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 .................................................................................................................. 1

1.1  The biggest challenges in ICS security ........................................................................ 1

1.2  Current standards, guidelines and regulations ............................................................... 4

1.3  Acceptance and use of standards, guidelines and regulations ........................................ 7

1.4  The need for an Operators / Infrastructure level Security Plan ...................................... 11

1.5  Attitude towards information sharing and other collaborative initiatives ..................... 13

1.6  Public Private Partnerships ............................................................................................ 15

1.7  Common test bed ............................................................................................................. 17

1.8  Dissemination and Awareness Initiatives ....................................................................... 18

1.9  The usefulness of an ICS-computer emergency response capabilities or equivalent alternatives .................................................................................................................. 20

1.10  Current situation of Technologic Threats and Solutions ............................................ 21

1.11  Legacy Related Risks ..................................................................................................... 23

1.12  ICT and ICS convergence problems .............................................................................. 25

1.13  Other Technology Issues ............................................................................................... 27

1.14  Present and Future Research ......................................................................................... 29

1.15  Pending debates on ICS security and other related issues ........................................... 30

2  References ......................................................................................................................... 33

3  Abbreviations .................................................................................................................. 44
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

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge 1: The lack of specific initiatives on ICS security</td>
<td>1.1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Aware.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge 2: The lack of a Common Reference in Europe</td>
<td>1.2</td>
</tr>
</tbody>
</table>

**Description**

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

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td>Technic.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Desktop Research (23)</td>
</tr>
</tbody>
</table>

**Challenge 3: The lack of an integrated management of ICS security**

**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.

**Challenge 4: Lack of involvement of the Top management**

**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.
Title: Challenge 5: Amortization of ICS investments
Number: 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 tomorrow’s. 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: Challenge 6: A long path for ICT security tools and services providers
Number: 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
Econom. Technic. Acad&R Public B. Stand. B.

Title: Challenge 7: Adaptive Persistent Adversaries as the threat of the future.
Number: 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Aware.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

---

### Title

Challenge 8: The security technical challenges of the SmartGrid: size, third party networks and customer privacy.

### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

---

### 1.2 Current standards, guidelines and regulations

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not all sectors are being targeted by EU policies.</td>
<td>2.1</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
</table>
## Current documents usually generic.

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.

### Standards and guidelines target: ICS communications, ISMS and the definition of security profiles

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, within the company, an Information Security Management System (ISMS). With regards to this, there are several documents that have been studied which guide operators on how to include industrial control systems into their ISMS.

Finally, there is a very useful set of documentation which addresses the security requirements/profiles and characteristics that new ICS components should include to comply with critical infrastructure protection programmes.

### Energy, the sector with a larger number of specific guidelines

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.

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of coordination among European countries</td>
<td>2.7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transportation, Water Supply or Agriculture within the less active sectors</td>
<td>2.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines are &quot;fresh&quot; and &quot;final&quot;</td>
<td>2.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>2.7</td>
</tr>
</tbody>
</table>
United Kingdom, Germany, and Norway.

**Impact**

Many European countries are developing their own guidelines while others will adapt existing ones.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.3 **Acceptance and use of standards, guidelines and regulations**

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Practices and Standards are considered to be the most effective measures.</td>
<td>3.1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>The most valued characteristics of security standards : a holistic approach, risk management guidance and business-orientation</td>
<td>3.2</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too technical standards less valued</td>
<td>3.3</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Man&amp;Int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public B.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Techic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Man&amp;Int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICS Sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Survey&amp;Interview</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

On the costs of implementing guidelines: they are considered acceptable.

**Number**

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 transferring security costs to manufacturers and might not be yet considering appropriate compensatory measures for their current ICS.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Man&amp;Int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICS Sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Survey&amp;Interview</td>
<td></td>
</tr>
<tr>
<td>Econom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public B.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stand. B.</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

Low level of adoption of security guidelines and standards.

**Number**

3.5

**Description**

Survey respondents showed that their current level of adoption 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 developing a security plan or even performing the initial risk analysis. Among the problems they are facing they highlight the low level of involvement of Top Management or the lack of a common framework to follow.

**Impact**

There is still work to do in the implementation of good practices, guidelines or standards.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Man&amp;Int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICS Sec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Survey&amp;Interview</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

Implementation of non European regulations, standards or best practices in industrial environments.

