Survey and interview analysis

For the Report : Good practices for an EU ICS testing coordination capability

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (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.

Authors

- Konstantinos Moulinos, ENISA
- Adrian Pauna, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Contributors

- Carlos Monreal Ibañez, S21sec
- Luis Tarrafeta, S21sec
- Daniel Herreras Rodríguez, S21sec
- Jairo Alonso Ortiz, S21sec
- Victor Fidalgo Villar, S21sec
- Edurne Osés Goicoechea, S21sec

The drafting of this Report would not have been possible without the feedback and cooperation kindly provided by a large number of organisations and individuals. We would like to thank all the experts that took part in the survey for this project (Experts listed in the : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability/list-of-interviewees-reviewers-and-workshop-participators/view).

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

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

Copyright Notice

ISBN 978-92-9204-074-1 doi: 10.2824/26451

Cover Photo credits: “GFAC chip” by “PNNL - Pacific Northwest National Laboratory” under Creative Commons License with the following conditions: Attribution, Non-Commercial use and Share Alike.

Table of content

1 Introduction

This document provides an analysis of the raw data from the online survey and the interviews. What is presented here is not the complete set of answers, but a processed summary of the most relevant aspects of the data. The chapter is divided into the following sections or topics:

- **Status**: Concerning the present situation of ICS Security Testing.
- **Objectives**: Questions intended to understand the testing capabilities that experts consider priority to develop in the EU.
- **Model**: Enquiries to discuss the most suitable organisational models.
- **Resources**: To identify any interesting resources that have to be taken into account in order to obtain results in the most efficient way.
- **Constraints**: Intended to foresee any challenges, limitations or problems that could arise within the process.
- **External Relationships**: Specific questions regarding how to articulate the cooperation and information flows between the testing body and all involved entities.

Each 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.

Although most of the questions were included in both the online survey and the interviews, some of them appeared in just one format. This was done in order to find a balance between the advantages and disadvantages of using Closed Questions (limit answers as much as possible) and Open Questions (free answers)

- Closed Questions provide less information, require more work to define and can miss some interesting answers but are easier to analyse.
- Open Questions provide more information but are more difficult to analyse and can lead to excessively complex debates.

Taking into account the number of people to be interviewed the following approach was used:

- Use as many ‘closed questions’ as possible to analyse easily.
- Leave always the option for ‘deeper explanations’ as open fields.

It has been considered that doing so:

- Any interesting knowledge, fundamental opinion or matter of discussion arose easily.
- Experts could focus on the points they have more interest in.

The data have been analysed from different points of view. Firstly, a global overview of all answers was interpreted to get the general ideas from the community. Then, all answers were reviewed taking into account the Stakeholder type or the Sector the experts belong to. In general terms, differences of opinion are more evident when grouping by Stakeholder type than by Sector. This could be related to the fact that many experts work in several sectors at the same time, or just because points of view are more consistent with their level in the value chain than with the nature of the final service they provide.

2 Status

2.1 CURRENT TESTING ACTIVITY

This question is exclusive for questionnaire respondents. It has a first part in which respondents have to select between five presented options and a second part in which explain deeply their response.

2.1.1 Does your Organisation perform Security test to the ICS devices and or applications it manufactures/buys/recommends?

According to the answers, respondents companies do not have the same level of commitment regarding ICS Security Testing. Excluding the 'Never' option, which only had one answer, there are significant percentages for all other responses. Figure 1 show this diversity of opinion among stakeholders.

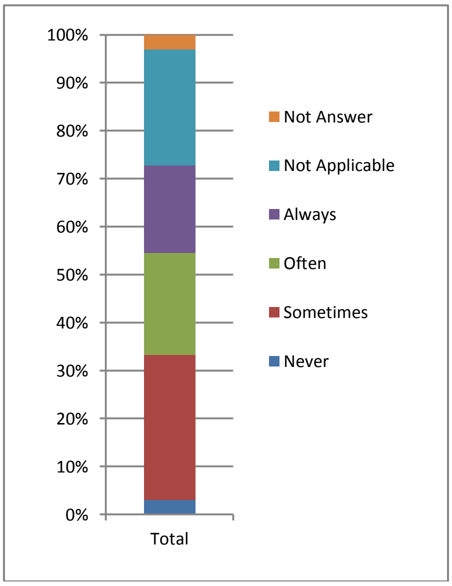


Figure 1: Percentage performing security tests

The 'Never' response percentage is very low, so the majority of consulted stakeholders consider security testing as something to take into account, at least 'Sometimes' (~30%) within companies. While 21% do it 'Often' and almost the same amount (~18%) do it 'Always'.

