enisa
European Network and Information Security Agency

Protecting Industrial Control Systems

Annex II. Survey and Interview Analysis

[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

Contents

1 Survey and Interview Analysis

This chapter presents to the reader an analysis of the raw data coming from the survey and the interviews. What is presented here is not the raw data itself, but a processed summary of the most relevant aspects of it. The chapter is divided into the following five sections or topics:

1. Organisational and policy aspects
2. Standards, guidelines and regulations
3. Economic and financial factors
4. Technical
5. Dissemination and awareness

Each one of these sections contains different concepts that are related to the topic of that section. However, interrelationships among concepts belonging to different sections can be highlighted. Key Findings presented in the main report are derived directly from this analysis.

1.1 Organisational and Policy Aspects

1.1.1 Cyber security challenges

All different stakeholders were asked about the main cyber security challenges in their area. The given answers covered a wide spectrum of subjects from many perspectives. Some of the most relevant ones were:

- **Gap between cyber security and other kinds of security, including physical security, environmental security, and process safety.** This statement is one of the most repeated ones. Many experts expressed the difficulty in making a valid Risk Assessment, and some stated the necessity of integrating cyber and physical security by using a holistic approach.

- **Lack of common/standard regulations.** Many experts consider that there is a lack of common regulations to follow in ICS. This is especially an issue when operators have different CIs in different countries, since they may have to deal with different regulations. As some interviewees expressed, **ICS security managers in Europe need a trustworthy source of useful information to follow**. However, this position is not equally supported by all stakeholders, since there are some discrepancies among them (see below).

- **Cyber attacks.** In particular, there is a concern with regard to the **advent of targeted attacks often performed by the so called Adaptive Persistent Adversaries** (The 451

Group, 2010). Additionally, many respondents showed concern about the possibility of having **malicious insiders** or the difficulty to protect remote devices such as FDADs, RTUs or PLCs, especially if they include wireless technologies.

- **Not enough involvement of senior management** or even an attitude of "we are doing enough" that is not always shared by the security staff.
- **Legacy issues and other technical issues.** Many different technical issues have been described, most of them related to security issues deriving from legacy equipment and the increasing presence of IT in ICS environments. Furthermore, several experts mentioned that security providers, coming from the IT market have a **poor understanding of ICS systems and their security needs**. Other technical issues are related to systemic dependencies and the difficulties to provide solutions where there are many different proprietary protocols.

Looking at the results from a "stakeholder" perspective, there are also some differences:

- Most ICS Security Products and Service Providers used to give technical answers, often related to the products and services they are familiar with, including also the presumable following steps in their evolution.
- Some experts, especially from Academia or R&D, also consider problematic the perception amongst some Operators' or Manufacturers' experts who still consider security-by-obscurity a valid approach.

1.1.2 Most effective mechanisms to address the challenges

All stakeholders were asked about the most effective way to address the challenges mentioned before. The answers given are shown in Figure 1 below:

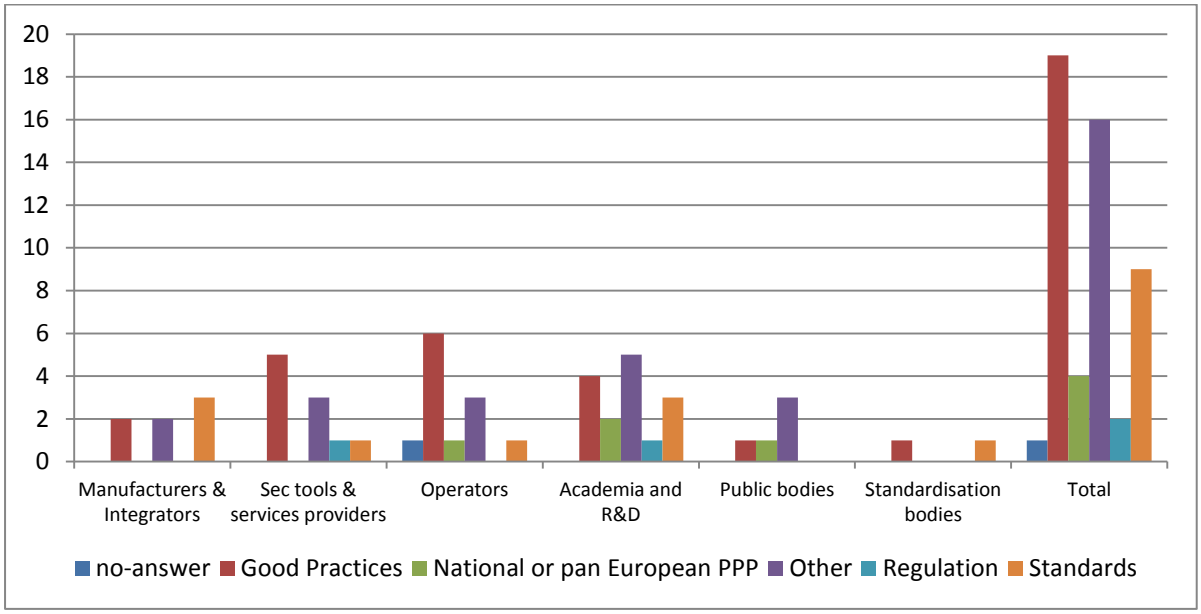

Figure 1: Most effective ways to address the challenges based on the opinion of stakeholders

From a global perspective:

- The most effective mechanisms are considered to be Good Practices (37%), followed by Standards (17%). Public-Private Partnerships (7%) and Regulations (4%) were the least supported mechanisms.
- More than 31% of respondents answered "Other" solutions, for which the experts suggested a variety of topics which often included aspects such as:
    - The combination of several of the aforementioned options. One of them might be the driver, but it will always be insufficient to address all issues.
    - Dissemination and Awareness as one of the most effective mechanisms.
    - Risk analysis and audits.
    - Considering security as a financial risk, so that ICS security would be considered important and be addressed by senior management.

Considering the different stakeholders it is interesting to see that:

- Manufacturers and Operators do not believe in regulations, only Security Tools and Service Providers and Academia have expressed direct support for it.
- Manufacturers, Security Tools and Service Providers and Standardization Bodies are not so interested in National or European PPP. There is a contrast between this and Operators, Academia and Public Bodies opinion.

1.1.3 Degree of adoption of Security Good Practices

All but Standardization Bodies answered about the degree of adoption of Good Practices on industrial devices and SCADA applications. Considering that 1 is a low level, and 5 is a high level of adoption, the respondents provided the following answers (Figure 2):

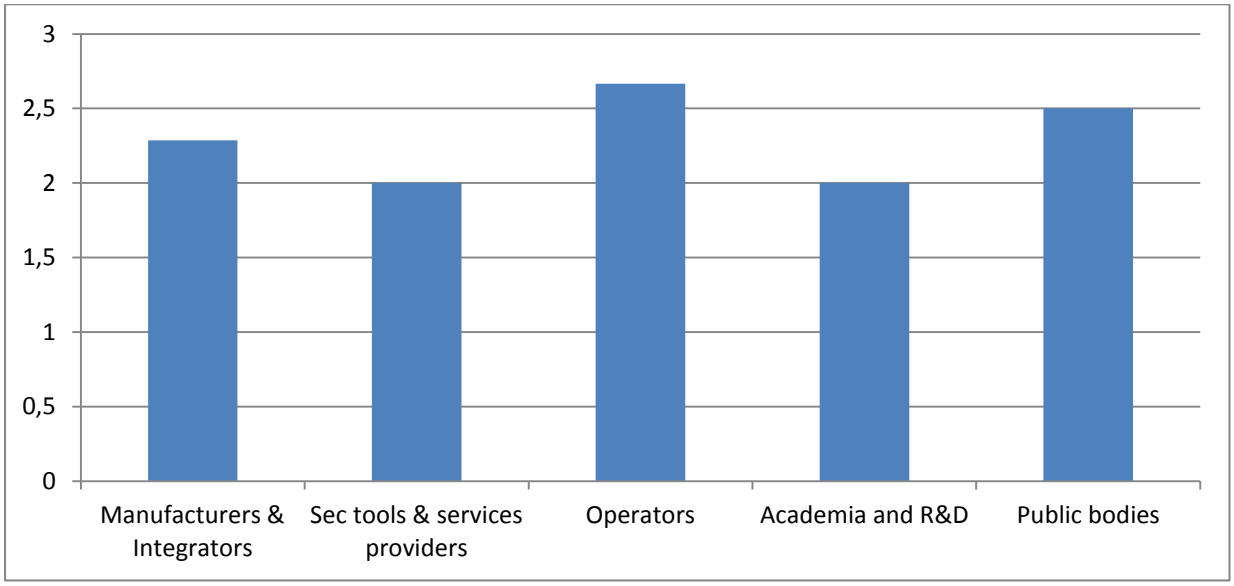

Figure 2: Degree of adoption of Good Practices per stakeholder (0-None, 1-Low, 2-Medium low, 3-Medium, 4-Medium High, 5- High)

The average level of adoption provided by stakeholders is, in every case, between low-medium and medium. There are no big discrepancies, but it is interesting to see that Operators consider themselves closer to medium adoption, while Security Tools and Service Providers consider that they are below that level.

It is important to state that manufacturers showed great discrepancies; a few considered themselves highly involved while most of them just medium-low. On the other hand Operators provided answers in the whole range of the proposed levels of adoption.

When asked about the most widely adopted ones, most respondents answered with examples on standards, good practices and regulatory documents (this topic will be covered further at point 1.2.2 Standards adoption status). Some US and international standards or regulatory documents such as NERC-CIP, ISA-99 or ISO27002 are among the most followed ones.

1.1.4 Participation in exchange platforms/national PPP

All stakeholders were asked about their participation in information exchange platforms and national Public-Private Partnerships (PPP) as well as their opinion on their effectiveness (Figure 3).

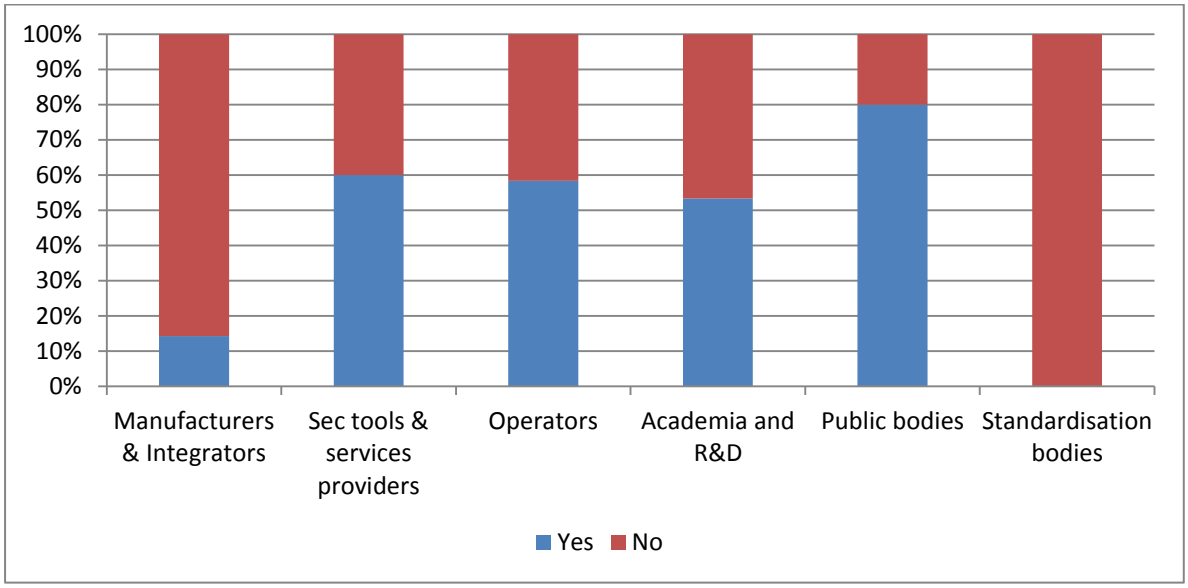

Figure 3: Participation in information exchange platforms/national PPP.

Despite the high interest which most stakeholders have shown in this kind of initiative in other parts of the study, less than half (47%) was actually participating in them. The fact that Manufacturers are so weakly involved in these initiatives (14%) may be surprising, especially in comparison with the other on-field stakeholders. They did not even provide the reasons for their reluctance.

The effectiveness of exchange platforms and PPP is, however, discussed. There were many spontaneous comments, regarding their interest and positive aspects, but some of them think it is difficult to provide real or long-lasting improvements in security through this type of cooperation.

Several vendors involved with the UK-CPNI were satisfied with the colour-code classification of the information shared. This provided them confidence on how this knowledge will be shared. But, apparently, the more restrictive the information is (i.e. red: just for members) the more difficult to use it effectively.

Some US interlocutors also showed their concerns about too big sharing initiatives, with excessive formalism, where many companies participate just to defend their economic interests. Different respondents consider that the info-sharing initiatives are more effective when they focus on specific business needs and not just in better ICS security technologies. The same technologies may be adapted for several functionalities, but specific issues come from productivity and business objectives.

1.1.5 Collaboration agreements within organizations

On average, a majority of stakeholders has collaboration agreements with other organizations (56%), but again, Manufacturers and Integrators are highly below the average (28%). Operators, in this case, are not so collaborative (40%) but all other stakeholder types are over the 60%.

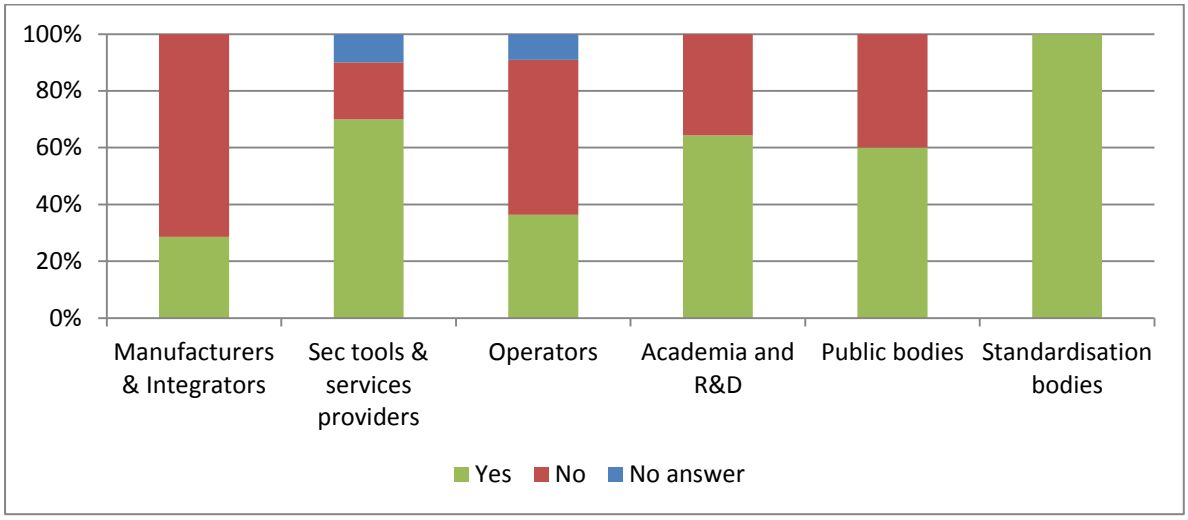

Figure 4: Collaboration agreements within organisations.

When asked about the areas covered in such agreements the most common ones were: risk assessment and management, particular technical issues and dissemination and awareness initiatives.

It is interesting to see that stakeholders, especially Operators, are often interested in sharing information with their peers (e.g. Operators with Operators) and that, sometimes, they lack support from public institutions to join them in associations, or organisms. Some experts informed that bilateral approaches are often stronger and more effective than multilateral agreements.

1.1.6 Relations among stakeholder types

Survey participants from each group of stakeholders were asked to evaluate how necessary it was to cooperate with other types of stakeholder.

In the following graph the global interests of each stakeholder type is displayed. The lowest punctuation was 0 (no interest) and the highest was 3 (highly interested).

Results are represented in two graphs. In the following Figure 5, each stakeholder shows their interests in cooperation with other stakeholder types.

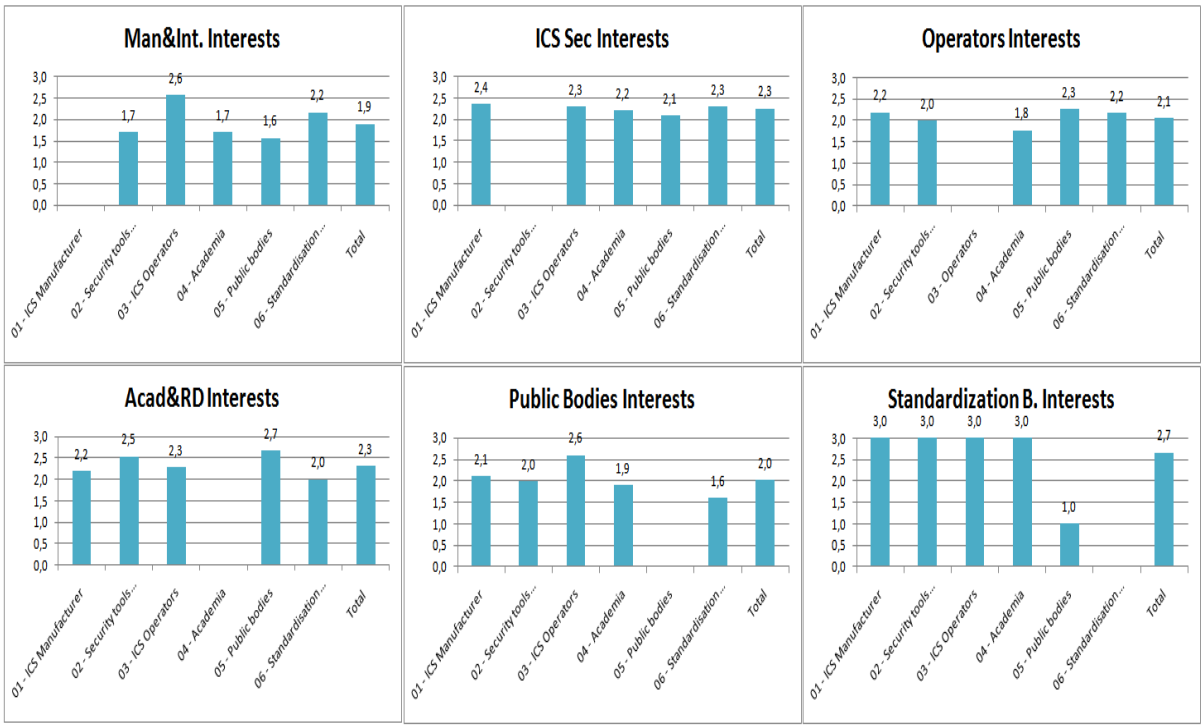

Figure 5: Interest by Stakeholder

On the other hand, the graph displayed in Figure 6 shows a complementary view of that information, displaying how much interest the other stakeholder types have in working with them.

Analysing the results (see Figure 5) it is easy to see that the average interest to cooperate among stakeholders is medium. Being Standardization Bodies, ICS Security Tools and Services Providers and Academia the ones showing the highest interest (more than 2'3)), and Manufacturers and Integrators the lowest (1'9). Operators, Public and Standardization Bodies are all very close or equal to 2.

