stakeholder Type**			**References**

Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Excessive size, constraints or private interests are the main disadvantages and risks of sharing initiatives	**5.2**

Description

Although the attitude is usually possitive, several experts warned about negative aspects of this kind of initiative, 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

Impact

It is important to take these risks into consideration for any future development of any sharing initiatives on ICS security.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Unbalanced interest in cooperation between each group of stakeholders	**5.3**

Description

There are big differences regarding the interest that each kind of stakeholder has in cooperating with the others. Operators are the most demanded by the rest, 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 the rest. Manufacturers seem to be very focused on cooperation with Operators even though all other stakeholder types would like to cooperate more with them.

Impact

Operators and Manufacturers are considered to be the key players in cooperation initiatives. Therefore, they should be actively engaged. Additionally, it should be analyzed why other stakeholders do not consider Academia as a relevant stakeholer.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Active collaboration between the ICT security sector and ICS Manufacturers, essential to improve ICS security	**5.4**

Description						
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.						
Impact						
Without Manufacturer cooperation, improving ICS security will be a much harder task.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Destkop Research (11) (24) (25)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Bilateral cooperation preferred to multilateral						**5.5**
Description						
A few experts stated that bilateral cooperation is usually more effective and efficient than multilateral initiatives.						
Impact						
Industry bilateral partnerships can provide better results for specific oriented objectives.						
Level			**Stakeholder Type**			**References**
Org&Pol.			Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.		

1.6 Public Private Partnerships

Title	Number
PPP sharing initiatives demanded by most stakeholders.	**6.1**
Description	
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.	
Impact	
It is important to acknowledge that the role of the public sector is considered to be a key factor for the success of these kind of initiatives.	

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Not involving all stakeholder types and slowness - main critics regarding Public-Private Partnerships	6.2

Description

Experts signalled several negative points of PPP's:

- Public entities do not always take all stakeholder types into account
- Public guidelines that arrived late.

Impact

Some actors might be discouraged to participate in PPPs.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.	Stand. B.	

Title	Number
National or European funded security programmes to be improved.	6.3

Description

A slight majority of the stakholders 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.

Impact

Stakeholders feel there are many opportunities to focus on.

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.		

Title	Number
Trust is an essential ingredient for the success of sharing initiatives	6.4

Description

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

Impact

Creating a circle of trust is key for the success of information sharing initiatives.

Level	Stakeholder Type	References

Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
				Public B.		

1.7 Common test bed

Title	Number
Need for independent evaluations and tests of ICS security products	**7.1**
Description	
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 really trustful. Operators indicate that independent evaluations and tests are missing.	
Impact	
There is a niche for industry and public bodies on providing indpendent evaluations and tests of ICS security technologies and products.	

Level			Stakeholder Type			References
	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Interest in creating a common test bed	**7.2**
Description	
A vast majority of participants were interested in the creation of a common test bed to certify technologies regarding ICS Security and interoperability.	
Impact	
The creation of such a test bed could foster the adoption and improvement of ICS security features.	

Level			Stakeholder Type			References
	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
PPP, a European scope and supported by Academia the desired caracteristics of the common test bed	**7.3**
Description	
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 the knowledge about methodologies.	
Impact	
The creation of such test bed could foster infomration sharing and reduce the heterogeneity of the ICS environment.	

Level			Stakeholder Type			References
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Concerns regarding a European common test bed	**7.4**
Description	
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 overly involved in the technological aspects and that do not like the kind of bounds that are derived from such a participation. Others think that it is unlikely that such an organisation could work fast enough to be useful.	
Impact	
If such an initiative is put in place there would be a number of companies that will opose resistance.	

Level			Stakeholder Type			References
Org&Pol.	Stand.		Man&Int			Survey&Interview
	Technic.		Acad&R			

Title	Number
A security reference model as an alternative to a European common test bed	**7.5**
Description	
A few experts signaled different options 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 which those already existent certifiying organisms in each Member State 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	
Impact	
Some experts believe that this alternative would face less resistances and will work more efficiently.	

Level			Stakeholder Type			References
Org&Pol.	Stand.		Man&Int	ICS Sec.	Operator	Survey&Interview (24) (25)
	Technic.		Acad&R	Public B.	Stand. B.	

1.8 Dissemination and Awareness Initiatives

Title	Number
Space for improvement in Dissemination and Awareness Forums.	**8.1**

Description						
Only two thirds of participants were aware of the current dissemination and awareness initiatives.						
Impact						
There is space for improving current dissemination and awareness initiatives.						
Level			**Stakeholder Type**			**References**
		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.		

Title	Number
High interest in participating in Dissemination and Awareness Forums.	**8.2**
Description	
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.	
Impact	
It is likely that more people would be interested in participating if they were informed.	

Level			Stakeholder Type			References
		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.		

Title	Number
Quality of ICS security events low-rated.	**8.3**
Description	
Participants stated that ICS security events quality could be improved. They considered that they are too commercial (so too general) or too academic (without the pressence of on-field stakeholders). 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.	
Impact	
Events on ICS security have to be improved.	