**Number**

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

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

**Impact**

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

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td></td>
</tr>
<tr>
<td>Acad&amp;R</td>
<td>Public B.</td>
<td></td>
</tr>
</tbody>
</table>

Opinions are divided regarding the effectiveness 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 resistance.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td></td>
</tr>
<tr>
<td>Aware.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Manufacturers' negative attitude towards best practices and standards

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting Industrial Control Systems</td>
<td>Annex V. Key Findings</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand.</td>
<td>Aware.</td>
<td>Man&amp;Int.</td>
</tr>
</tbody>
</table>

### Compliance is not a market driver in ICS security

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting Industrial Control Systems</td>
<td>Annex V. Key Findings</td>
</tr>
</tbody>
</table>

#### 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 happened in other regions and technological environments.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Man&amp;Int.</td>
</tr>
<tr>
<td>Econ.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### No need for a specific law to prosecute cyber criminal targeting ICS

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting Industrial Control Systems</td>
<td>Annex V. Key Findings</td>
</tr>
</tbody>
</table>

#### 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 kind 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
</table>
### Annex V. Key Findings

#### 1.4 The need for an Operators / Infrastructure level Security Plan

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for an Operator/Infrastructure level security plan template</td>
<td>4.1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Survey&amp;Interview</td>
</tr>
<tr>
<td>Public B.</td>
<td>Operator</td>
<td>Public B.</td>
</tr>
<tr>
<td>Stand. B.</td>
<td>Operator</td>
<td>Stand. B.</td>
</tr>
</tbody>
</table>

**Title**

Sections to be included in the Operator/Infrastructure level security plan

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
</tr>
</tbody>
</table>

**Description**

Most respondents believe that the plan should include operational and physical security, technical issues, training and awareness, security governance (roles and responsabilities), business impact measures, and crisis management.
Protecting Industrial Control Systems

Annex V. Key Findings

**Impact**

A hollistic approach could help operators and other stakeholders to unify their security situation.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Standard</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

Risk Management to be included in the ICS security plan

**Number**

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

Awareness topic to be included in the ICS security plan

**Number**

4.4

**Description**

On-field staff should have guidance regarding: a) proper understanding of the current information technology and cyber security issues; b) differences between ICT and ICS technologies, along with the process safety and associated management processes and methods; c) developing practices that link the skill sets of all the organizations to deal with cyber security collaboratively.

**Impact**

Education and awareness issues should not be overlooked in a comprehensive security plan.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

**Title**

Security plans need to be adapted for every operator

**Number**

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview (29)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developping security programs, too costly for operators</td>
<td>4.6</td>
</tr>
</tbody>
</table>

**Description**

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

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview, Desktop Research</td>
</tr>
</tbody>
</table>

1.5 *Attitude towards information sharing and other collaborative initiatives*

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest in sharing initiatives</td>
<td>5.1</td>
</tr>
</tbody>
</table>

**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.
Protecting Industrial Control Systems

Annex V. Key Findings

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excessive size, constraints or private interests are the main disadvantages and risks of sharing initiatives</td>
<td>5.2</td>
</tr>
</tbody>
</table>

**Description**

Although the attitude is usually positive, 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unbalanced interest in cooperation between each group of stakeholders</td>
<td>5.3</td>
</tr>
</tbody>
</table>

**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 stakeholder.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active collaboration between the ICT security sector and ICS Manufacturers, essential to improve ICS security</td>
<td>5.4</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

1.6 Public Private Partnerships

Title

PPP sharing initiatives demanded by most stakeholders.

Number

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.
## Annex V. Key Findings

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

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

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

### 6.3 National or European funded security programmes to be improved.

**Description**

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

**Impact**

Stakeholders feel there are many opportunities to focus on.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

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

**Description**

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

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:** The table and text format was adjusted for readability and coherence.
1.7 **Common test bed**

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for independent evaluations and tests of ICS security products</td>
<td>7.1</td>
</tr>
</tbody>
</table>

**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 independent evaluations and tests of ICS security technologies and products.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest in creating a common test bed</td>
<td>7.2</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP, a European scope and supported by Academia the desired characteristics of the common test bed</td>
<td>7.3</td>
</tr>
</tbody>
</table>

**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 information sharing and reduce the heterogeneity of the ICS environment.
1.8 Dissemination and Awareness Initiatives

Title: Space for improvement in Dissemination and Awareness Forums.

Numbers: 8.1
Annex V. Key Findings

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aware.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
</tbody>
</table>

**Title**

High interest in participating in Dissemination and Awareness Forums.

**Number**

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aware.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
</tbody>
</table>

**Title**

Quality of ICS security events low-rated.

**Number**

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 presence 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aware.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
</tbody>
</table>

**Title**

Top Management awareness to be fostered

**Number**

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 business driver, providing economic reasons such as that, if considered during the PDCA cycle, it
can be good for efficiency purposes.