Taking a look by stakeholder type:

- ICS Manufacturers are mainly interested in working with Operators and Standardization Bodies. They show medium-low interest in working with any other. But checking Figure 6 it is clear to see that most stakeholders are more interested in working with them.

- Security Tools and Service Providers have one of the highest scores for interest in cooperation, but they get just medium attention from most other stakeholders. Only academia shows a high interest in cooperation with them.

- Operators have special interest in working with Public & Standardization Bodies and Manufacturers, and the interest is mutual as shown in Figure 6. In fact, they are the stakeholder most in demand.

- Academia and R&D have the highest interest in cooperation, with Public Bodies and Security Tools and Service Providers getting the top scores. However, they are not very appealing to other stakeholder types (with the exception of ICS Security Tools and Services providers, which show a medium interest level).
- Public Bodies focus their attention on Operators, while Academia is the stakeholder type that gets a higher score when rating how necessary it is that Academia collaborates with them.
- Standardization Bodies have a high interest in working with any other stakeholder type, except Public Bodies. It is interesting to notice that public bodies don't show a very high interest in collaborating with standardisation bodies either.

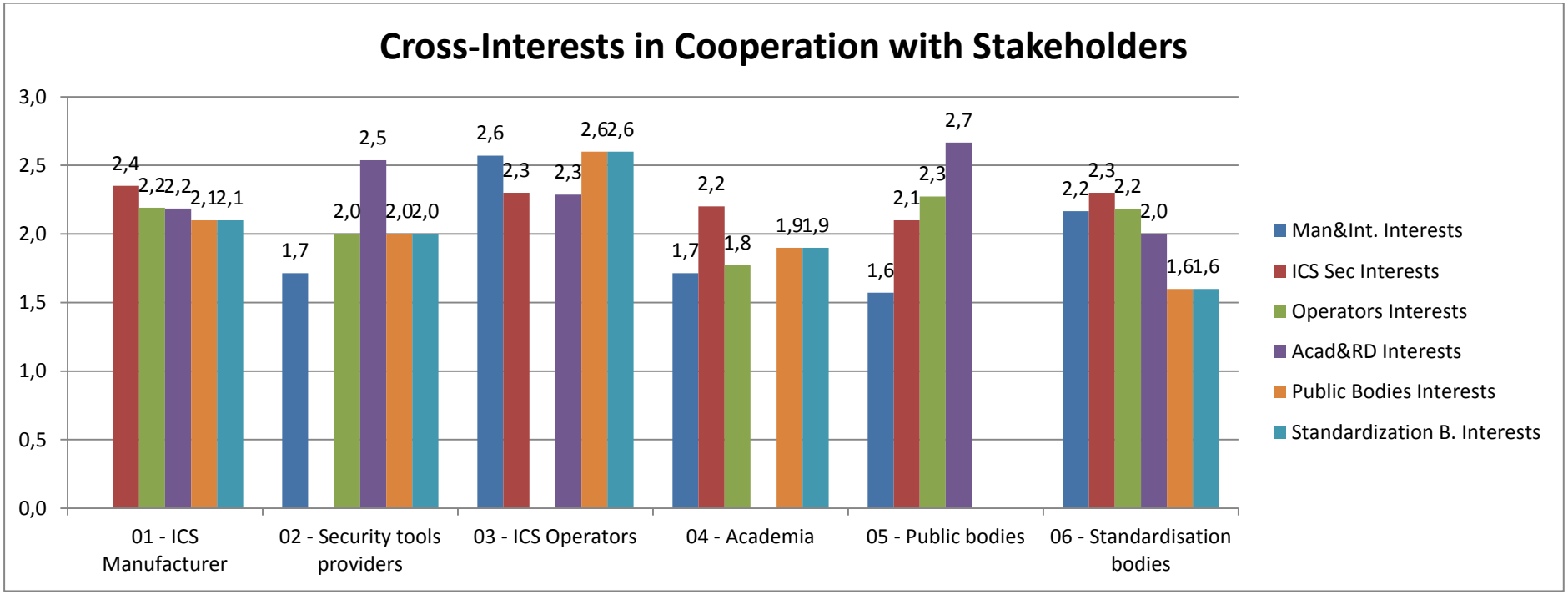

Figure 6: Cross-interest in cooperation. (Note: Graph represents the interest other stakeholders have in working with the one on the X axis).

1.1.7 Interest in creating a common test bed

All stakeholders were asked about their interest in the existence of a common test bed to validate and verify (i.e. certify) security aspects and functionalities of control equipment, industrial systems and applications.

As shown in Figure 7 there was a very high level of consensus in favour to the existence of such a test bed. Just 12% of Manufacturers and 20% of the Public Bodies were unsupportive of the idea.

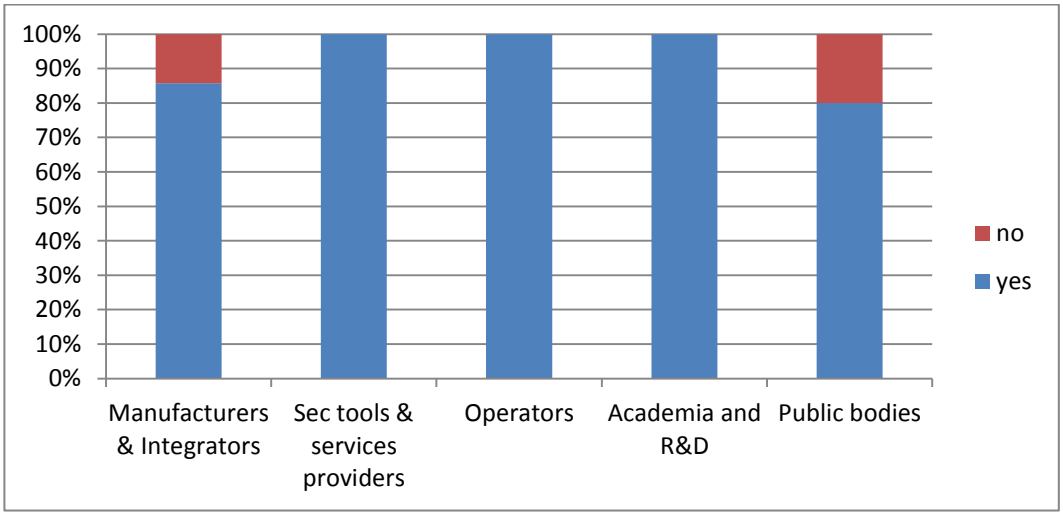

Figure 7 Interest in the existence of a test bed for the verification of security functionality of ICS equipment and applications

Regarding how it should be founded, a high majority of stakeholders (81%) believe that this should be done on a public-private basis. Only a minority of the respondents, but corresponding to a significant 33% within Manufacturers, think that it should be completely public. Furthermore, there is almost no agreement for the private alternative.

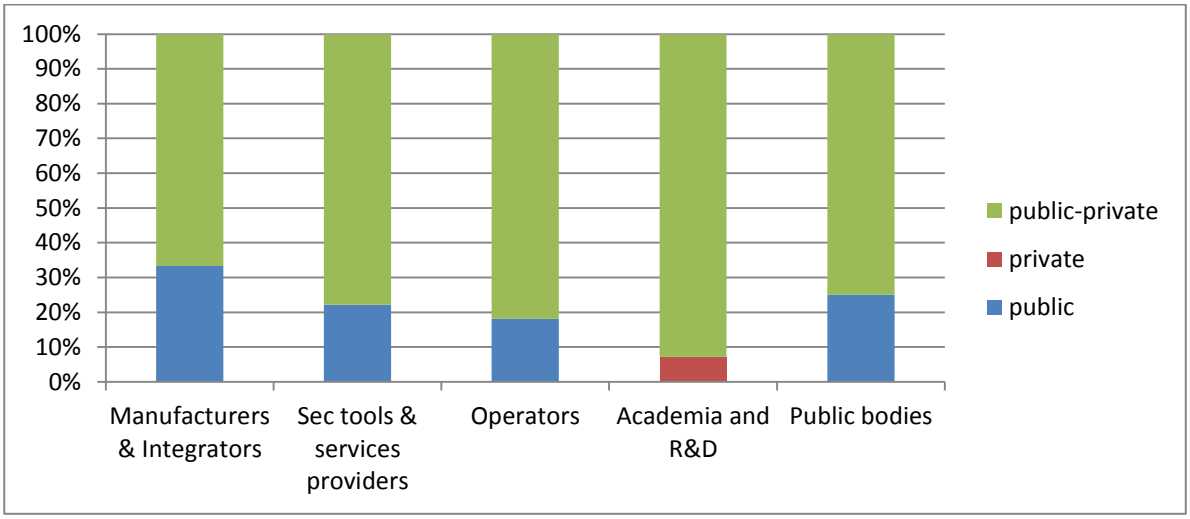

Figure 8 The basis in which the test bed should be founded: public, public-private, private

As shown in Figure 9, there is also wide agreement in providing this test bed at a European level, as an alternative to having multiple national initiatives. Only among Security Tools and Services Providers and Public Bodies could there be some debate: 25%-33% of the respondents of these two types of stakeholders are for the "national" alternative.

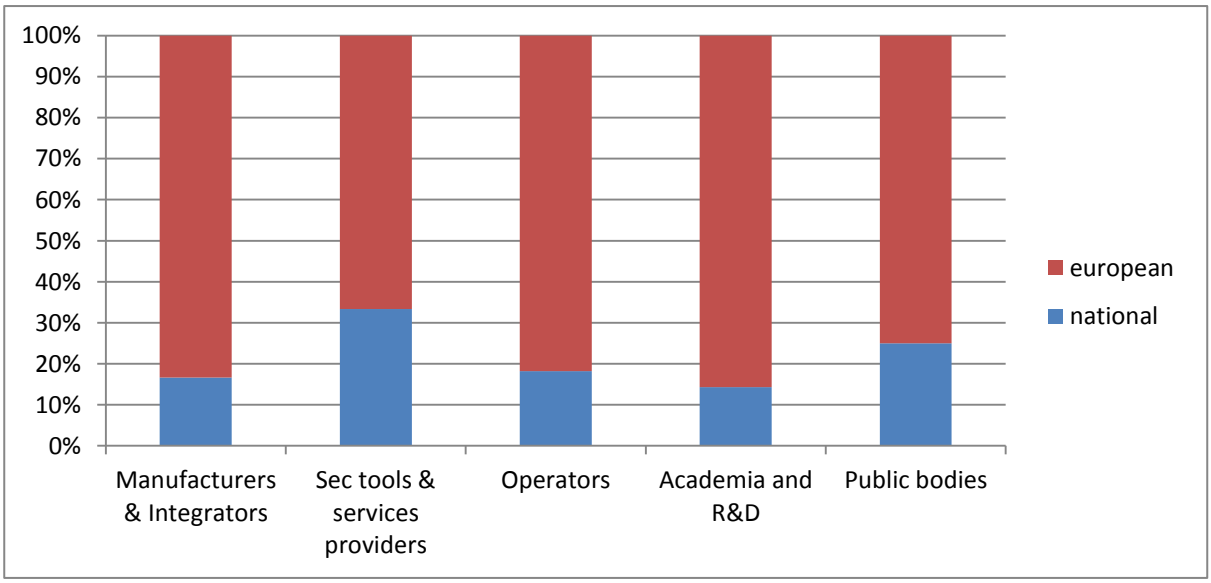

Figure 9 About the scope of the test bed. Two options are provided: European or national

During the interviews, the topic was discussed further with some interlocutors. One of the experts shared with us a reason why such test beds would be very appreciated by operators. He argued that simple Windows patches, applied in a few days on IT platforms, may take 2 years to apply to an ICS network because of the great need for caution to prevent outages or disasters. A test bed could greatly compress that timeframe. Some other experts think that it

is unlikely to create an efficient test bed, able to check all relevant technologies. Furthermore, they provided possible alternatives to such a test bed:

- define a security model or framework such as Common Criteria or FIPS, adapted for ICS,
- make existing national certifying organisms in all member states or at European level, follow this criteria to certify any product;
- a competent public authority, to force operators to use certified systems or applications.

Academia was specifically asked whether and how they would like to contribute to this test bed. With 93% positive answers, they think they can provide:

- A deeper view into some technical aspects, and also be more general and complete as they would be presumably more business agnostic, independent and objective.
- Some of them have experience at developing test beds.
- Tests could be designed in cooperation with operators to provide real data and procedures.
- They could help identifying relevant technologies to aid ICS players.

Some experts also pointed out the fact that some programs as ESCoRTS, VIKING or ASTROM are paving the way to such a structure.

1.1.8 The challenges of introducing the Smart Grid

Manufacturers were asked about their challenges and concerns regarding the Smart Grid. There were a variety of opinions:

- The technical challenge was 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.
- There is a debate about the suitability of developing European security standards and certifications. Some consider this necessary, while others think that homogeneous

solutions are less preferable for security and they also mistrust political interferences and their consequences[1].

- Some experts have the impression that companies do not show a high interest in cyber security.
- A few experts expressed their concern about compromising end customer privacy.

1.1.9 Operators' independency in Security Controls implementation

Operators were asked about who was in charge of the implementation of security controls that affect ICS. They had four possible answers to choose:

- to do it all on their own,
- to require external expertise only for very specific purposes,
- to assume only some high-level security controls, such as the definition of security policies,
- to ask for advice for all security controls.

As seen in Figure 10 most operators are completely or mostly independent regarding security controls, although half of them require some support. It is interesting to point out that it is not common to depend on external experts for most or all controls.

To a certain extent, the answers given to this question could show the attitude of Operators towards the security of their ICS. ICS are behind the most critical parts of their core business, and therefore they 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 will be showed later in this chapter (see section 1.1.10), 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.

[1] *Such as compulsory backdoors to be created and shared with governments.*

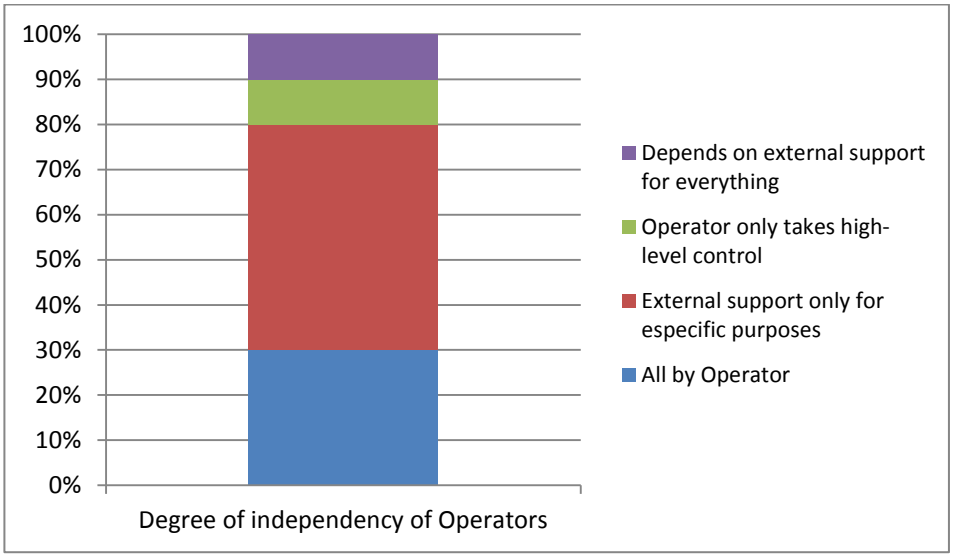

Figure 10: About who is in charge of implementing security controls for ICS protection

1.1.10 Operators current status in implementation of Security Good Practices

Operators were asked about their current status with regard to the implementation of security good practices and policies affecting their control and supervisory systems. They were offered four predefined levels and an open text box to describe their situation.

As seen in Figure 11, the biggest group of operators (36%) is now at the early stage of performing a Risk Analysis. 27% have finished it and now have a security roadmap. Only 18% are currently undertaking security projects regarding a strategic security roadmap.

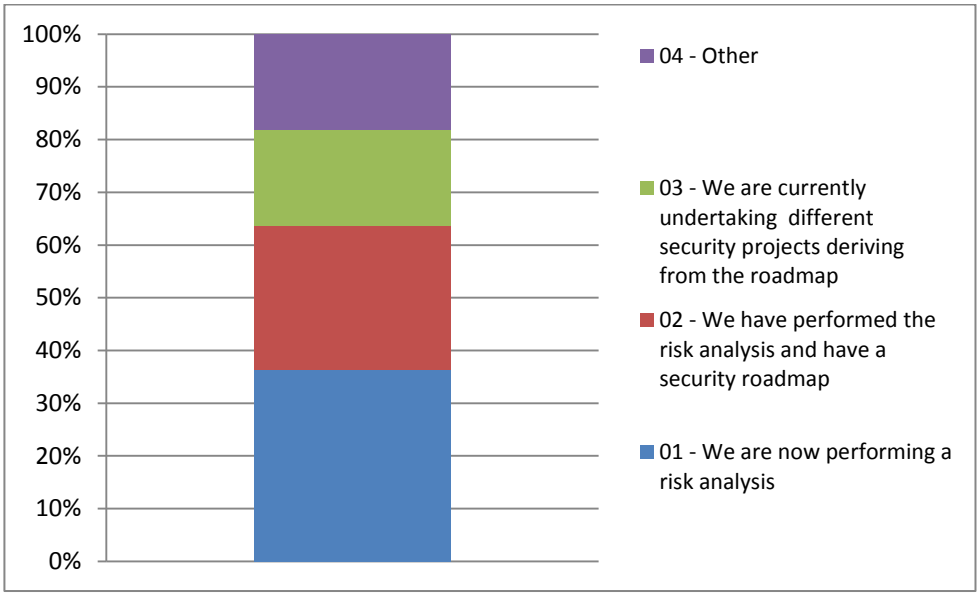

Figure 11 Operators' current status with regard to the implementation of security good practices and policies

When they had the opportunity to explain their situation, several expressed the difficulties in developing an agreed plan between different management boards, states or sectors.

1.1.11 Security Management in Organizations

Operators, Public and Standardization bodies were asked about several issues related to ICS security management.

Regarding whether the same person should be in charge of logical and physical security, a strong disagreement was found between them. Most Operators (70%) believe that they should be different people, while Public Bodies think it should be the same person (80%).

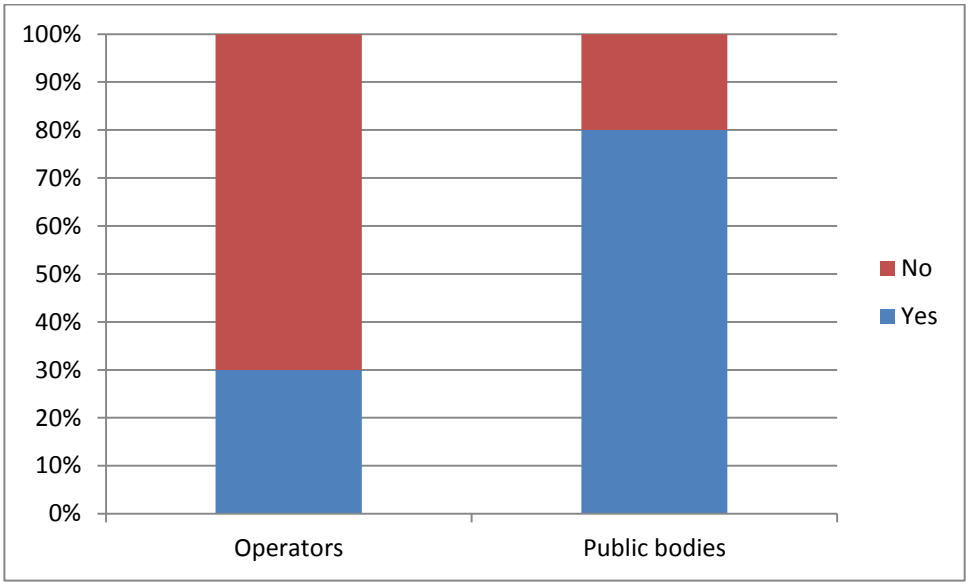

Figure 12 Operators and Public bodies opinion with regard to whether the same person should be in charge of logical and physical security

There were also discrepancies about to who the ICS Security Manager should report to. The given options were the Chief Information Security Officer (CISO) or the highest level of Management. All public Bodies respondents chose Top Management, opinion shared by less than a half of Operators.