Level			Stakeholder Type			References
		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.		

Title	Number
Top Management awareness to be fostered	**8.4**
Description	
Many experts agreed that one of the main difficulties in improving ICS security is to defending security costs before the Top Management. There is a current of opinion that states that it has to be presented as a bussines 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 reprioritising 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".
Impact
Security costs must be understood by Top Management, otherwise security may not be properly taken into account.

Level			Stakeholder Type			References
		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview (23)
			Acad&R	Public B.		

Title	Number
Discussion on technology-centric forums	**8.5**
Description	
A few experts stated that Dissemination and Awareness forums do focus too much on security technologies or generic security aspects, not giving enough attention to the Bussines 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 an horizontal subject.	
Impact	
By following the previous suggestions, involving Senior Management and solving security problems could be more successful.	

Level			Stakeholder Type			References
		Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
			Acad&R	Public B.		

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

Title	Number
Creation of an ICS-computer emergency response capability	**9.1**
Description	
According to a large number of experts an ICS-computer emergency response capability should be developed or in place.	
Impact	
An ICS-computer emergency response capability could be a reference for stakeholders.	

Level	Stakeholder Type	References

Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (23)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
PPP and cross-border as desired characteristics of an ICS-computer emergency response capability						**9.2**
Description						
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.						
Impact						
A common reference in Europe would be welcome.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Characteristics of the an ICS-computer emergency response capability						**9.3**
Description						
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.						
Impact						
There is no complete agreement about how the ICS-computer emergency response capability should be organised. There are different alternatives to consider.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.10 Current situation of Technologic Threats and Solutions

Title	Number
About the technical threats identified by experts	**10.1**
Description	
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 human unintentional human errors due to a lack of interest or understanding of ICS security issues.	

Impact						
ICS security threats are now merging with ICT threats.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
ICS security "taken in their own hands"						**10.2**
Description						
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.						
Impact						
ICS are behind the most critical parts of the core business of many CI operators. Therefore, operators might not be willing to subcontract their protection (i.e. not to reveal critical information to third-party companies). However, this might also be interpreted as a measure of the maturity level of ICS protection. As it is clear from other Key Findings, operators are still in the first stages of implementing ICS security controls: performing a risk analysis, defining security plans, or starting to implement some of the projects of the plan.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
IDS/IPS, DPI, VPN and NAC, the most recommended security technologies.						**10.3**
Description						
IDS/IPS, DPI, VPN and NAC technologies are the most popular security technologies for Operators, Academia and Security Tools and Service Providers. The next on the list are: conventional firewalls, application whitelisting, host bastioning, wireless security and multi-factor authentication.						
Impact						
N/A						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Discrepancies among stakeholders on the most appropriate security technologies						**10.4**
Description						
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.						
Impact						

Operators prefer to use mature and more economic technology.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	**Number**
Discrepancies within most demanded/acquired security services.	**10.5**
Description	
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.	
Impact	
Operators are recommended to use services that they declare to be rarely using. Moreover, ICS security service providers are providing services that Operators are not aware of. This discrepancy might be due to the fact that many of the security services are part of the whole ICS deployment contract signed between the ICS vendor and the operator. Operators are not really aware that the ICS systems they are acquiring already come with security products (e.g. firewalls, IDS/IPS, etc.) or hardenned against security threats. It is the ICS Manufacturer that demands part of the security services to ICS tools and Services providers.	

Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.11 Legacy Related Risks

Title	**Number**
Untrusted and legacy devices and protocols - nowadays' biggest threat	**11.1**
Description	
According to the survey, the biggest threat to the security of ICS is the existence of untrusted. This is usually related to the use of legacy or proprietary technologies that often include security breaches (e.g. backdoors).	
Impact	
ICS users have reasons to mistrust their own devices or the ones in the market.	

Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	**Number**
Legacy devices working under invalide assumptions. Long lifecycle of ICS.	**11.2**

Description						
Obsolete technologies were designed with invalid assumptions such as "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 protectin 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.						
Impact						
Many working devices are not prepared to face current cyber security threats.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Built-in security needed						**11.3**
Description						
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.						
Impact						
If security is not taken into account from the beginning more expensive compensating solutions are needed.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (23) (1)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Most Manufacturers already produce built-in security functionalities						**11.4**
Description						
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.						
Impact						
Vendors have started to address the need for built-in security.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number

Modular approach to built-in security requested by most on-field stakeholders.						**11.5**
Description						
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.						
Impact						
If ICS products are manufactured in this way updating their security capabilities will be much easier.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.12 ICT and ICS convergence problems

Title						**Number**
ICS importing the ICT solutions and the ICT problems						**12.1**
Description						
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).						
Impact						
ICS networks complexity is increasing with ICT technologies as well as associated risks.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
Regular ICT solutions need to be adapted further to the ICS scenario						**12.2**
Description						
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 some commercial data diodes are compatible with a very small set of industrial protocols while they are still focusing on traditional ICT protocols such as FTP, SMTP, CIFS, etc.						