If results are evaluated by sector division (Figure 2), excluding 'Not Answer' and 'Not Applicable' results, all sectors except 'Other or not applicable' group do security tests 'Always' in almost 50% of devices, and, including 'Often' responses, the percentage rises to 70%. The 'Something' answer accounts for less than 30% of responses, except in the 'Manufacturing' group, which are more involved in this activity, and their lowest rated level was 'Often'.

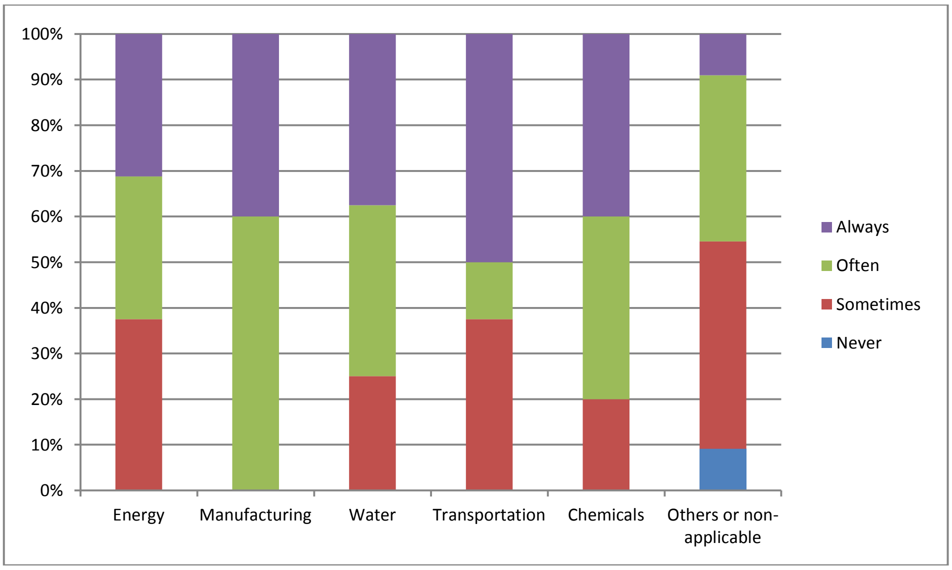


Figure 2: Percentage performing security tests

Compared with sector division, stakeholder type division shows that 'Sometimes' response has more presence, with approximately 30% in many cases, except in 'ICS Security Tools and Services Providers' group, which have a greater awareness and a more common used of this type of tests. It is important to highlight that 'Public Bodies for ICS Protection' group has no responses for 'Always' option and 'Academia and R&D' is the only group with a 'Never' in its responses. This could be because of the fact that there are no production devices in research installations and, hence, security is not considered critical.