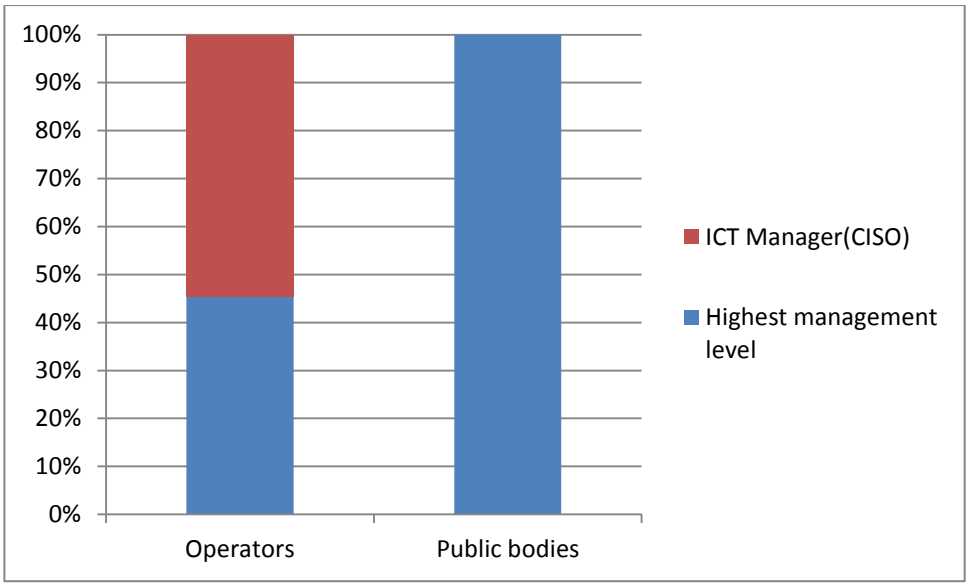

Figure 13 About who the ICS Security Manager should report to

When asked about how much commitment operations staff should have on specific ICS security issues, a great majority thinks that they should be highly committed periodically participating in IT security courses and being aware of the general ICT security policy and of the specific control systems' security policy.

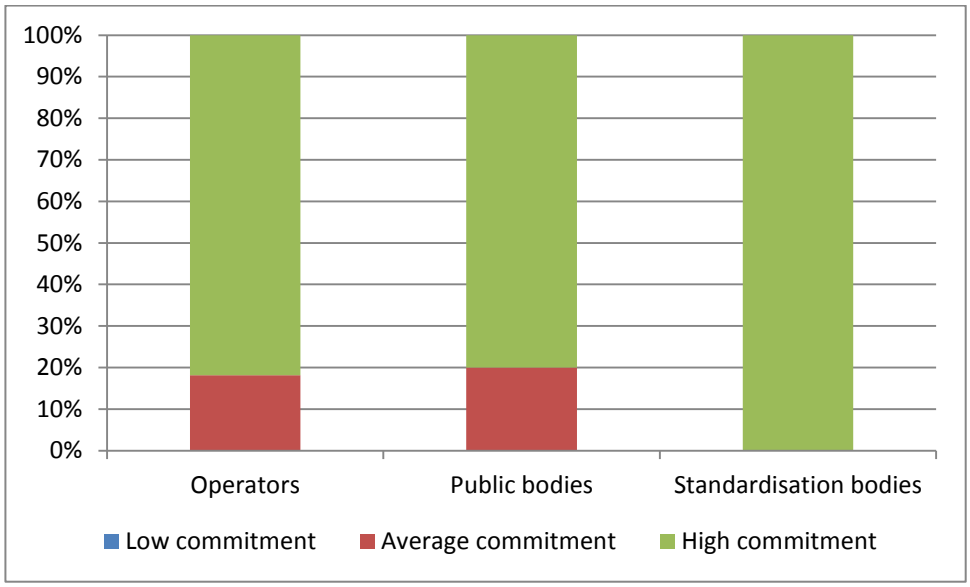

Figure 14 About the commitment of Operations staff with regard to ICS security

Then they were asked if each operator would need to define their own operator and/or infrastructure level security plan. Within the answers:

- All respondents think that there should be security plans defined for each operator.
- Most think it would be useful to have a general template or guiding document with local variations.
- This was agreed especially by electric operators, where interdependencies are strong.
- Among the Spanish experts, there were various positive comments regarding the Spanish Law for the Protection of Critical Infrastructures (LPIC) and the regulation to articulate it (RDPIC) as a way to provide order, homogeneity and a reference framework, raising the importance of logical security in CIs.

In relation to which aspects should be addressed in such security plans, both Operators and Public Bodies showed a high level of agreement. All Operational, Physical Security, and Technical issues are widely supported, and just some (33%) believe other aspects should be included. Within the answers several interviewees expressed there must be one security plan, with a holistic approach addressing all security aspects: safety, cyber security, physical security, environmental security, etc.

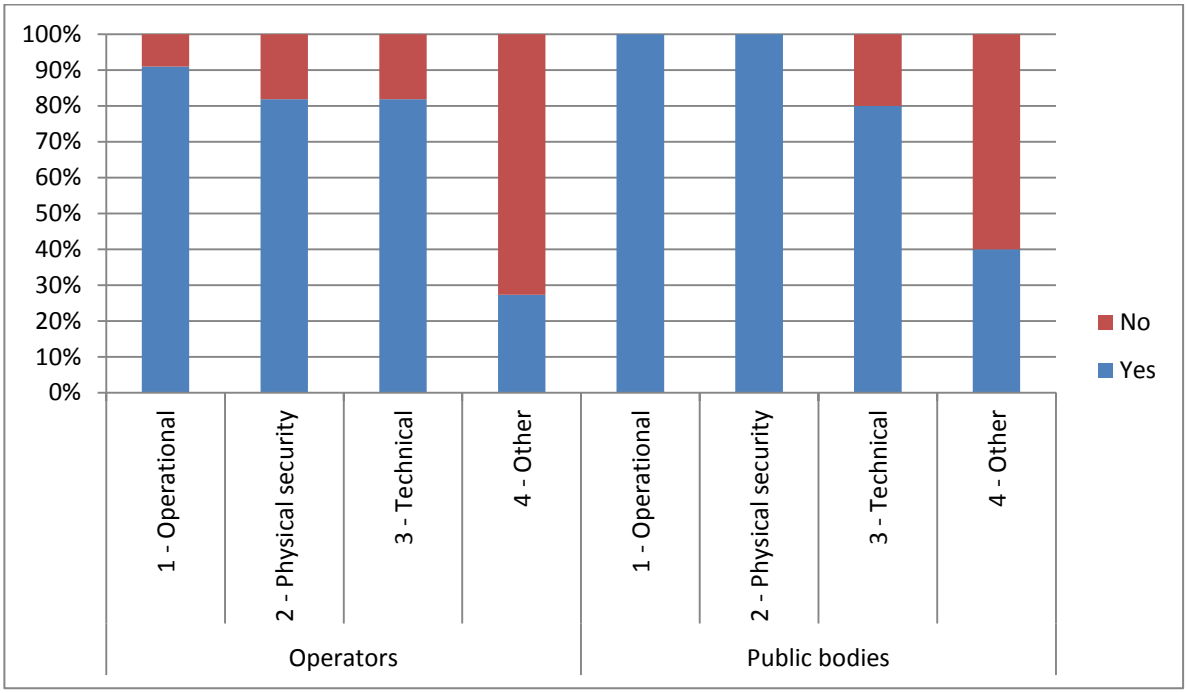

Figure 15 Aspects to be addressed in security plans

Other interesting points to address in security plans were (in order of the frequency with which they are mentioned):

- Education and awareness, especially within Top Management
- Security governance, roles and responsibilities
- Business impact and trying to present security as a Business Driver
- Crisis management and communication
- Audits

1.1.12 Cyber security perception within operators

Operators were asked whether cyber security was considered a burden for the normal activity of the control systems.

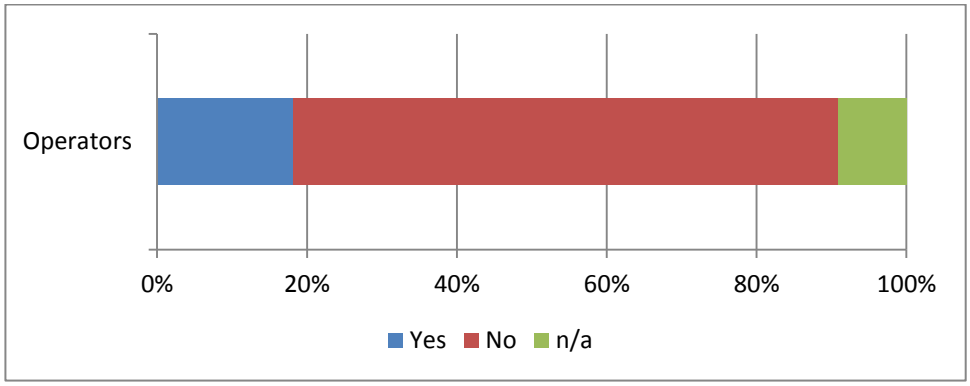

Figure 16 On the perception of security as a burden by ICS Operators

Just a minority of them (18%) have this perception, while 72% of them consider cyber security as an inherent part of the normal activity of the control systems. The main obstacles to deal with are:

- Awareness at all levels of people not involved in security, from board management to final users and staff not committed to ICS security (including ICT), was the biggest problem for most of them.
- A few of them signalled the high costs of security pointing out the difficulty in explaining this (and justifying the investments) to Top Management.

1.1.13 Other Organizational Aspects from the interviews

Some other topics arose during the interviews. The most relevant ones were:

- Regarding the recent recommendation in the US to consider sabotage attacks against CI as an act of war, and whether something similar is needed in Europe:
    - Most refer to the existence of common criminal laws that protect these assets in the same way as any other. They also state that in the US this area is more developed, but not all of them think this is better, arguing that this process has been carried out “too fast”.
    - Some think that current criminal laws are not very tightly related, but this might become useful over time.
    - Some think that a similar code for the EU is interesting, but that it may not be applicable since the current state of the art in forensic techniques does not allow for gathering the strong evidence needed to be 100% sure to start a war.
- About convergence of physical and logical security:

- Most think that it should be unified, as they both influence each other. Furthermore, the boundaries are fading as some attacks (and risks) that needed physical action years ago may be perpetrated in cyber space nowadays.
- Many experts think that there should be one security responsible person supported by two separate branches, or even three (safety, physical protection and logical security).
- Some consider it is too soon for this convergence.

- Some experts warn that there are still designs created under the conception that security can be and add-o layer to be placed later. They express that this is an error stating that security must be built in from the very beginning of the design phase.
- It is important to be aware of the fact that there is a difference between being secure and being compliant. If Top Management feels secure through being compliant, there is a reason to worry. Not all funding has to be spent on, and just on, being compliant.

1.2 Standards, guidelines and regulations

1.2.1 Familiarity with ICS security standards, guidelines and regulations

With regards to this, a comprehensive check on the standards and regulations[2] known and used by the different stakeholder was performed[3]. Standards proposed were those with a worldwide influence from standardisation organisations like IEEE, IEC, or ISO. Some others from the USA were also included since they are considered by many a reference in ICS security.

[2] *In the following they will all be called "standards" for simplicity even if they are Guidelines or regulations*

[3] *Standardization bodies were removed, as there was only one respondent.*

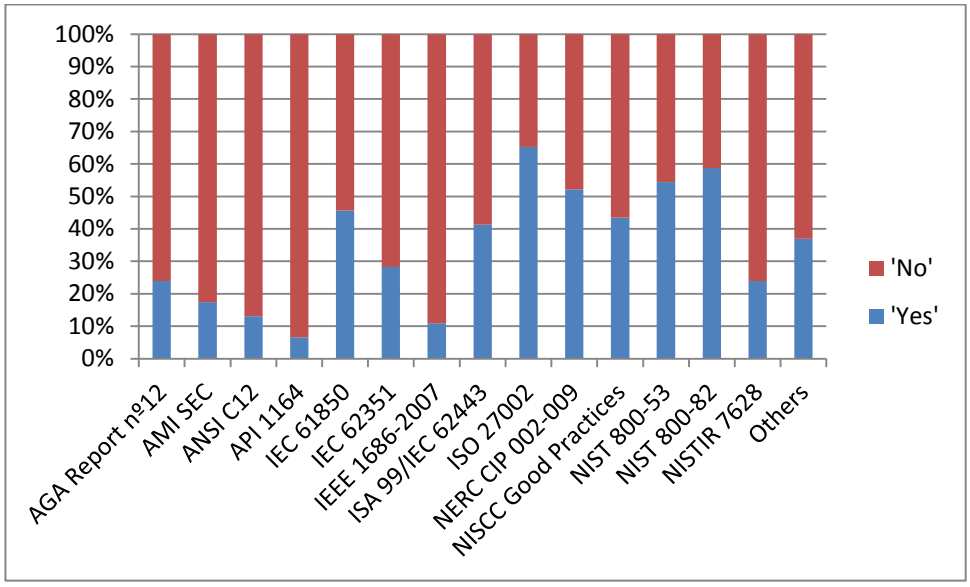

Figure 17 Average familiarity level with a number of standards, guidelines and regulatory documents

By analysing the results for each standard, independently of the stakeholder type (Figure 17)[4]:

- It is seen (as it was presumed) that the generic ISO-27002 is the standard most stakeholders are familiar with.
- NIST 800-82 guideline, regarding the ICS protection, is also well known.
- Many other US documents coming from the NIST are closely followed. Even a brand new one such as the NISTIR 7628 that just concerns Smart Grids.
- It might be surprising that experts are familiar with some regulations, such as NERC-CIP, when they only apply in the US. This is remarkable for Operators (see Figure 18).
- US Standards such as AGA 12 or API 1164 only affect certain sectors. Therefore their low grades can be considered logical.
- Regarding IEC 62351 it is interesting to point out that Manufacturers and Operators are pretty familiarised with it while ICS Security Tools and Service Providers and Public Bodies are not.

[4] *In Figure 18 there is a more detailed graph of these results by stakeholder type.*

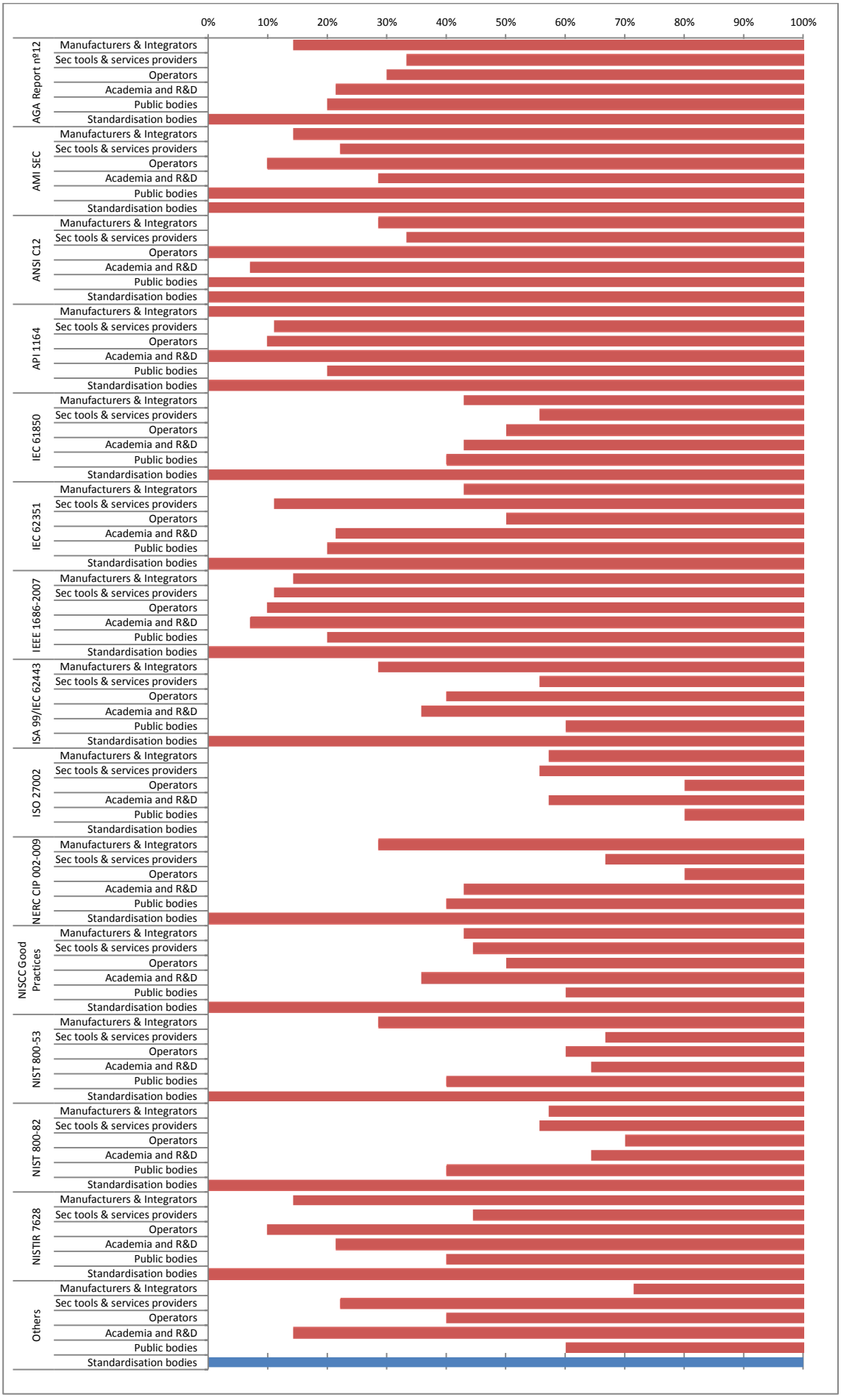
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
AGA Report nº12
AMI SEC
ANSI C12
API 1164
IEC 61850
IEC 62351
IEEE 1686-2007
ISA 99/IEC 62443
ISO 27002
NERC CIP 002-009
NISCC Good Practices
NIST 800-53
NIST 800-82
NISTIR 7628
Others
Manufacturers & Integrators
Sec tools & services providers
Operators
Academia and R&D
Public bodies
Standardisation bodies

Figure 18 Familiarity level by stakeholder type

1.2.2 Standards adoption status

ICS Manufacturers and integrators, ICS Security Tools and Services Providers, as well as Operators were asked on the degree of adoption regarding the implementation of the standards already presented. Several options were given: discarded, observed, implementation in progress, and implemented.