Impact						
If ICT solutions do not address the technical specificities of ICS they will not be of much help in the protection of such environments.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
ICT staff does correctly understand ICS requirements						**12.3**
Description						
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.						
Impact						
If ICT and ICS staff are not able to work collaborately it is unlikely that they will be able to reach unified and appropriate solutions for their problems.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
ICS providers are not aware of security best practices of the ICT world						**12.4**
Description						
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.						
Impact						
If ICS logical security responsible staff do not self-adapt to the new ICT security requirements they could neglect actual risks.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (28)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	Number
Warnings about ICT security vendors into ICS.	**12.5**
Description	
Many respondents expresed their concern about the appearance during the last few years of conventional ICT security vendors, trying to sell their technologies to ICS operators without deeply understanding their requirements.	

Impact						
Some security solutions in ICS environments may not be appropriate or even harmful.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Potential role in ICS-ICT security integration.						**12.6**
Description						
To correctly adapt security requirements and functionalities into the ICS environments, Academia stakeholders may play an important role as they have the necessary ressources. Developping theoretical frameworks to help both vendors and customers to understand what is needed and how to address it.						
Impact						
ICT and ICS technology convergence could be done in a more reliable way.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.13 Other Technology Issues

Title						Number
Hardening often requires support from vendors and security tools and services providers						**13.1**
Description						
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 strong support from vendors and often requires Security Tools and Service Providers.						
Impact						
All on-field stakeholders need to cooperate to facilitate hardening tasks.						
Level			**Stakeholder Type**			**References**
			Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (23)
	Technic.					

Title						Number
Difficulties with vulnerability mangement on the Operators side and in the commirment of Manufacturers						**13.2**
Description						
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						

researches (who disclose vulnerabilities) and Manufacturers.						
Impact						
This situations generate misconfindence. An eventual ICS-computer emergency response capability (or alternative initiatives) may help to solve this kind of issues.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
ICS security dependance of the ICT QoS						**13.3**
Description						
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.						
Impact						
Monitoring and guaranteeing these performance metrics should be included as part of the security objectives when implementing security controls.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
Security in remote accesses						**13.4**
Description						
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.						
Impact						
Remote functionalities should always grow in parallel to security measures.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
Cloud Computing not to be adopted in core ICS technologies						**13.5**
Description						
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.						
Impact						
It is unlikely that Cloud Computing will be adopted in core specific ICS networks.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.14 Present and Future Research

Title						**Number**
Current research lines						**14.1**
Description						
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, Smat Grid standards and measures of effectiveness						
Impact						
Lines of research have proven to give interesting results.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
Future research lines						**14.2**
Description						
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.						
Impact						
Future research should focus on ICS specific problems. This means that direct application of ICT solutions and techniques is not enough anymore. This is particularly true for targeted attacks detection and response.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title	**Number**

Future threats a research topic						**14.3**
Description						
Experts considered that in the future their biggest technical challenges will be to deal with external targetted attacks, internal threats (both intentional and unintentioned) as well as increased difficulties in the vulnerability management and privacy issues, due to the growth of Smart Grids.						
Impact						
It is necessary to define solutions for targeted attacks.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

1.15 Pending debates on ICS security and other related issues

Title						**Number**
The security by obscurity debate						**15.1**
Description						
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.						
Impact						
If there is no general agreement both approaches will coexist, which can cause problems if one is proven to be less effective than the other.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (24) (25)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						**Number**
The debate about regulation enforcement by fines.						**15.2**
Description						
A slight majority of respondents think that the regulation enforcement in Europe should not follow the NERC-CIP approach of the US.						
Impact						
The adoption of such measures will face great resistance.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Reasons againts regulation enforcement by penalties						**15.3**
Description						
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.						
Impact						
Regulation enforcement by fines does not guarantee ICS to be secure and even could compromise theri security in various ways.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Reasons for regulation enforcement by penalties						**15.4**
Description						
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.						
Impact						
If regulation enforcement based on penalties is to be used it should be made in parallel to awareness raising tasks.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Debate regarding Smart Grid dependency on third party telecomm Operators.						**15.5**
Description						
A majority of stakeholders perceive as negative the dependency on third parties when providing Smart Grid services. However, there is a number of voices, specially from Academia, that consider it could provide benefits for Operators.						
Impact						
Consequences of this situation must be studied in depth in order to provide an objective point of view.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Concerns regarding Smart Grid dependency on third party telecomm Operators.						**15.6**
Description						
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 telecommincation operator. Many agree to require encryption and signatures to prevent information leaks.						
Impact						
Operators may need to adopt more security measures.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

Title						Number
Positive points regarding Smart Grid dependency on third party telecommunication Operators						**15.7**
Description						
A few respondents consider a benefit for operators to rely on specialized telecommication 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.						
Impact						
There are important benefits deriving from subcontracting third-party telecommunication operators in the Smart Grid.						
Level			**Stakeholder Type**			**References**
Org&Pol.	Stand.	Aware.	Man&Int	ICS Sec.	Operator	Survey&Interview, Desktop Research (26)
Econom.	Technic.		Acad&R	Public B.	Stand. B.	

2 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. 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*.

3 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