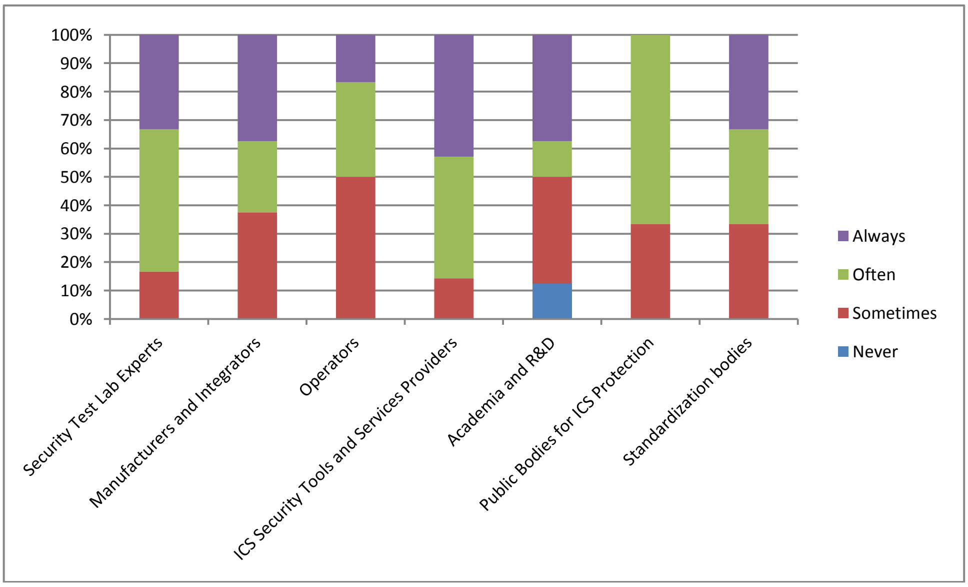


Figure 3: Percentage performing Security tests by stakeholder type

2.1.2 If yes, how are these tests performed?

Many experts, and their companies, perform tests in their own facilities and with their own devices. As a general rule, tests are done in preproduction scenarios or independent test labs specifically created for these security functions. Many experts stated that sometimes they do tests during maintenance time in production systems, while the system is not active.

All stakeholders coincide in doing test in passive mode, sometimes by just ‘sniffing and analysing’, since intrusive tests can damage their devices. But this does not mean that some companies are performing – with proper cautions – other techniques such as penetration testing. Not taking into account security test, stakeholders do tests such as resilience test, power fail test and contingency test.

During the interviews some experts, especially from CI, explained that they do not trust any certification or vendor claim without performing their own testing, at least for SAT Tests (‘Site Acceptance Tests’, for an ‘in-house’ perspective[1]). Then, they can use two different testing methods:

- ‘Correct Data’ to assure that everything works correctly under ‘expected conditions’, and
- ‘Incorrect data’, more creative and controversial, as they try to analyse how the system works under ‘abnormal conditions’ – something that can have many interpretations.

2.2 STANDARDS: Which standards/guides/good practices on ICS security Test Bed frameworks do you use or intend to use?

This question presented a set of standards or good practices guides to rate their level of use. Answers left blank were considered as ‘not taken into account’ which, in some cases, represent up to 50% of answers. The best-rated standards were the ‘ISA 99’ and its derivates, followed by NIST documents.

It is important to note that there were many ‘Not aware’ and ‘Not interesting’ responses, but these results could be justified because some of the documents presented are not specifically for testing purposes. ‘UCAIUG AMI-SEC-ASAP ‘and ‘TSWG’ documents have the lowest ratings; ISO/IEC ones have similar percentages of ‘Not aware’ and ‘Not interesting’ but they also have an important percentage of ‘Necessary’ responses.

[1] Opposed to FAT Testing (Factory Acceptance Tests), an ‘outside’ perspective and then considered ‘not so critical’.