The answers to this question are summarised in the following figure:

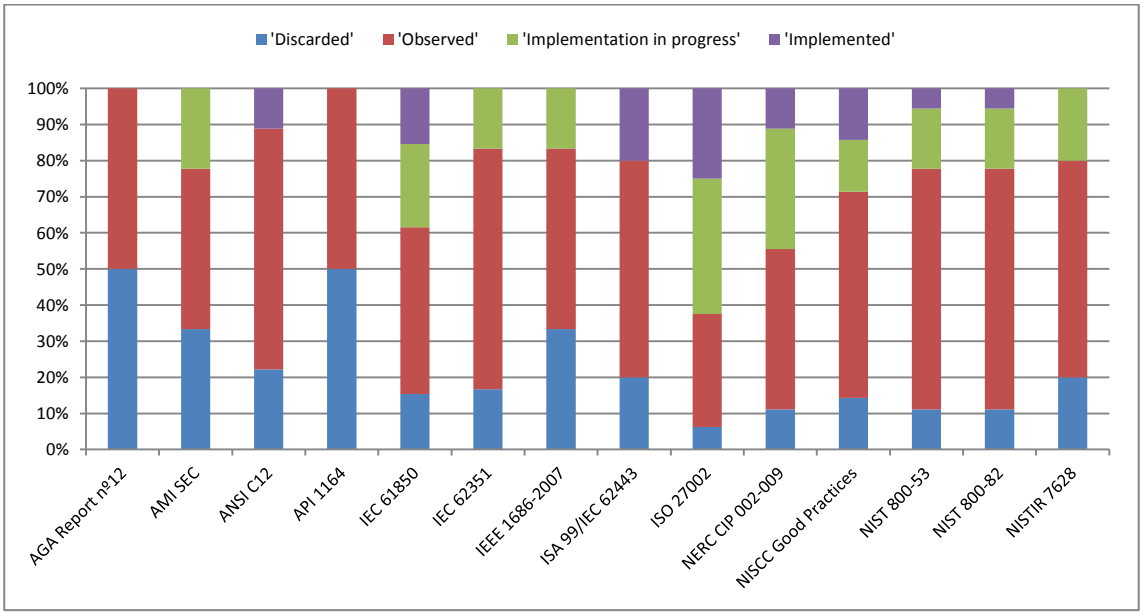

Figure 19 About the implementation of ICS related security standards

From the graph above some interesting results are inferred:

- Standard ISO 27002 is the most adopted and the least discarded. Almost 90% of the respondents have at least observed it, and over 20% have already implemented it.
- Surprisingly, NERC-CIP is highly adopted, even if most respondents are from European countries. NIST 800-53 and SP 800-82 are also widely observed and even implemented in some cases.
- In the case of ISA99 none of the interviewees are currently in the process of implementing it. Some have already accomplished it (20%) and many are thinking about it. This might reflect hesitation from stakeholders due to its difficulty in adoption and that there are still missing parts to be published.
- Others, like IEC 62351, IEEE 1686-2007 or NISTIR 7628 are being widely observed, and some stakeholders are trying to implement them even if no one has yet completed.

This might be a consequence of their recentness (NISTIR 7628) or a difficulty in their application.

- AGA 12 and API 1164 are not interesting for our respondents, as shown before.

1.2.3 Most valuable aspects of security standards

The overall impression that Manufacturers and Security Tools and Service Providers have on security standards is positive. They consider that:

- Security and Risk Management are the most important aspects which should be addressed by standards.
- A holistic approach to security is also welcome.
- Some experts warn about the danger in providing possible attack clues to attackers when they get too technical.
- There is a disagreement between those that believe that security through obscurity is convenient and those who believe in the advantage of open standards and other measures such as host bastionning (hardening) and vulnerability management.

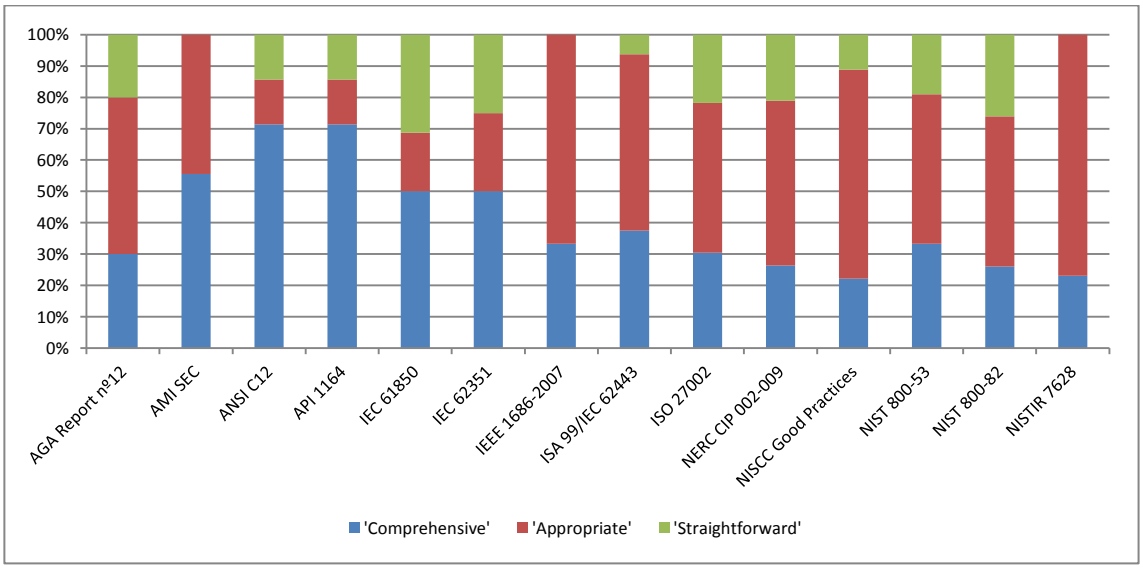

Figure 20 Classification of ICS security standards based on their contents

However it was also observed that there is some frustration regarding them. For instance an expert shared his opinion on utilities that have invaded standardization groups to ensure that the standards are not too expensive to comply with. As a result, lots of standards are diluted before they are accepted by the entire body.

Stakeholders were asked to classify the different standards as Comprehensive[5], Appropriate[6] or Straightforward[7]. Even if those values are not mutually exclusive, it was requested to state their most valuable characteristic.

- It is interesting to see that most adopted standards (such as ISO27002, NERC CIP or ISA99) are the ones that make the greatest variety of impressions.
- Those perceived as valuable to business are adopted.
- Standards mostly perceived as "comprehensive" are, in general, the same ones that were not being implemented (see point 1.2.2)

1.2.4 Manufacturers attitude towards standards

Manufacturers were asked about their degree of involvement to help their clients to be compliant with the standards presented. Five different options were presented: negative attitude, indifference, interested, working on it, and high priority.

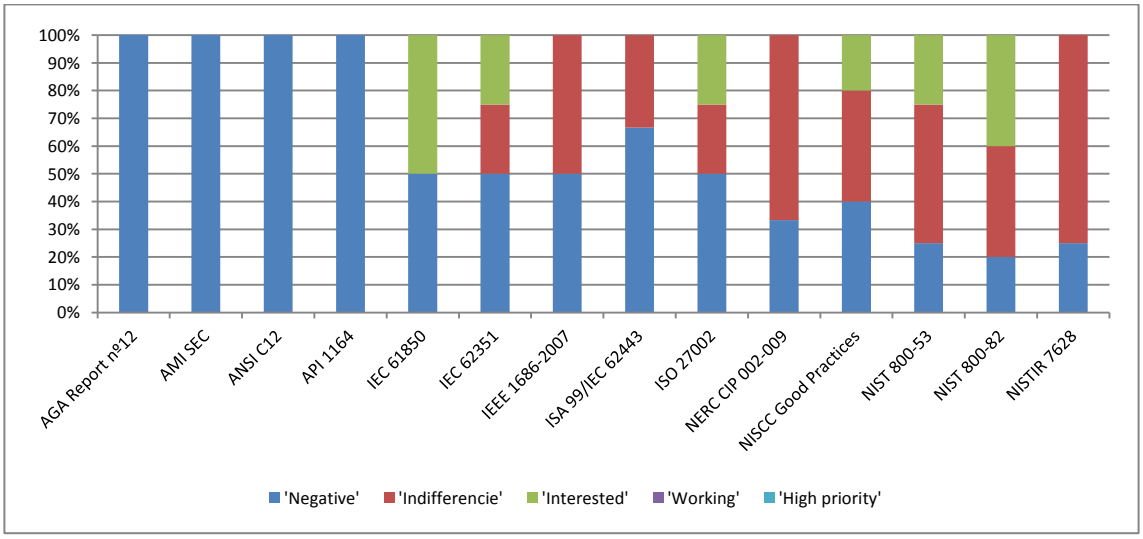

Figure 21 Manufacturers' attitude towards ICS security standards

Manufacturers' attitude towards the standards is displayed in Figure 21. From the results it is easy to see that:

[5] *The concepts being presented cover the most important security aspects and with an appropriate level.*

[6] *The standard/guideline is necessary and adds value to the business.*

[7] *The concepts being presented are well defined and clearly oriented.*

- Manufacturers show very little interest in the selected standards. They have, mainly, a negative or indifferent attitude towards most standards.
- None of them is considering these standards a high priority. No one was working on helping their clients be compliant, either.
- There is some interest (always less than 50%) in only six out of 14 standards (IEC 61850, IEC 62351, ISO 27002, NISCC GP, NIST 800-53 and NIST 800-82).
- IEC 61850 has the peculiarity of being the most problematic one. It raises 50% of interest and 50% of negative attitude.

1.2.5 Developing European security Good Practices for the industry

Most respondents think it will be necessary that best security practices and security standards for the Industry (manufacturers, operators, providers, etc.) are developed in Europe. This means to develop pan-European standards first, then each member state could use those as a basis for their own standards or as a direct reference.

- 64% of Operators think that it would be useful, even if a significant part of them (27%) have some reservations. They do not want certification per se if it does not provide real security in their systems.
- Many think that it is not necessary to “reinvent the wheel” but instead just to work in cooperation with the USA, Asia or Australia, trying to clarify the links between the already too numerous existing documents. One of the experts mentioned that a conclusion of the ESCoRTS project is necessary to describe how to use existing standards to improve security of ICS. In fact, one of the tasks deriving from the follow-up of the ESCoRTS project was to send a proposal to DG Enterprise to obtain the support to come forward with a document in order to bridge that gap.
- Some of them would prefer not to work too closely with the USA and take more advantage of the progress done by European Member States.
- The influence of private interests also raises some distrust within stakeholders. Objectiveness must be guaranteed by Public or Academic entities.
- Public Bodies showed interest in developing good practices even if most have never participated in such an initiative.
- During the interviews, some experts pointed at ENISA and Euro-SCSIE as driving forces in this initiative.

1.2.6 Public Bodies perception on EPCIP

A majority of respondents (75%) consider that the work done in the European Programme for Critical Infrastructure Protection (EPCIP) and the deriving National Critical Infrastructure Programmes have been effective in fostering the adoption of security Good practices. During the interviews, it was stated that the Stuxnet phenomenon, appearing in general media, has also fostered the adoption of security good practices.

1.2.7 Market impact of security standards

Security Tools and Service Providers and Operators were asked if service or products are specifically demanded to fulfil compliance requirements. 61% of respondents said that it is, in fact, one of the buying reasons.

Some interesting opinions about this topic were given:

- ICT Security vendors have started to focus on ICS security compliance during the last two years, but the impression is that they are only superficially adapting technologies, and not providing real ICS security.
- There are still many operators that do not need to be compliant with ICS security regulation. Extra budget to be compliant with regulations from outside Europe is hard to justify.
- Several Operators are making efforts to implement security controls following good practices or regulatory documents even if compliance with them is not compulsory.
- During the interviews, a few 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 pointed out as an appropriate organism to do so.

1.2.8 Regulation enforcement by penalties

As NERC-CIP has been implanted in the US by charging fines to non-compliant Operators, the suitability of the idea was discussed with Operators and Public Bodies. The most interesting aspects of this discussion are described below:

- There is a strong debate. About 60% do not like the approach since companies may focus on not being fined instead of being secure. Good practices and standards, supported by Public Bodies (at national or European level) are preferred.

- During the interviews various interlocutors warned about the fact that NERC-CIP allowed operators to decide on which are their own “critical assets”. This allows operators to pass the compliance audits without being secure.
- On the other hand, many think that this is an effective way to proceed, as inexperienced management could see the impact of not being secure in their economic balance sheet.
- A Public Body expert stated that the experience with Operators is that they don’t want to be regulated (with the nuclear sector the only exception) but when they understand the cascading effects to their networks when another Operator has a severe failure they normally change their point of view.
- An expert explains that in the USA the experience is that utilities most often react to standards such as NERC CIP, which can carry fines for non-compliance. He considers that there is a tremendous amount of work that could be done to better secure control systems, but it may not happen unless there is either (1) more standards that have financial consequences or (2) a terrorist attack that scares everybody senseless.

Other interesting aspects regarding this topic that arose during the interviews are:

- Sometimes governments require compliance for regulations in which operators have not participated. This can cause many problems due to unrealistic demands.
- Public Guidelines often arrive late, causing inefficiencies. For example, if a problem has to be solved but there are no guidelines, the operator would have to solve it on their own, requiring greater effort. Later, when there is a public guideline, it is very likely (almost certain) that some changes would have to be made.
- A few experts think that some exemptions to liability could be promoted for companies that implement security requirements.

1.2.9 Need for Smart Grid Security Guidelines at a European level

Operators were asked about the usefulness of creating a standard such as NISTIR 7628 at the European level and none gave a negative answer. They do believe that it is a good idea to use the efforts made in the US, improving and adapting it to the EU reality.

Operators from outside the electric sector believe that this type of guide would also be welcome for other industries.

1.3 Economic and financial factors

1.3.1 Economic impact of implementing Good Practices, Standards or Regulations

This concept included two different concepts that could be related based on an economic point of view.

The first concept was about the economic impact of implementing good practices, standards or regulatory obligations. Manufacturers, Security Tools and Services Providers, and Operators were asked with respect to their own businesses and under the umbrella of ICS security. On the other hand, public bodies and standardisation bodies were asked on how they consider these three categories of stakeholders face this issue.

Answers to these questions are summarised in the figure below:

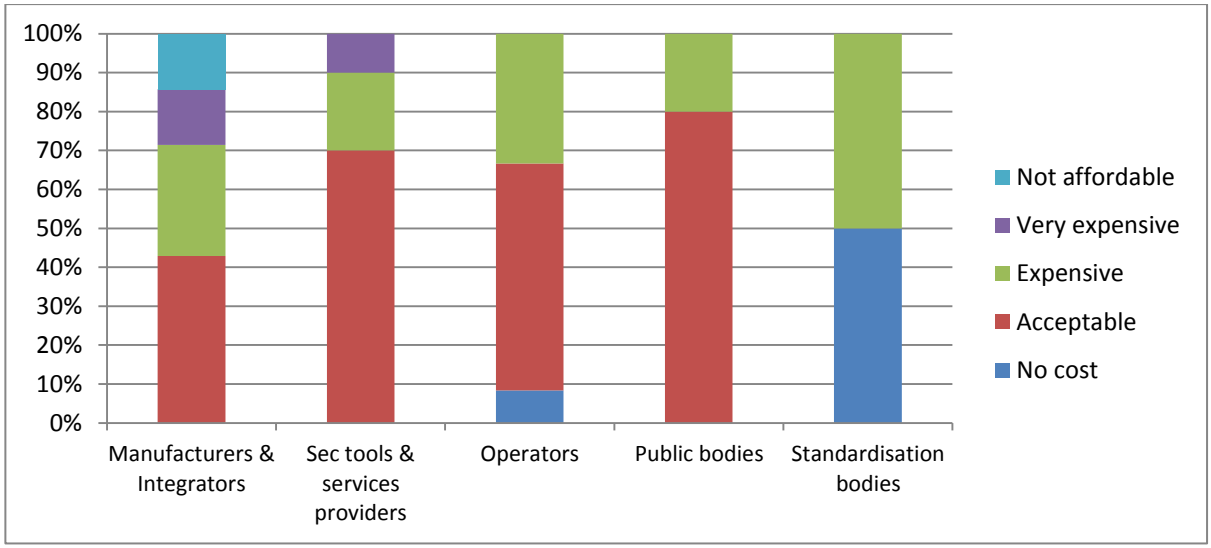

Figure 22 Economic impact of implementing good practices, standards or regulatory obligations

From the figure above, it can be concluded that:

- Manufacturers and integrators are the ones for which implementing standards, guidelines and regulatory documents is considered to be most expensive. Almost 30% consider it very expensive or even prohibitively expensive. Only 42% consider it acceptable.
- Most Security Tools and Service Providers (70%) consider those costs acceptable, even if some (less than a 10%) consider them very expensive.
- It is interesting to see that most Operators (68%) consider the cost more than acceptable, while the rest think it is just expensive. Based on the answers provided by experts, this could be explained by Operators' regular practices of putting new ICS

systems out to tender where security requirements are included together with other functional requirements. Vendors usually lower prices to win the contract and Operators get what they want at a reasonable cost.

- During the interviews, several experts from Public and Standardisation Bodies expressed the opinion that costs should be considered as acceptable as they represent "minimum requirements" that can result in money savings if considered as a part of the PDCA[8] cycle.

The second concept about which stakeholders were asked is on the degree of involvement of the Management staff of their own companies in addressing cyber security issues related to ICS security. An overview on the answers provided by the experts that participated in the survey is shown in the next figure.

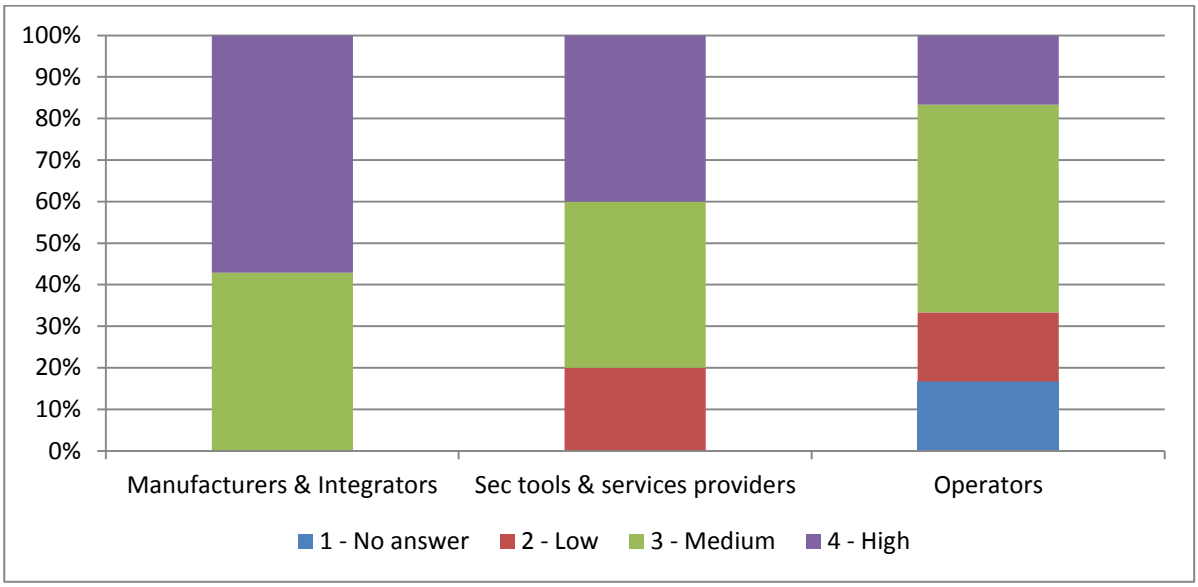

Figure 23 Degree of involvement of the Management staff on ICS security issues

From the figure above, it can be concluded that:

- There is a correlation between the involvement and cost. Stakeholders that rated the involvement of their Management on ICS cyber security issues higher are also the same ones that consider security more expensive.