Incidents in industrial control systems should serve as a basis for risk assessment updates and to lead corrective measures and 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware.</td>
<td>Man&amp;Int</td>
<td>ICS Sec. Operator</td>
</tr>
<tr>
<td></td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion on technology-centric forums</td>
<td>8.5</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware.</td>
<td>Man&amp;Int</td>
<td>ICS Sec. Operator</td>
</tr>
<tr>
<td></td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation of an ICS-computer emergency response capability</td>
<td>9.1</td>
</tr>
</tbody>
</table>

**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.
1.10 Current situation of Technologic Threats and Solutions

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the technical threats identified by experts</td>
<td>10.1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

---

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

---

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

---

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.
Operators prefer to use mature and more economic technology.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Man&amp;Int</td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td>Academic&amp;R</td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Survey&amp;Interview</td>
</tr>
</tbody>
</table>

**Title**

Discrepancies within most demanded/acquired security services.

**Number**

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.

---

### 1.11 Legacy Related Risks

**Title**

Untrusted and legacy devices and protocols - nowadays' biggest threat

**Number**

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.

---

**Title**

Legacy devices working under invalidate assumptions. Long lifecycle of ICS.

**Number**

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 protecting these systems, but for economical reasons a compensating, multi-layer approach is being implemented in most networks. The situation is worsened by the fact that ICS technologies lifecycle is much longer than the usual ICT lifecycles. As a result, many current ICS systems may remain vulnerable for longer.

Impact

Many working devices are not prepared to face current cyber security threats.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Man&amp;Int</td>
<td>ICS Sec.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in security needed</td>
<td>11.3</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Man&amp;Int</td>
<td>ICS Sec.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Manufacturers already produce built-in security functionalities</td>
<td>11.4</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Man&amp;Int</td>
<td>ICS Sec.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

Title | Number |
## Annex V. Key Findings

### 1.12 ICT and ICS convergence problems

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS importing the ICT solutions and the ICT problems</td>
<td>12.1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular ICT solutions need to be adapted further to the ICS scenario</td>
<td>12.2</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

#### Title

ICT staff does correctly understand ICS requirements

#### 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 collaboratively it is unlikely that they will be able to reach unified and appropriate solutions for their problems.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

#### Title

ICS providers are not aware of security best practices of the ICT world

#### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol.</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

#### Title

Warnings about ICT security vendors into ICS.

#### Description

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

#### Title
- **Hardening often requires support from vendors and security tools and services providers**

#### 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.

#### References
- Survey&Interview, Desktop Research (23)

#### Title
- **Difficulties with vulnerability management on the Operators side and in the commitment of Manufacturers**

#### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS security dependance of the ICT QoS</td>
<td>13.3</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security in remote accesses</td>
<td>13.4</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org&amp;Pol</td>
<td>Stand.</td>
<td>Aware.</td>
</tr>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Man&amp;Int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS Sec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acad&amp;R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public B.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stand. B.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Computing not to be adopted in core ICS technologies</td>
<td>13.5</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

### 1.14 Present and Future Research

#### Title

Current research lines

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
</tr>
</tbody>
</table>

#### 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, Smart Grid standards and measures of effectiveness.

#### Impact

Lines of research have proven to give interesting results.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>

#### Title

Future research lines

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
</tr>
</tbody>
</table>

#### 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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td></td>
</tr>
</tbody>
</table>
1.15 Pending debates on ICS security and other related issues

Title: The security by obscurity debate

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.

Title: The debate about regulation enforcement by fines.

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.
### Reasons against regulation enforcement by penalties

**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 their security in various ways.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technic.</td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>

### Reasons for regulation enforcement by penalties

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technic.</td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>

### Debate regarding Smart Grid dependency on third party telecomm Operators.

**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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technic.</td>
<td>Acad&amp;R</td>
<td>Public B.</td>
</tr>
</tbody>
</table>
Protecting Industrial Control Systems

Annex V. Key Findings

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concerns regarding Smart Grid dependency on third party telecomm Operators.</td>
<td>15.6</td>
</tr>
</tbody>
</table>

**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 telecommunication operator. Many agree to require encryption and signatures to prevent information leaks.

**Impact**

Operators may need to adopt more security measures.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive points regarding Smart Grid dependency on third party telecommunication Operators</td>
<td>15.7</td>
</tr>
</tbody>
</table>

**Description**

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

**Impact**

There are important benefits deriving from subcontracting third-party telecommunication operators in the Smart Grid.

<table>
<thead>
<tr>
<th>Level</th>
<th>Stakeholder Type</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Econom.</td>
<td>Technic.</td>
<td>Acad&amp;R</td>
</tr>
</tbody>
</table>
2 References


Annex V. Key Findings


Annex V. Key Findings


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


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
CI   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
### Annex V. Key Findings

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

Annex V. Key Findings

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-  Infrastructure For Heterogeneous, Resilient, Secure, Complex, Tightly Inter-Operating
SECTION  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
NBS  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
Annex V. Key Findings

SSL  Secure Sockets Layer
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