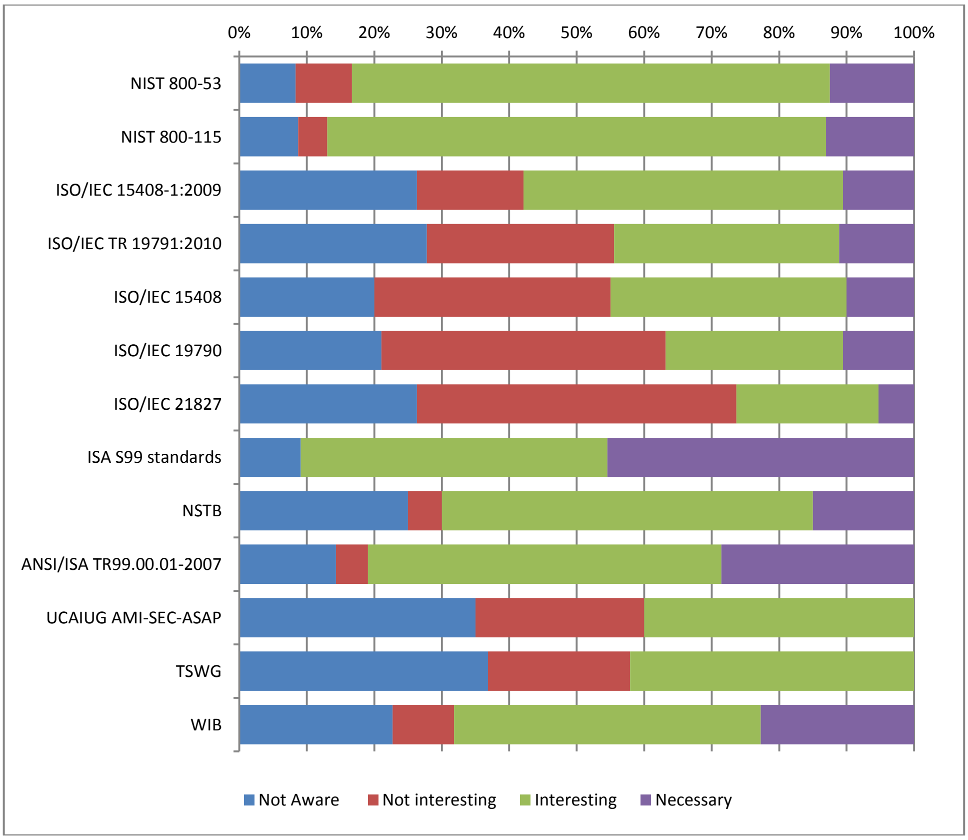
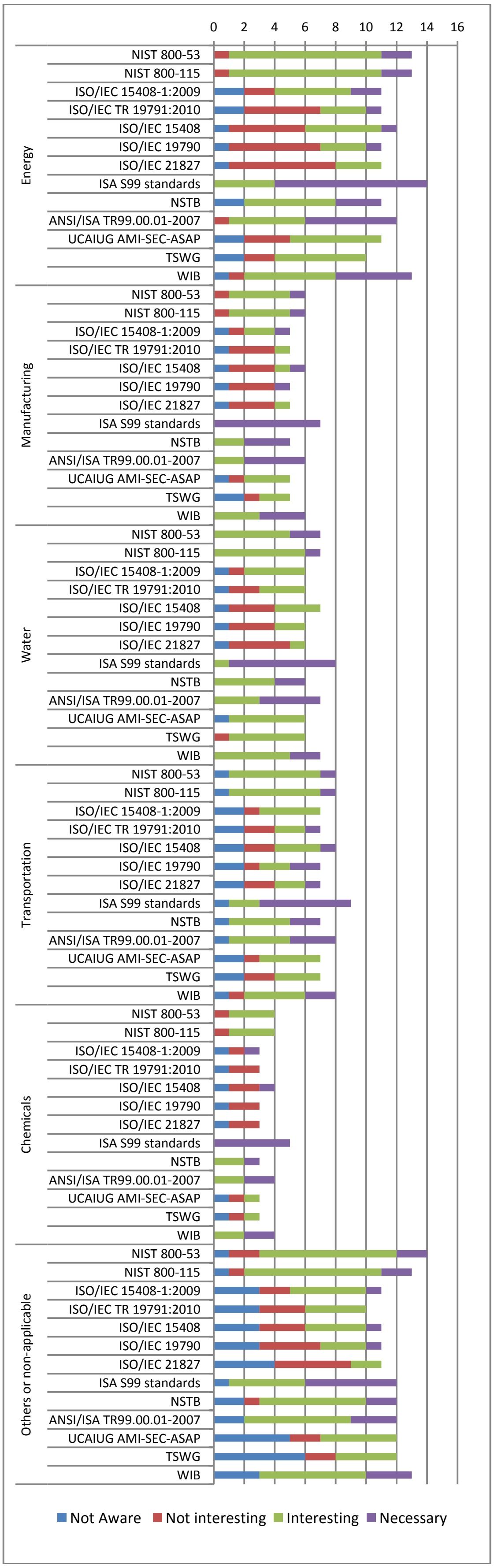


Figure 4: Degree of use of the different standards, guides or good practices

Data division by stakeholder type highlights that ‘Transportation’ and ‘Others or not applicable’ groups are the least aware of presented documents; on the other hand, the ‘Academia and R&D’ sector group has the most ‘Not aware’ selections for all presented documents, followed by ‘Manufacturers and Integrators’.


0
2
4
6
8
10
12
14
16
Energy
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Manufacturing
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Water
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Transportation
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Chemicals
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Others or non-applicable
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Not Aware
Not interesting
Interesting
Necessary