- Manufacturers and Integrators managers are the ones most involved. 57% of interviewees considered that they are highly involved, while the rest rate this involvement as medium. There is a contrast between these answers and the

[8] *Plan-Do-Check-Act*

perception that many interviewees have about how security is implemented in ICS environments, in which devices are not designed taking into account security at the design phase. This might be because nowadays ICS vendors are in fact already considering security requirements at the design phase[9], or due to a disagreement on the necessary level of security perceived by different stakeholders.

- Security Tools and Services Providers have the impression that their Management is less involved with ICS security issues.
- And what is worse, less than the 20% of Operators consider that Management is highly involved. About a half of them rated this involvement as medium and some (15%) think that their involvement is low.

1.3.2 Participation in National or European funded programmes to develop security devices or architectures

When asked if they were participating in National or European funded programmes to develop security devices or architectures, the participants answered as follows.

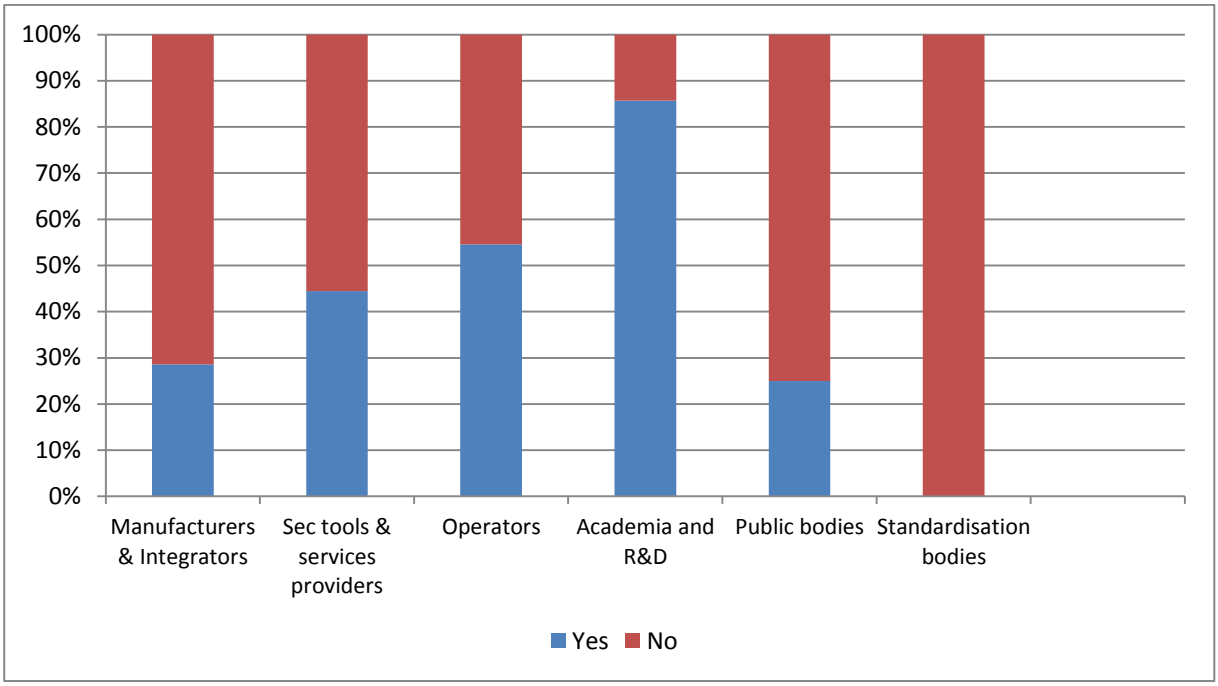

Figure 24 Participation in National or European funded programmes

- From a global point of view, there is a small majority of stakeholders (54%) involved in this kind of programme.

[9] *It is important to remember the issue about legacy components in ICS networks.*

- Comparing these results with the ones presented in section 1.3.1, we see that stakeholders that associate security with high costs are the ones that are less involved in this class of initiatives.
- Academia and R&D companies are the most involved stakeholder types in this kind of initiative.
- Surprisingly, Security Tools and Services Providers and, specially, Manufacturers are not very involved.
- When analysing the initiatives examples provided by the experts it could be concluded that:
    - Most of these initiatives were technical R&D focused, with a high impact from FP7 programme.
    - The few Manufacturers involved in funded programmes were always focused in the Smart Grids area.
    - Some programmes focusing on the development of Good Practices, and Education were mentioned. Especially the ones related with the CPNI in the UK and the Netherlands.
- Most experts from Manufacturers, Security Tools and Services Providers, and Operators expressed that these kinds of programmes are interesting, and necessary. However, a few of them considered that they are too theoretical (such as FP7). More practical programmes, such as test beds, and information sharing initiatives were demanded. A few of them think that this test bed should even be mandatory.
- Manufacturers were more reluctant to these kinds of programmes than any other group of experts:
    - Some of the respondents were not comfortable with the idea of public bodies getting involved in technical developments, even though public funding would help them develop technologies faster.
    - They consider themselves as having enough money and prefer not to ask for public funding. Thus avoiding having to deal with Governments asking them to include “backdoors” to bypass their security measures.
    - Moreover, they mentioned that Public Bodies’ role must be developing standards, guidelines, legislation and education.

1.3.3 Information for ICS Security programmes

Experts were asked whether they consider that there is enough information on public funded programmes. In the following figure it is shown that answers are equally divided between the "yes" and the "no".

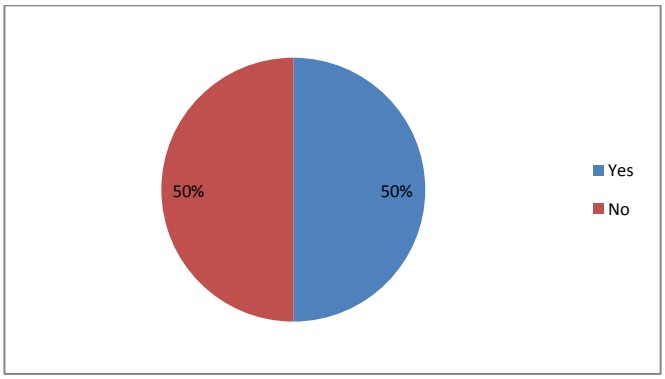

Figure 25 Stakeholders asked whether there is enough information on public funded security programmes

Half of the respondents were not aware of this kind of programs. When asked about how to improve it the following two proposals arose:

- Some experts think that a web-based resource including these kinds of initiatives will be helpful.
- Others think that some marketing effort to show programmes objectives and results would help increase their visibility.

1.3.4 Usefulness of Public Funded projects and initiatives and other related issues

ICS Security Products and Services providers were asked specifically about the usefulness of these programmes. A big majority, 80%, believed so, even if they expressed some criticisms and problems when asked further.

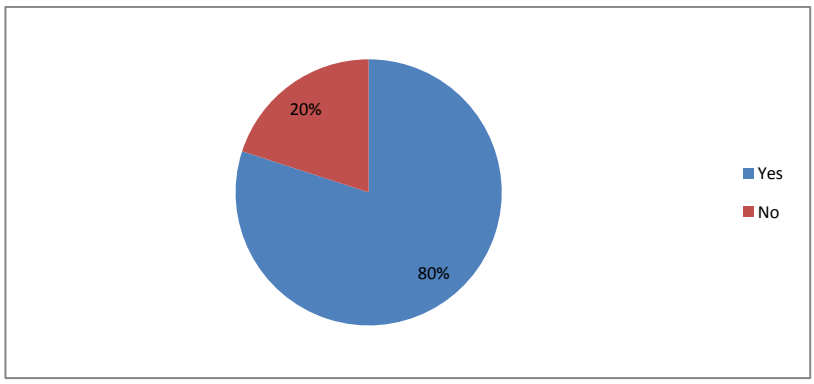

Figure 26 About the usefulness of public funded security initiatives

The main reasons to consider them useful were:

- The advantages of information sharing and collaboration amongst partners (i.e. acquiring and providing specific expertise and tools).
- The possibility of creating integrated solutions with a broader scope.
- They help raise awareness on specific issues.
- Public support can help long term R&D funding, which is not always a priority for companies, usually looking for short-term results.

But there were also several critics and proposals on how to improve:

- For a few experts, these programmes could be better articulated to take advantage of the results.
    - They need to be planned to solve concrete problems, but to do so participating companies should already have a profound knowledge of the achievable results or include an initial phase for such a study.
    - However, current programs do not usually allow for doing so. They lack the time or resources to acquire enough knowledge about the "state of the art".
    - Therefore, FP7 and similar (e.g. national level funding schemes) should be supported with more funding to make long term research activities for private companies more attractive.
    - Moreover, projects should be more flexible in terms of deadlines and objectives, since R&D can lead you through very different paths to what was initially planned.
- There has not been much interest in ICS security during recent years. There is normally more interest in "embryonic" areas.
- A few experts believe that security products should not be made for the public. Therefore, there is still a debate in this area about the security-through-obscurity approach.

On the other hand, Public Bodies were asked about the upcoming new funding initiatives being planned by the public sector to improve protection, resiliency and security capabilities of ICS behind Critical Infrastructure. The few answers received stated that they are normally part of public-private initiatives and sometimes in cooperation with non-EU states.

An interesting case to point out here was the one in which initiatives in the security field can also be done with no public funding, on a voluntary basis, where private companies participate for other reasons, such as Market positioning. This was the case of the new regulatory schema for CI protection in Spain. In this case, the representatives of the private sector work collaboratively on a voluntary basis to develop reference security plans for CIs. A public body is the driving factor (i.e. facilitator and instigator).

1.3.5 Public-private cooperation for Operators

Operators were asked if public organisms should help privately owned companies by means of public funded programmes to improve the security of their ICS. A large majority of respondents (91%) agreed saying "yes".

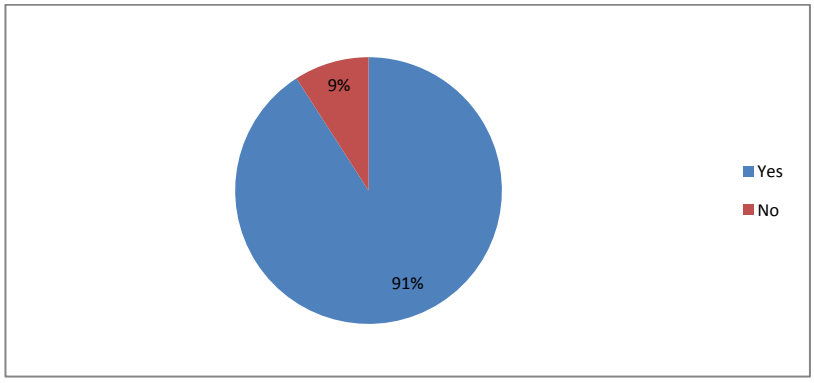

Figure 27 Operators point of view with regard to the necessity of public bodies to help them improve ICS security by means of public funded programmes

The main reasons they gave to support this opinion are:

- Those are matters of public interest. Independent of ownership, governments should help companies and not only ask them to carry out their ICS protection duties.
- Governments have strategic and economic interests in ICS-CI. Private companies have an economic interest, which is also related to reputation and trustworthiness. So, even if they have different perspectives they also share objectives.
- Without a public body acting as a facilitator it is unlikely that companies will work together. In fact, various operators working under UK-CPNI influence consider this an example of success.

1.4 Technical

1.4.1 Current and future threats in ICS protection

All stakeholders were asked about their opinion on the current trends in the threat environment of Industrial Control Systems and what would they be in the future. There was a variety of answers for the current panorama, but most experts pointed out at least one of the following current trends:

- Virus and malware. The Stuxnet case[10] has drawn lots of attention.
- An increasing interest in hacking ICS systems by potential attackers.
- Low interest in security or the (wrong) feeling that their systems are secure enough by those responsible.
- Practical difficulties in patching and vulnerability management.
- Human errors. From configuration mistakes to wrong device uses.

When asked about the threats coming up in the near future, experts have emphasized:

- External targeted attacks. Respondents think that the attacks against ICS systems will occur more often with terrorists, enemy countries or hacking-for-profit backed by criminal organizations. A few stated that it might even be used to generate mistrust within competitors, as sabotage or business war.
- Internal threats. Just disgruntled employees or malicious staff members or contractors motivated by any of the reasons mentioned above.
- More difficulties in vulnerability management, as a consequence of distributed intelligence, virtualization, public networks and cloud computing.
- Privacy issues specially related with Smart Grid capabilities and privacy laws in the EU.

Then experts were asked about which of those threat trends, both present and future, are the most challenging ones. They stated:

- Targeted attacks are considered the biggest problem, because they are difficult to predict, and can be tailored to harm an organization.

[10] *Some experts defined it as a "Military Project" more than a virus.*

- Legacy equipment. As ICS systems have a very long lifecycle, during the years it would be more complicated to manage their vulnerabilities, or cover security needs.
- Human factor. Targeted attacks might take advantage of this. It is really challenging to build and design systems to avoid human errors (e.g. involuntary infections). For example, USB removable storage devices were specifically pointed out many times during the interviews.

Manufacturers & Integrators, ICS Security Tools and Services Providers, and Operators were asked about the more probable logical and physical threats and to rate the degree of impact of these threats. Considering 1 as low impact, 2 as medium, 3 as high and 4 as critical, the average impact of the most common answers is displayed in Figure 28.

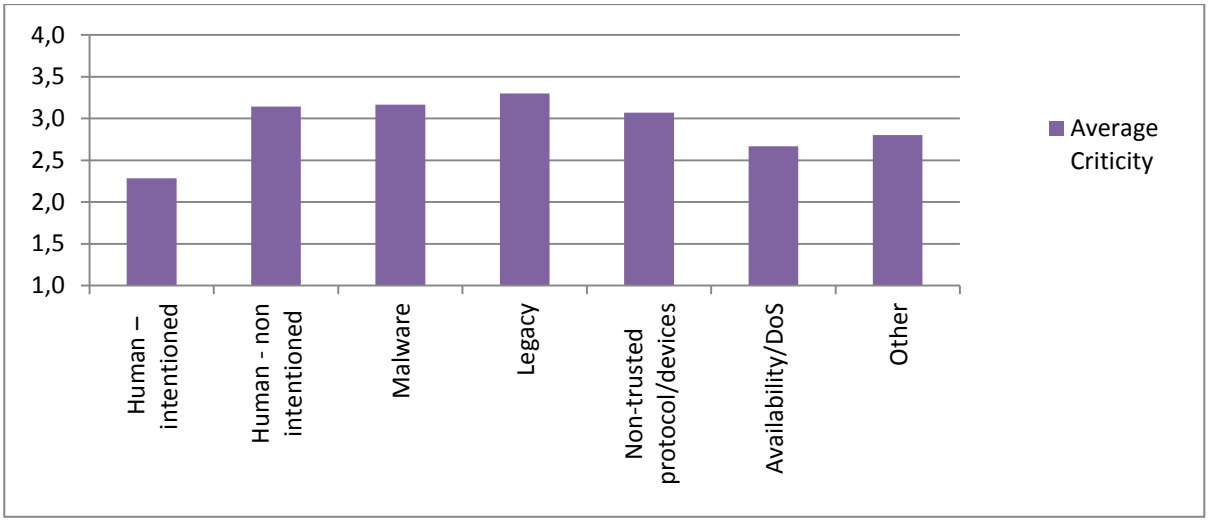

Figure 28 Impact of the most relevant threats identified by the respondents

From this figure, and also considering each stakeholder's answers, it is possible to interpret that:

- Security Tools and Service Providers consider several menaces regarding communications (such as those deriving from the use of wireless technology, Internet connections, etc) as critical. On a second level they think that access control to applications and equipment are important.
- Operators consider threats against availability as the most important ones, including device or communication manipulation. They are also the most concerned about the "human factor" threat, highlighting accidental errors or malicious activity.
- Most manufacturers consider as a critical threat the existence of insecure equipment (legacy or just untrustworthy because of backdoors and similar) in secure networks, as

well as non reliable (often proprietary) protocols. There are experts who are afraid that firmware backdoors that can bypass all security software protections are already being included into new embedded devices and ICS software.

- Additionally, during the interviews several specialists specifically highlighted their concerns about the security issues originating in insecure equipment. Some of the most interesting comments made by the experts were:
    - During years isolation was considered as a security layer, but this is no longer true as remote control technologies evolve.
    - This has advantages for control, patching and update, but it may lead to security flaws.
    - There are backdoors in this equipment. Some promoted by governments, some because of vendors.
    - The security-by-obscurity approach was brought back again at this point, with experts claiming for transparency.
    - Several experts stated that built-in security in those devices would be good, but this implies reducing the expected lifecycle of current networks which might be too expensive.
    - Compensating security flaws with a multi-layer security approach, and assuming that some components will change is the current method.
    - An expert also stated the need for Memory Foot Prints, already existent in some Smart Grid devices, during the whole device lifecycle to take better decisions.

1.4.2 Future research lines in ICS Security

Academia, Public Bodies and Standardisation Bodies were asked about future research lines to improve the different aspects of ICS security. Some of the experts also mentioned current research lines which in fact enriched the question.

In fact, regarding tools and technologies for ICS security they are currently working on, the experts signalled:

- New testing methodologies and tools for system interdependencies
- New security and functionality metrics

- Better access controls for devices
- Security in Wireless networks[11]
- Vulnerability analysis
- Intrusion Detection Systems
- Study and test performance of current Smart Grid installations
- Smart Grid standards and effectiveness measures.

Regarding the trends of future research in ICS security, the more common ones were:

- More robust and flexible architectures.
- Early anomaly detection by means of Network Behaviour Analysis and Security Information and Event Management systems.
- Contextualisation: correlation between security data and business-processes data
- Patching and updating equipment without service disruption.
- Tools and methodologies to integrate and manage logical and physical threats.

1.4.3 Challenges of ICS security to classic ICT security

As ICT technologies presence in the ICS world increases, new challenges appear. Stakeholders were asked about the most challenging issues when bringing cyber security capabilities and adapting regular ICT security products to the control systems world. The most relevant challenges are summarized below:

- The security culture differences between the two worlds. ICT security has always been studied as Confidentiality-Integrity-Availability, while in ICS priorities are Safety-Reliability-Availability. This has deep implications, and as a result conventional ICT security products cannot be directly applied to ICS networks without a proper understanding of these differences. Many experts believe that this issue needs to be rethought and some point to Academia researchers as the ones who can provide solutions. Some examples of these implications were given by experts, affecting to different processes:

[11] *In section 1.4.4 there is additional information about the real adoption by these technologies.*

- The difficulties of making an ICT technician understand that a true 24*7 ICS device can never stop. Not even for Risk Analysis, updates, or penetration tests.
- The dramatic consequences that excessive traffic or regular fingerprinting practices (e.g. TCP/UDP port fingerprinting) can have in an ICS Network.
- ICS security staff are not always aware of security risks and practices in the ICT world.
- ICT security vendors try to get into the ICS market without understanding the differences.
- Some ICS technologies are not covered by ICT security products, such as specific protocols or systems.
- Each world has its own standards (ISO 2700X versus ISA 99x and IEC 62443).

- Another relevant issue that was mentioned once again is that current ICS components will remain operative for, at least, another decade, so the only way to improve security is to go for a multi-layer security approach. In any case, several experts also stated that new products are becoming more prepared for security and this will improve in the near future.

1.4.4 Security technologies in use or to be implemented

ICS Security Tools and Service Providers were asked about the security products and technologies that industrial customers were asking for. At the same time, Operators were asked about the products and technologies that they were planning to buy in the near term. Moreover, Academia was asked about which security technology would be urgent to implement in order to reduce current risks for ICS. A closed set of technologies was provided.

The following figure shows an aggregated summary of the different solutions that represents the most popular technologies today for ICS protection.

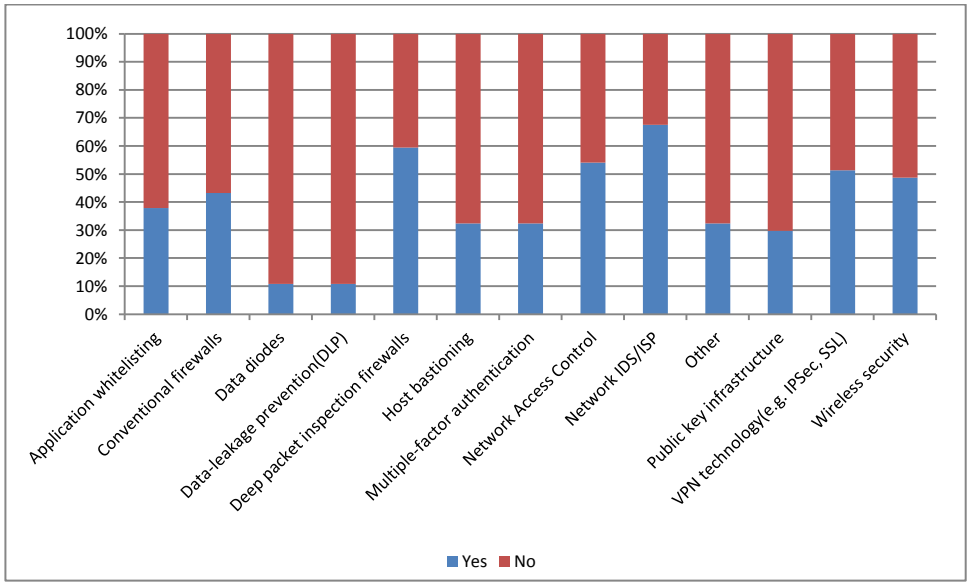

Figure 29 Popular technologies for ICS protection

As seen in Figure 29:

- IDS/IPS are the most popular ones (68%), followed closely by specific DPI (59%), NAC (53%) and VPN (51%)
- On a second level we find wireless security (48%), conventional firewalls (42%), Application whitelisting (38%), host bastioning (hardening) and multi-factor authentication (both 32%) or PKI (29%).
- Some technologies that have not had success yet are Data Diodes and DLP (10%)
- 32% of respondents signalled other technologies, mostly antivirus, special DNS, Network Behaviour Analysis or Security Information and Event Management.

If we compare the answers from each stakeholder, some interesting information can be inferred, particularly when we compare the technologies which operators are planning to acquire in the near term with respect to those technologies that are actually being demanded from ICS Security Tools and Services Providers (see Figure 30):

- Operators are not implementing or planning to use the technologies that ICS Security Operators and Providers claim to be demanded.
- This is especially evident in cases such as multi-factor authentication or DLP, in which they have no interest at all.

- Moreover, wireless security seems to be very important for Security Tools and Service Providers and Academia, but Operators are not using or planning to use it in the near future.
- DPI firewalls are not as often installed as Security Tools and Service Providers and Academia think they should be. On the other hand, conventional firewalls are very present.
- IDS/IPS is still considered the most interesting technology, and VPN also has a good level of agreement.

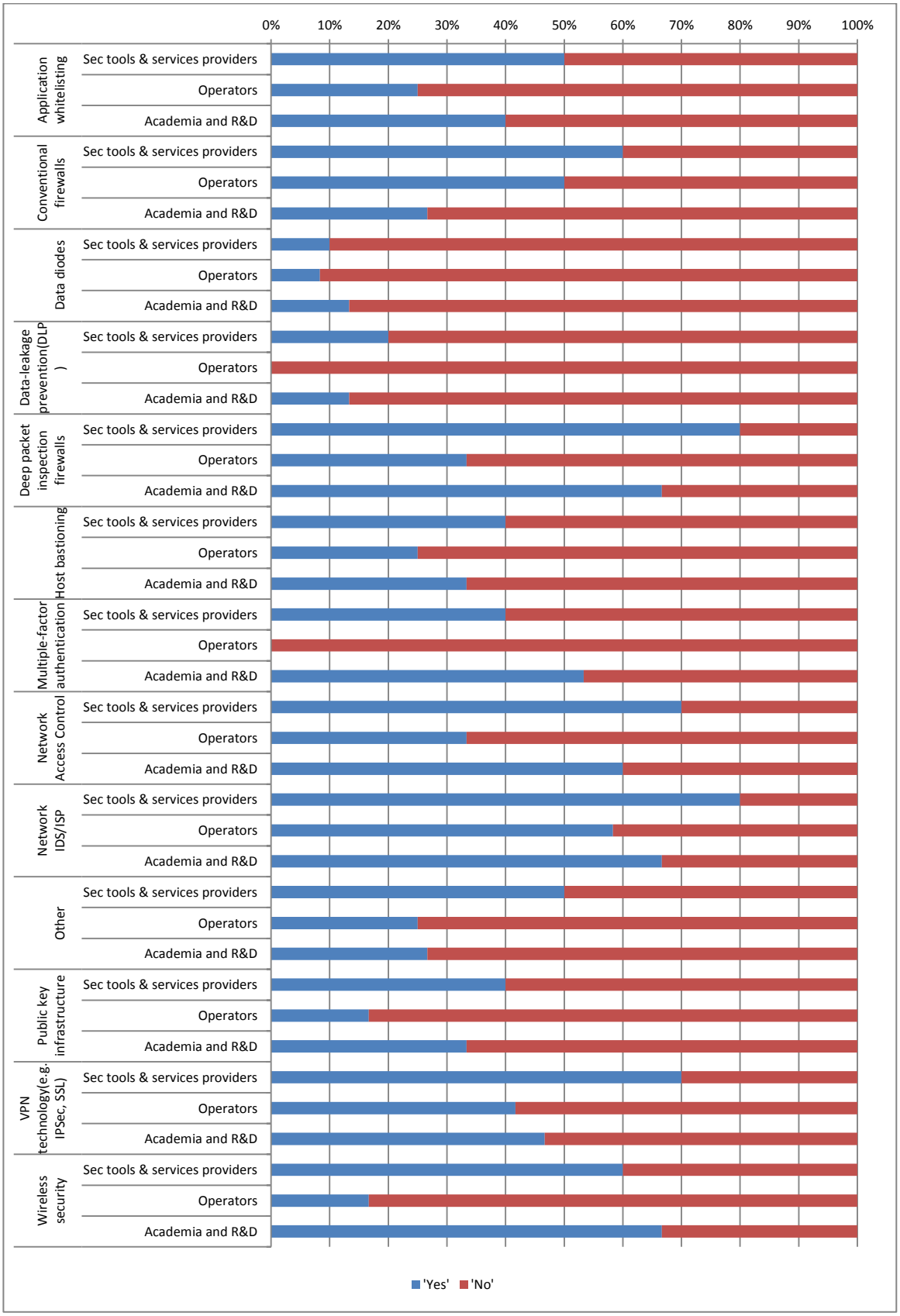
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Application whitelisting
Conventional firewalls
Data diodes
Data-leakage prevention(DLP)
Deep packet inspection firewalls
Host bastioning
Multiple-factor authentication
Network Access Control
Network IDS/ISP
Other
Public key infrastructure
VPN technology(e.g. IPSec, SSL)
Wireless security
Sec tools & services providers
Operators
Academia and R&D
'Yes'
'No'

Figure 30 Technologies being demanded, offered or recommended by Stakeholder type

1.4.5 Cyber security built-in in ICS products

Manufacturers were asked if their clients asked them to include cyber security capabilities in their ICS products. At the same time Operators were asked if they are asking their providers to include cyber security mechanisms in control systems' devices and applications. As seen in figure 23, the answers on both sides are coherent, showing that this is the case in about 75% of cases.

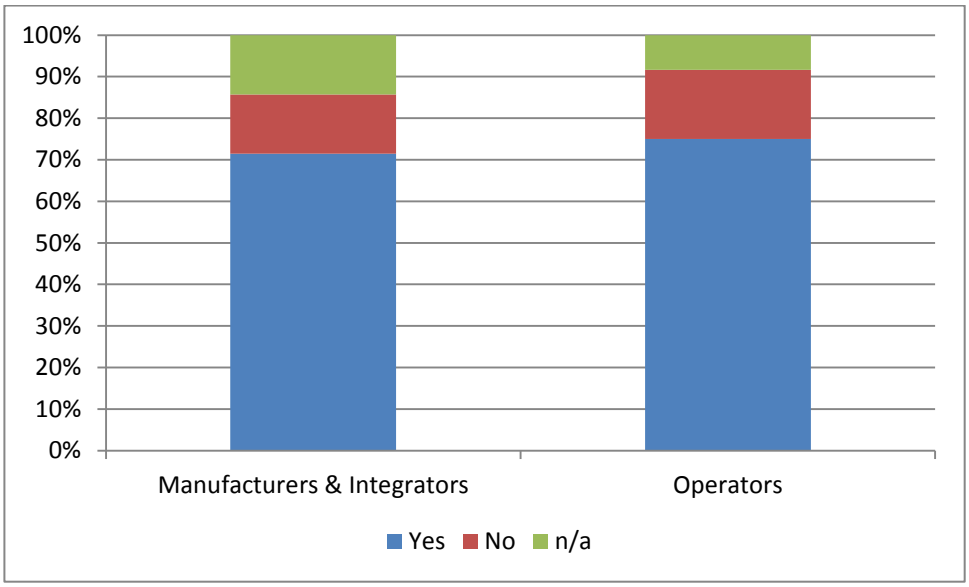

Figure 31 About the demand/offer of cyber security capabilities in ICS components

Both stakeholder types were also asked to provide examples on this issue. As a result, the most frequently implemented security functionalities were cryptographic keys (including PKIs) and firmware upgrades by digitally signed patches. In terms of desirable technologies, intrusion prevention and anti-malware capabilities are at the top. During the interviews, several experts explained that this is considered a "plus", but if this increases the price too much the option is rejected.

In a different but related question, manufacturers and integrators were asked about the cyber security capabilities they are currently providing in their devices and applications. At the same time, ICS Security Tools and Services Providers were asked if their products were already including specific cyber security functionality or capabilities for ICS. According to the answers, Manufacturers usually provide encryption solutions (at communication or user/pass storage level), built-in firewalls, redundancy or hardened OS. It is important to state that 15% of manufacturers still do not provide any kind of functionalities. On the other hand, Security Tools and Service Providers business is focusing on providing security on legacy systems or solutions which are not being addressed by manufacturers directly, like encryption of legacy

control protocols (e.g. VPN), transparent IDS/IPS, Deep Packet Inspection (DPI) for control systems protocols, and virtualization.

1.4.6 Cooperation in developing methodologies and tools for risk or vulnerability analysis

Organisations such as Security Tools and Service Providers, Academia and Public Bodies were asked if they have developed or fostered new methodologies or tools to analyze risks and vulnerabilities.

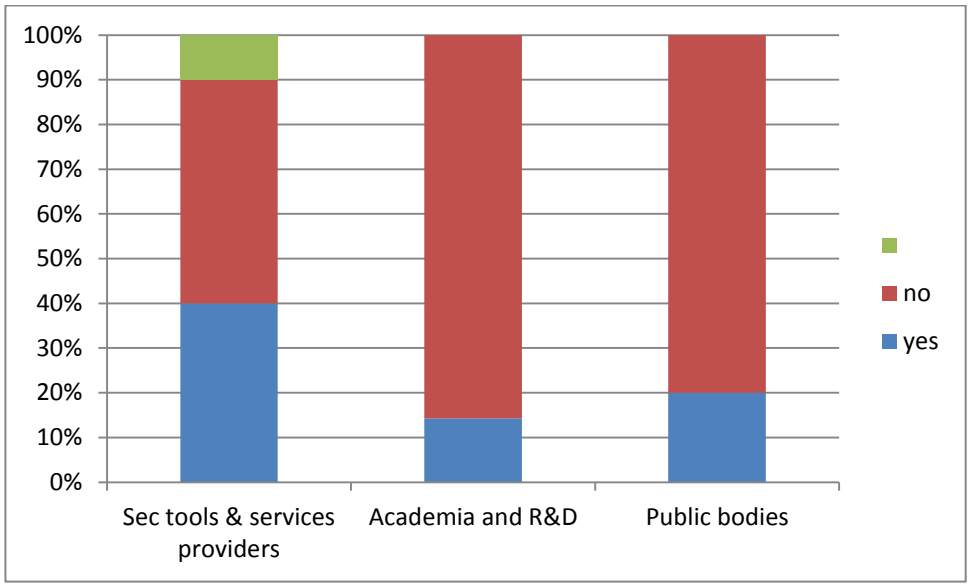

Figure 32 Development of novel risk and vulnerability analysis methodologies and tools

As can be seen in Figure 32 only a minority group of them have participated in such activities. Security Tools and Service Providers are the ones most involved in these tasks (40%) while Public Bodies (20%) and Academia (15%) do not participate in them very often.

It is interesting to contrast these results with those in section 1.1.10 where operators mention that they are currently undertaking risk analysis or even other projects resulting from a previous risk analysis phase. Even if there are companies that might have performed risk and vulnerability analysis using new tools and methodologies it is also possible that many others are using regular ICT ones, which are not optimal for ICS environments. Moreover, it is also interesting to highlight that risk analysis appears as one of the most demanded/desirable security services for ICS, as can be seen in section 1.4.7.

1.4.7 ICS security services status

Operators and Security Tools and Service Providers were asked about the most demanded security services in ICS. At the same time, Academia and Public Bodies were asked to give their impression about the ones that they consider more desirable.

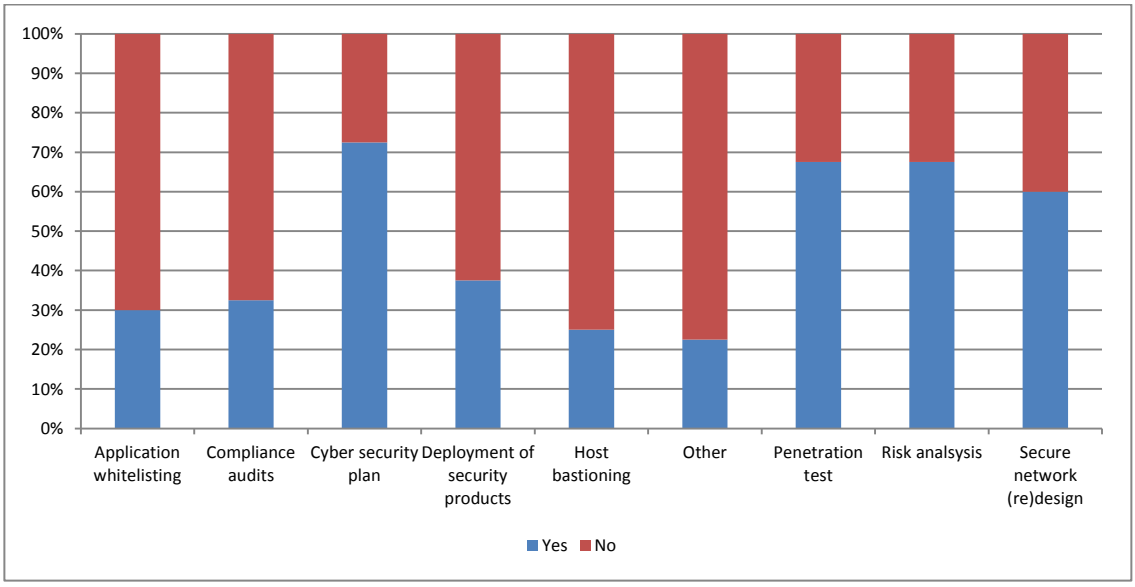

Figure 33: Most demanded and desirable ICS security services

As seen in Figure 33,

- Cyber Security plans (72%), Penetration Test and Risk Analysis (68%) and Secure Network Design (60%) are at the top.
- There is a big difference with respect to all other proposals, such as deployment of security products (38%), compliance audits (32%), application whitelisting (30%) or host bastioning/hardening (24%).

There were few significant discrepancies between stakeholder types as seen in Figure 34. Just Security Tools and Service Providers thought that compliance audits are very much in demand compared to other stakeholder perception (70% to 20%) and something similar happens when referred to the deployment of security products.

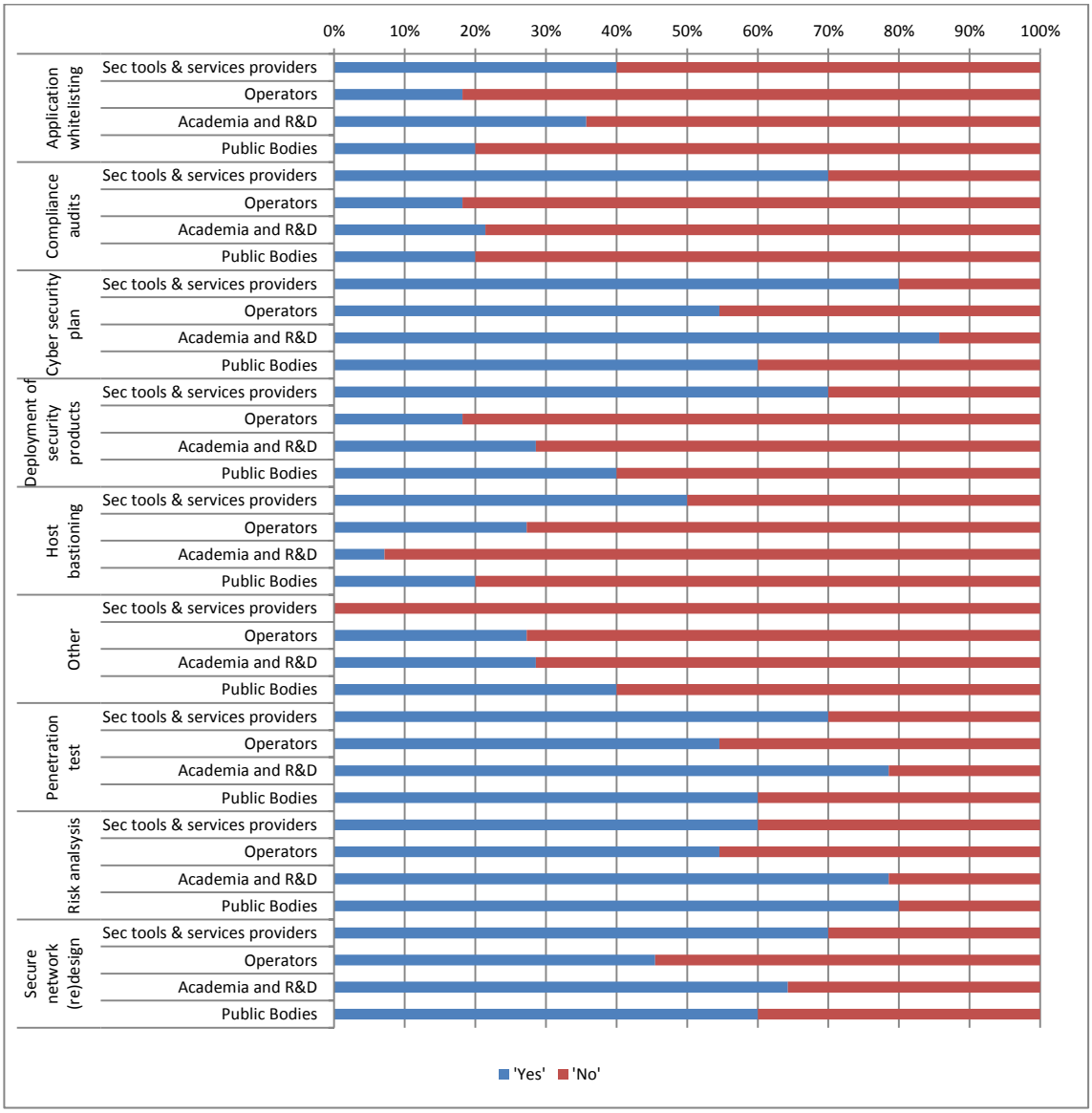

Figure 34 Most demanded and desirable ICS security services by stakeholder type

This information was compared with the real status of activity. In Figure 35 the services currently being provided by Security Tools and Service Providers are represented and in Figure 36 the ones that have been contracted by operators.

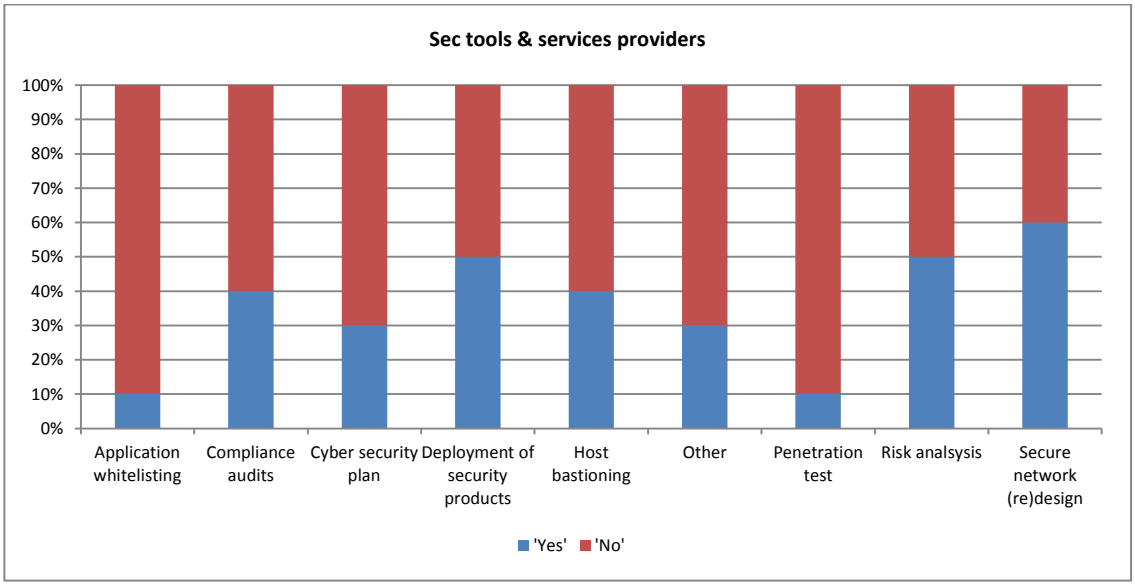

Figure 35: ICS security services currently provided by Security Tools and Service Providers

From those results one could conclude that:

- Operators might not actually be making use of those services that ICS Security Tools and Service Providers are claiming they are buying.
- Operators might be trusting Manufacturers for including cyber security in their ICS systems. In turn, Manufacturers would be the ones actually demanding those services from third-party companies like ICS Security Tools and Services Providers.
- Just Penetration Testing (35%) and Secure Network Design (27%) are visible to Operators. This means that Operators are directly buying these services from ICS Security Tools and Services Providers.
- Network (re)design figures match in both cases. However, Penetration testing is claimed by Operators to be one of the most demanded services, while ICS Security Tools and Services Providers consider this service as one of the less demanded ones together with application whitelisting.
- This discrepancy might be due to the fact that penetration testing could be currently done by regular ICT security companies which are not providing specific ICS security services and which are not participating in this Study.

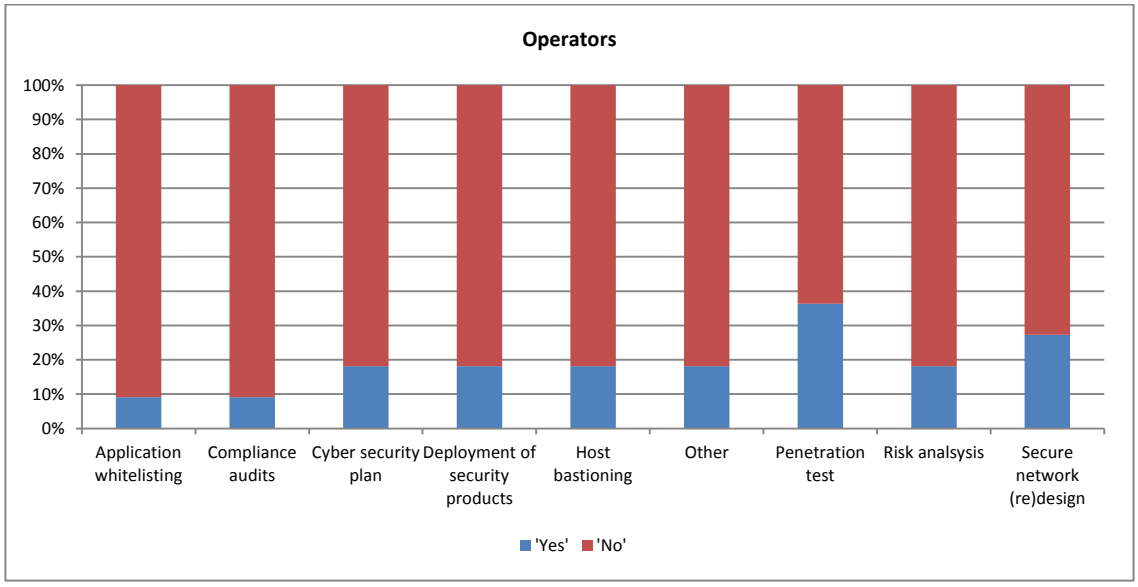

Figure 36: ICS security services actually demanded by Operators

1.4.8 Smart Grid technical challenges and other issues

Stakeholders were asked about their involvement in Smart Grid security and the issues they considered more challenging. The three main issues described were:

- The size of the networks, including the amount of assets, data, nodes or controls required may be overwhelming. For example, the quantity of smart meters may reach millions, and they all provide lots and detailed information about the customers. To track all this information is the biggest challenge.
- End customer confidentiality and the problems derived from privacy laws. Theoretically, just the operator and the consumer should have access to this information. Should meter readings be considered personal data?
- Trustworthiness of transmission channels, as operators rely on third parties to operate.

Security Tools and Service Providers were also questioned about their services and solutions in the field of Smart Grid security. They claimed that they are already providing solutions regarding device authentication and encrypted communications between different elements such as data concentrators and smart meters.

On the other hand, experts from Academia and R&D were asked about their interest in and projects regarding the security of the Smart Grid. The general impression is that they are already getting familiar or working in Smart Grid topics. Some of these topics include market

research or technical aspects like cyber security by design, training programs and security testing methodologies for these environments.

1.4.9 Dependencies of ICS with third party telecommunication infrastructures.

All stakeholders were asked about the implications of ICS relying on third party communication infrastructures from a cyber security point of view. They all admitted that interdependencies exist, and that this may lead to security failures in ICS. They emphasized:

- Operators' lack of control and knowledge over the status of the network. Operators cannot identify, neither solve any problem without the collaboration of the telecommunication service provider.
- Public and private channels may be multiplexed over the same physical segments. Many coincide to require encryption and signatures to prevent information leaks.

However, a few respondents also provided a positive analysis. They stated that it might actually be beneficial for operators to rely on specialized companies for this kind of services letting the operators focus on their core business. Moreover, this situation might also make operators consider security and important issue since they will have to secure the information being transmitted over third-party networks, either addressing this on their own or by putting pressure onto telecommunication companies to get a secure service.

1.4.10 About cloud computing in the ICS environment

During the interviews, several experts were asked their opinion on the cloud computing paradigm and its applicability in ICS networks.

- Many stated that this could be promising in some aspects, such as to improve computational capacity of ICS systems.
- However, the majority stated that cloud computing is still too immature or even not a valid paradigm when considering stringent QoS aspects and real time operation of ICS. They stated that Cloud Computing services are designed for IT networks and ICS has other needs.
- Even for valid use cases, some experts warned that every detail must be crystal clear in the contract. One of them said that standardized requirements at a European level would foster the adoption of these technologies.

1.5 Dissemination and awareness

1.5.1 Knowledge about and participation in forums or workgroups concerning cyber security in ICS environments

All experts were asked if they knew any forums or work groups concerned with cyber security aspects in Industrial Control Systems and if their organisation participated in them.

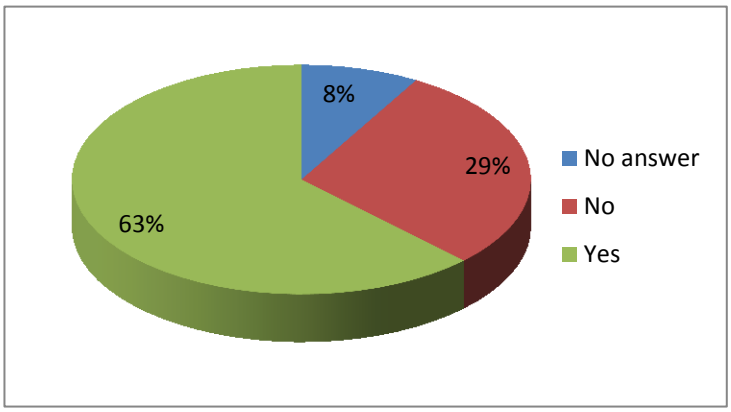

Figure 37: Percentage of stakeholders that are aware of forums and/or workgroups on ICS security.

As seen in Figure 37, a majority (63%) of participants are aware of some initiative of this kind.

Taking a look at Figure 38 in which the results are split by stakeholder type the most aware stakeholders are Academia (85%) and Public Bodies (75%). Security Tools and Service Providers (70%) and Manufacturers (60%) are also informed. It is interesting that only 50% of operators are aware of this kind of initiative. Standardization bodies are not statistically significant, as there was only one answer to this topic.

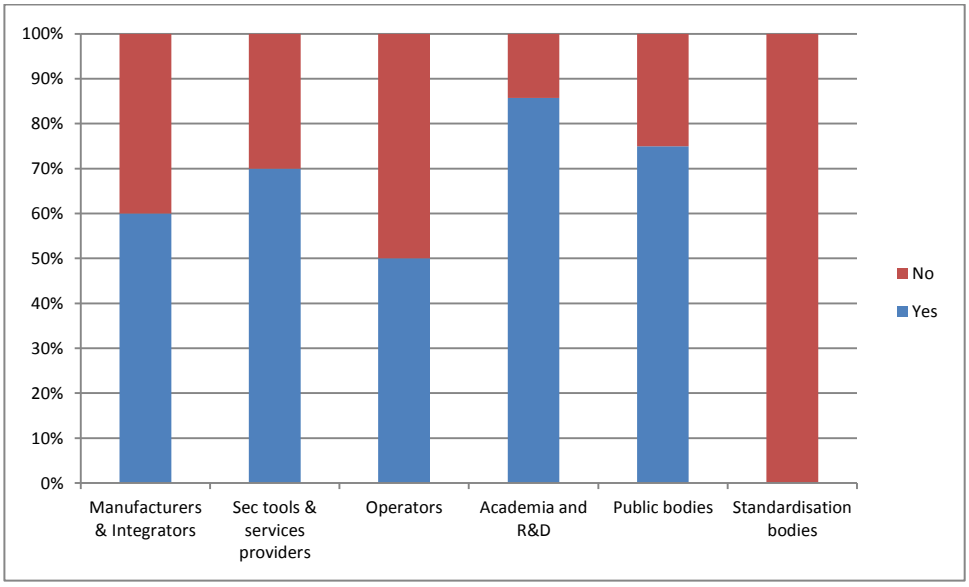

Figure 38: Percentage of stakeholders that are aware of forums and/or workgroups on ICS security by type.

Participants were then asked if they were actively taking part on any of them.

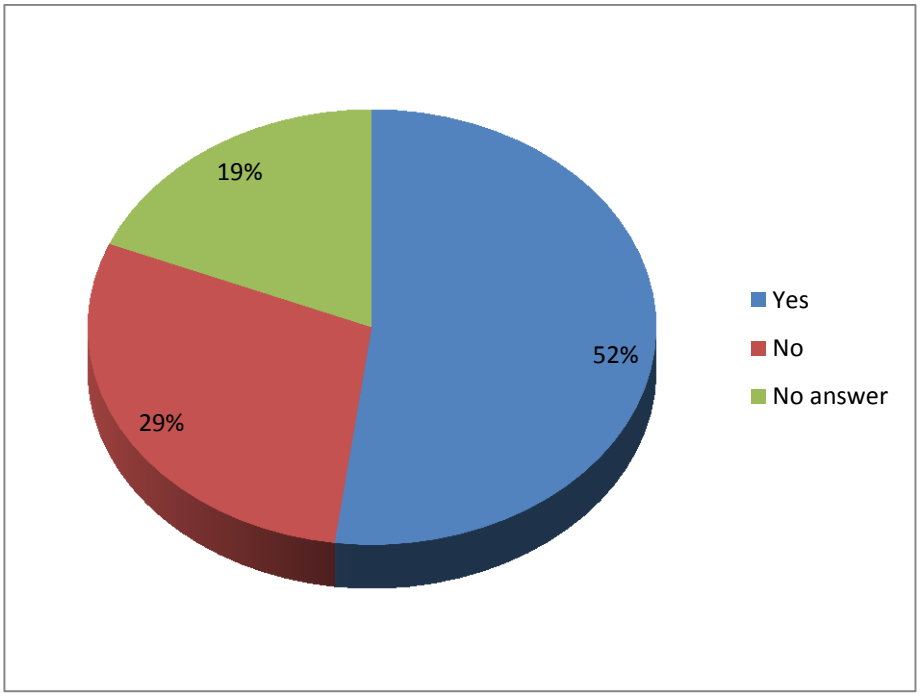

Figure 39: Percentage of stakeholders participating in forums or workgroups on ICS security.

As seen on Figure 39 the participation rate is very high (52%) when compared to the data shown in Figure 37. It means that the 82% of organizations that are aware of this kind of initiatives are actively working on them.

These results are even more illustrative when checking stakeholders separately:

- All Operators and Academia organisms, and a high majority of Security Tools and Service Providers (95%) that are aware of these initiatives are actually cooperating on them.
- This is not the case for Manufacturers (66%) and Academia 66%) and Public Bodies (33%). This may represent a lack of interest, or just that the initiatives they are aware of are not appropriate for them.

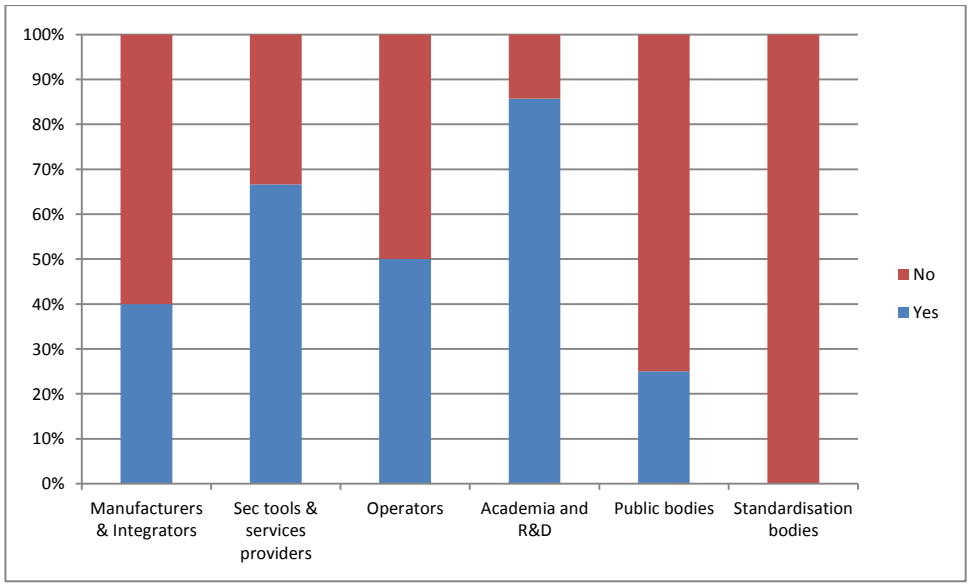

Figure 40: Percentage of participation in initiatives by Stakeholder type

1.5.2 Evaluation of the forums and work groups in which stakeholders are actively participating

Only respondents that were actually working in forums and work groups on ICS security were asked to rate them according to one of the following options:

- *Indifference:* Something that is obsolete or without interest.
- *Overlapping:* The work done in this group overlaps with others.
- *Active:* This group is working hard but not much on cyber security issues.
- *Interesting:* This group is focused on actual cyber security risks and challenges.

As seen in Figure 41:

- Respondents rated most groups/forums as interesting (78% of the groups/forums). Some of the most repeated ones have been SANS EU SCADA, E-SCSIE, ESCoRTS and diverse initiatives from ENISA, NIST, CPNI.UK and CPNI.NL.
- 16% of the groups/forums were rated as active groups.
- The number of groups that are considered overlapping is very small (2 groups, 4%). They were ISA-99 (which was also rated as "interesting" by others) and Linked-In PCS Security.
- There was just one group (2%) rated as without interest or obsolete by one respondent: AMETIC.
- During the interviews some respondents expressed the opinion that this kind of initiative should also exist divided by business more than by technology.

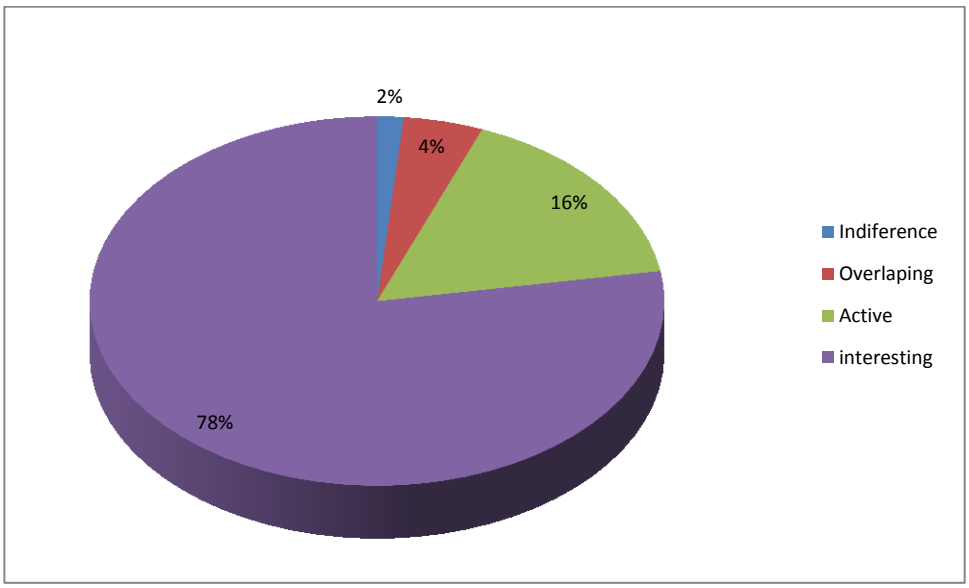

Figure 41: Evaluation of forums and working groups.

1.5.3 About the number and quality of dissemination events on ICS security

Experts from Academia and from Security Tools and Service Providers believe that there should be more events (i.e. conferences, workshops, webinars, and similar) targeting dissemination of research results, products and solutions as well as raising awareness on cyber security aspects of Industrial Control Systems.

Security Tools and Services Providers suggest having specific events focusing on existing standards of ICS security, to disseminate their content and raise end user awareness. They

also consider that many of these events have a low quality level since the quality of the content presented is very poor.

Academia and R&D believe that current events are too theoretical and do not have enough participation from manufacturers and integrators. Researchers believe that at this present time there are many security-related events, but on general security problems, and with presentations being repeated from meeting to meeting. Some consider that it would be important that each event focused on a particular problem and try to find practical solutions amongst them all.

It is also interesting to highlight here some of the opinions from Academia that arose during the interviews. They considered 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. Academia needs to have papers published somewhere in order to improve the curriculum and reviewers are not tough or even professional. Some conferences ask to submit papers already accepted in other conferences and will be accepted with no further analysis. It is easy to fool them (they are in need of publications). The same happens with journals. It was also stated that, for instance, Microsoft is ranking journals and conferences as a way to correct this. It was suggested that there should be consensus on the convenience of continuing to publish in conferences and journals that have made business out of low quality papers/articles.

1.5.4 About the participation in ICS security dissemination events on ICS security

Manufactures and Integrators, ICS Security Tools and Services Providers and Academia were asked if they usually give conferences, webinars or perform any other dissemination action to disseminate their ICS security solutions or work. At the same time, Operators and Public bodies were asked if they attend these events.

An overview of the answers provided by the respondents is shown in Figure 42.

Based on the results, we can assure that:

- Manufacturers, Security Tools and Services Providers, and Operators are very active in these kind of initiatives (Security Tools and Service Providers have a 70% of positive responses; additionally, a 67% for Operators and 58% for Manufacturers)
- Operators also indicate that they regularly attend presentations given by Security Tools and Service Providers and Manufacturers.
- Public Bodies are also present with a 40% of participation.
- However, operators and public bodies' staff state that they attend general events more often, which are lately more related to Smart Grids.

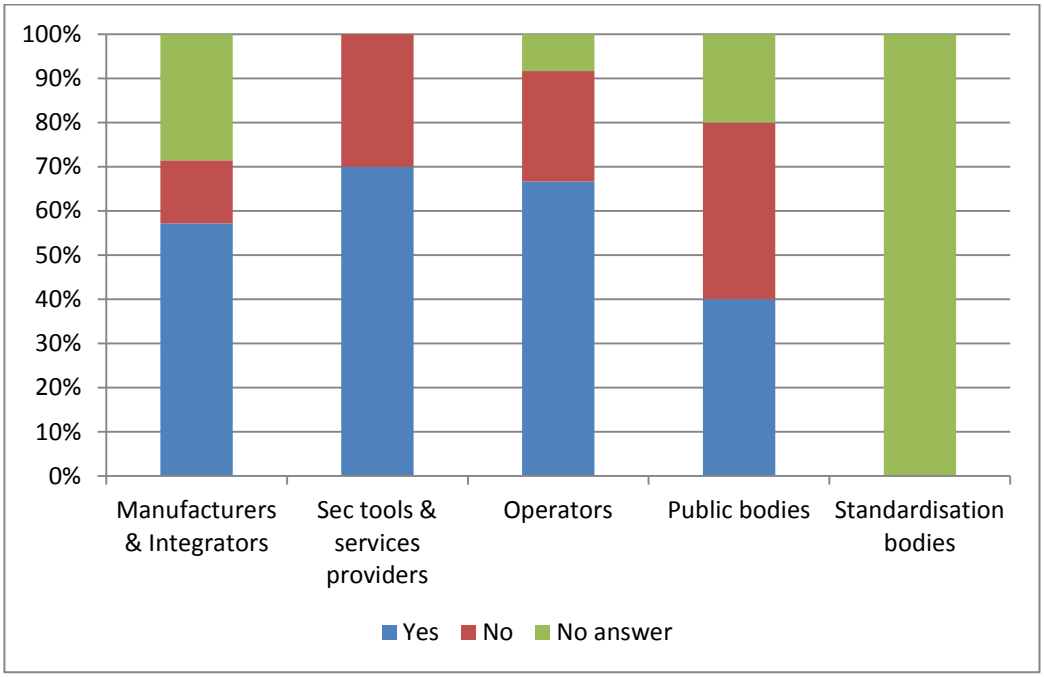

Figure 42: Participation in ICS security events

Additionally, Experts were questioned about how necessary the presence of the different actors in dissemination events is as well as on the difficulty of finding information about security products and services specifically designed for ICS at such events.

The most interesting issues discovered are that:

- Manufacturers do not think that Security Tools and Service Providers are very necessary (just 29% support it, and there is another 29% that do not answer). The others think that they could provide interesting real cases, but it would not be likely that their customers will accept being described as “victims”.
- 100% of researchers interviewed believe that it is necessary to improve relations between research and operators.
- Some Operators consider that they do not have problems finding information about the equipment and security solutions they need, but they miss independent evaluations and specific tests performed in real ICS environments.
- All interviewed stakeholders indicate that the issue of cyber security appears in all the events they attend, but not as a main issue, although it is increasingly important.
- However, cyber security is treated in a general way not addressing specific aspects of ICS.

1.5.5 Knowledge about the Smart Grid concept

Most participants were asked about their knowledge of Smart Grid technology and its security issues. Based on the results we can state that in general they can be considered to be familiar with it, or even experts:

- Many of the respondents said that Smart Grid security will be something to consider in the future, but currently there are not too many funding programmes addressing this issue.
- Some researchers have published several reports on security in Smart Grids and in components that comprise it, but they still think that the maturity level of security solutions available for this environment is low.
- Security Tools and Service Providers have been working on projects or have done research on Smart Grids. Some of the solutions discussed are generic and are not specifically developed for industrial networks. Some others are specific solutions for Smart Grid that mainly focus on the communications protocols.
- Most Academia respondents are, or have been, working in technical research.
- Just one Public Body declared to be related to smart grids, collaborating with energy companies to develop tests focusing on security and flexibility aspects of the solutions.

1.5.6 Other dissemination aspects: ICS-CERT

During the interviews, several other topics related to dissemination aspects were discussed. However, the way in which ICS vulnerabilities are discovered and disseminated in Europe was a main topic. Actually, experts were asked about the suitability of creating an ICS-CERT at European level:

- Almost all participants supported the idea.
- Private organizations are already doing this kind of work on their own.
- Network of Trust: It is important to classify and provide guidelines, but not to expose real systems.
- UK CPNI has made good progress in this, as well as other country CERTs. There are experiences of private labs in other countries (INL, Sandia…) that are also helpful.
- European ICS CERT should be a PPP and have peers in other continents or countries.

- Some consider ENISA should promote it or even support it if they have the resources (something like an Interpol) and define a reference standard to deal with vulnerabilities.
- Some experts think that those CERTs should focus on industry sectors instead of focusing on horizontal aspects like cyber security only. Each sector's needs are different, crisis management is also different, and it will be easier to involve Operators' Top Management since it will be easier to show the business orientation.

2 References

1. **European Network and Informations Security Agency (ENISA).** *EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection.* [Online] 2010. 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.

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

3. **Boyer, Stuart A.** *SCADA: Supervisory Control and Data Acquisition.* Iliad Development Inc., ISA. 2010.

4. **Institute of Electrical and Electronics Engineers (IEEE).** *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. 1994.

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

6. **Bailey, David and Wright, Edwin.** *Practical SCADA for Industry.* s.l. : Newnes, 2003.

7. **West, Andrew.** SCADA Communication protocols. [Online] http://www.powertrans.com.au/articles/new pdfs/SCADA PROTOCOLS.pdf.

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

9. **Boyer, Stuart A.** *SCADA Supervisory and Data Acquisition.* 2004.

10. **International Society of Automation (ISA).** ISA99 Committee - Home. [Online] http://isa99.isa.org/ISA99 Wiki/Home.aspx.

11. *Identifying, understanding, and analyzing Critical Infrastructure Interdependencies.* **Rinaldi, Steven M., Peerenboom, James P. and Kelly, Terrence K.** 2001, IEEE Control Systems Magazine.

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

13. **Tsang, Rose.** *Cyberthreats, Vulnerabilities and Attacks on SCADA networks.* 2009.

14. **Falliere, Nicolas, Murchu, Liam O and Chien, Eric.** *W32.Stuxnet Dossier.* Symantec. 2011.

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

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

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

18. —. *Process control and SCADA security. Guide 5. Manage third party risk.* Centre for the Protection of National Infrastructure.

19. —. *Process control and SCADA security. Guide 7. Establish ongoing governance.* Centre for the Protection of National Infrastructure.

20. **International Electrotechnical Commission (IEC).** *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. 2007.

21. **Department of Homeland Security (DHS).** DHS officials: Stuxnet can morph into new threat. [Online] 2011. http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat.

22. **McAfee.** Global Energy Cyberattacks: "Night Dragon". [Online] 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

23. **Gartner.** Assessing the Security Risks of Cloud Computing. *Gartner.* [Online] 2008. http://www.gartner.com/DisplayDocument?id=685308.

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

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

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

27. **International Electrotechnical Commission (IEC).** *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. 2010.

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

29. **DigitalBond.** DigitalBond. *ICS Security Tool Mail List.* [Online] http://www.digitalbond.com/tools/ics-security-tool-mail-list.

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

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

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

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

34. —. *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.* 2005.

35. —. *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.* 2006.

36. —. *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.* 2006.

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

38. **Commission of the European communities.** *Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* 2008.

39. —. *Communication from the commission to the European parliament. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* 2009.

40. —. *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.* 2011.

41. **Suter, Manuel and Brunner, Elgin M.** *International CIIP Handbook 2008 / 2009.* 2008.

42. **IRRIIS Project.** Homepage of the IRRIIS project. [Online] 2006. http://www.irriis.org.

43. **CRUTIAL Project.** CRitical Utility InfrastructurAL resilience. [Online] 2006. http://crutial.rse-web.it.

44. **CI2RCO Project.** Critical information infrastructure research coordination. [Online] 2008. http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=79305.

45. **ESCoRTS Project.** Security of Control and Real Time Systems. [Online] 2008. http://www.escortsproject.eu.

46. **INSPIRE Project.** INcreasing Security and Protection through Infrastructure REsilience. [Online] 2008. http://www.inspire-strep.eu.

47. **VIKING Project.** Vital Infrastructure, Networks, Information and Control Systems Management. [Online] 2008. http://www.vikingproject.eu.

48. **The White House.** Executive Order 13231. [Online] 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

49. **Jeff Trandahl, Clerk.** USA Patriot Act (H.R. 3162). [Online] 2001. http://epic.org/privacy/terrorism/hr3162.html.

50. **Department of Homeland Security (DHS).** Homeland Security Presidential Directive-7. [Online] 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

51. **Stouffer, K. A., Falco, J. A. and Scarfone, K. A.** *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).* s.l. : National Institute of Standards and Technology, 2011.

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

53. **The White House.** National Strategy for Information Sharing. [Online] 2007. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

54. **United States Computer Emergency Readiness Team (US-CERT).** US-CERT: United States Compueter Emergency readiness Team. [Online] http://www.us-cert.gov.

55. —. Control Systems Security Program: Industrial Control Systems Cyber Emergency Response Team. [Online] http://www.us-cert.gov/control_systems/ics-cert/.

56. —. Control Systems Security Program: Industrial Control Systems Joint Working Group. [Online] http://www.us-cert.gov/control_systems/icsjwg/index.html.

57. **Huntington, Guy.** *NERC CIP's and identity management.* Huntington Ventures Ltd. 2009.

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

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

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

61. **Web application Security Consortium.** Web Application Firewall Evaluation Criteria. [Online] 2009. http://projects.webappsec.org/w/page/13246985/Web Application Firewall Evaluation Criteria.

62. **Masica, Ken.** *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.* 2007.

63. —. *Securing WLANs using 802.11i. Draft. Recommended Practice.* 2007.

64. **Ginter, Andrew.** *An Analysis of Whitelisting Security Solutions and Their Applicability in Control Systems.* 2010.

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

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

67. **Holstein, Dennis K.** *P1711 "The state of closure".* s.l. : PES/PSSC Working Group C6, 2008.

68. **Holstein, Dennis Cease, Li, Haiyu L and Meneses, Albertin,.** *The Impact of Implementing Cyber Security Requirements using IEC 61850.* 2010.

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

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

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

72. —. *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

73. —. *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

74. —. IEEE Power & Energy Society. [Online] http://www.ieee-pes.org.

75. —. IEEE PES Computer and Analytical Methods SubCommittee. [Online] 2000. http://ewh.ieee.org/cmte/psace/CAMS_taskforce.html.

76. **International Federation of Automatic Control (IFAC).** TC 3.1. Computers for Control — IFAC TC Websites. [Online] http://tc.ifac-control.org/3/1.

77. —. Working Group 3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/5/4/working-groups/copy2_of_working-group-1-decentralized-control-of-large-scale-systems.

78. —. TC 6.3. Power Plants and Power Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/6/3.

79. **International Federation for Information Processing (IFIP).** IFIP WG 1.7 Home Page. [Online] http://www.dsi.unive.it/~focardi/IFIPWG1_7.

80. —. IFIP TC 8 International Workshop on Information Systems Security Research. [Online] http://ifip.byu.edu.

81. —. IFIP Technical Committees. [Online] http://ifiptc.org/?tc=tc11.

82. *Security of Industrial Control Systems, What to Look For.* **Zwan, Erwin van der.** 2010, ISACA Journal Online.

83. **Weiss, Joseph.** *Protecting Industrial Control Systems from Electronic Threats.* s.l. : Momentum Press, 2010.

84. **International Society of Automation (ISA).** LISTSERV 15.5 - ISA67-16WG5. [Online] http://www.isa-online.org/cgi-bin/wa.exe?A0=ISA67-16WG5.

85. **Meridian.** Meridian. [Online] http://www.meridian2007.org.

86. **Centre for the Protection of Critial Infrastructure (CPNI).** Meridian Process Control Security Information Exchange (MPCSIE). [Online] http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie.

87. **SANS.** SCADA Security Advanced Training. [Online] 1989. http://www.sans.org/security-training/scada-security-advanced-training-1457-mid.

88. —. The 2011 Asia Pacific SCADA and Process Control Summit - Event-At-A-Glance. [Online] 2011. http://www.sans.org/sydney-scada-2011.

89. **Open Smart Grid.** Open Smart Grid. [Online] http://osgug.ucaiug.org/default.aspx.

90. **INTERSECTION Project.** INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks (INTERSECTION). [Online] 2008. http://www.intersection-project.eu.

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

92. **Centre for the Protection of Critical Infrastructure (CPNI).** CPNI. [Online] http://www.cpni.gov.uk/advice/infosec/business-systems/scada.

93. **Rijksoverheid.** Scenario's Nationale Risicobeoordeling 2008/2009. [Online] 2009. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/21/scenario-s-nationale-risicobeoordeling-2008-2009.html.

94. **Energiened.** Energiened Documentation. [Online] http://www.energiened.nl/Content/Publications/Publications.aspx.

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

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

97. **eSEC.** eSEC. *Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza.* [Online] http://www.idi.aetic.es/esec.

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

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

100. **Department of Energy (DoE).** Cybersecurity for Energy Delivery Systems Peer Review. [Online] 2010. http://events.energetics.com/CSEDSPeerReview2010.

101. —. Control Systems Security Publications Library. [Online] http://energy.gov/oe/control-systems-security-publications-library.

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

103. **Berkeley III, Alfred R. and Wallace, Mike.** *A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council.* s.l. : National Infrastructure Advisory Council, 2010.

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

105. **Smart Grid Interoperability Panel (SGIP).** SGIP Cyber Security Working Group (SGIP CSWG). [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

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

107. **Smith, Steven S.** *The SCADA Security Challenge: The Race Is On.* 2006.

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

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

110. **Asad, Mohammad.** Challenges of SCADA. [Online] http://www.ceia.seecs.nust.edu.pk/pdfs/Challenges_of_SCADA.pdf.

111. **Amin, Saurabh, Sastry, Shankar and Cárdenas, Alvaro A.** *Research Challenges for the Security of Control Systems.* 2008.

112. **ZigBee.** ZigBee Home Automation Overview. [Online] http://www.zigbee.org/Standards/ZigBeeHomeAutomation/Overview.aspx.

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

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

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

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

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

118. —. *Process control and SCADA security. Guide 4. Improve awareness and skills.* Centre for the Protection of National Infrastructure.

119. —. *Process control and SCADA security. Guide 3. Establish response capabilities.* Centre for the Protection of National Infrastructure.

120. —. *Process control and SCADA security. Guide 2. Implement secure architecture.* Centre for the Protection of National Infrastructure.

121. —. *Process control and SCADA security. Guide 1. Understand the business risk.* Centre for the Protection of National Infrastructure.

122. —. *Process control and SCADA security.* Centre for the Protection of National Infrastructure.

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

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

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

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

127. —. *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. 2009.

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

129. —. *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. 2007.

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

131. —. *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. 2010.

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

133. —. *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* British Columbia Institute of Technology (BCIT). 2005.

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

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

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

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

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

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

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

141. —. *CIP-001-1a: Sabotage Reporting.* North American Electric Reliability Corporation. 2010.

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

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

144. —. *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). 2009.

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

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

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

148. **Theriault, Marlene and Heney, William.** *Oracle Security.* First Edition. s.l. : O'Reilly, 1998. p. 446. 1-56592-450-9.

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