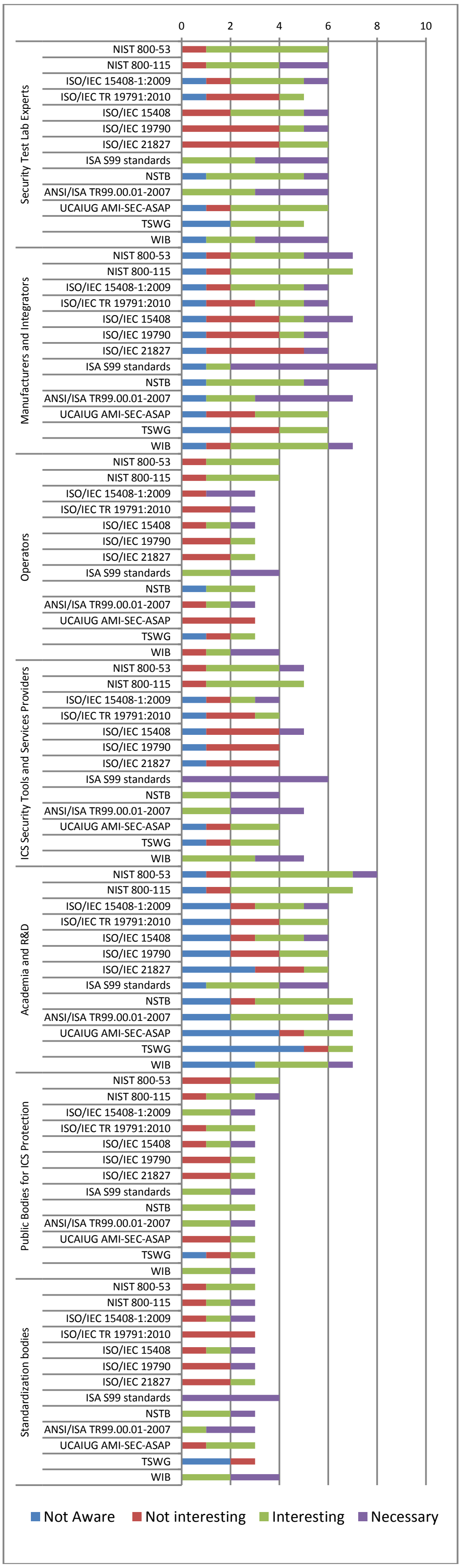

0
2
4
6
8
10
Security Test Lab Experts
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Manufacturers and Integrators
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Operators
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
ICS Security Tools and Services Providers
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Academia and R&D
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Public Bodies for ICS Protection
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Standardization bodies
NIST 800-53
NIST 800-115
ISO/IEC 15408-1:2009
ISO/IEC TR 19791:2010
ISO/IEC 15408
ISO/IEC 19790
ISO/IEC 21827
ISA S99 standards
NSTB
ANSI/ISA TR99.00.01-2007
UCAIUG AMI-SEC-ASAP
TSWG
WIB
Not Aware
Not interesting
Interesting
Necessary

Figure 5: Degree of use of the different standards, guides or good practices by sector and by stakeholder type respectively

An interesting opinion of an interviewer is that '*In the industrial world, people (especially operators) are reluctant to include "wide" security methodologies like these because they see them as "too big" and also somehow immature. It is better to go little by little.*' This concrete opinion highlights another stakeholder point of view: They prefer their own methodology, adapted to their necessities. Or, as another expert stated, they follow the ISO model, so they can start with very generic ones, making them more specific in future iterations.

Respondents and interviewers also mentioned other documents and standards that were not presented among the options. These documents are shown in ANNEX II along with a description of the good practices guides and standards for security testing.

2.3 RISK MANAGEMENT: Do you use or intend to implement a Risk Management System to control an ICS system security? Do you think a testing framework could help you to do so?

The group of experts were asked about the use of a risk management system and the bulk of the stakeholders answered positively. It should be noted that the set of experts who responded negatively to the question are mainly security test lab experts; other types of participants answered that they already implement a system of risk management.

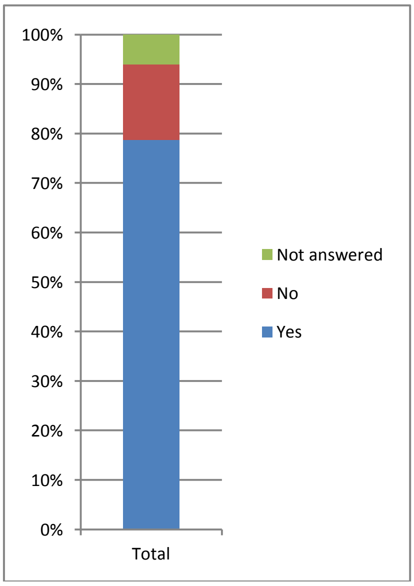


Figure 6: Percentage using risk management system

In the second question, 'Do you think a testing framework could help you to do so?', the negative answer was only selected by the 'Public Bodies for ICS Protection' and 'Academia' experts group. Checking it by sectors, all other than 'non-applicable' have agreed in answering 'Yes'.

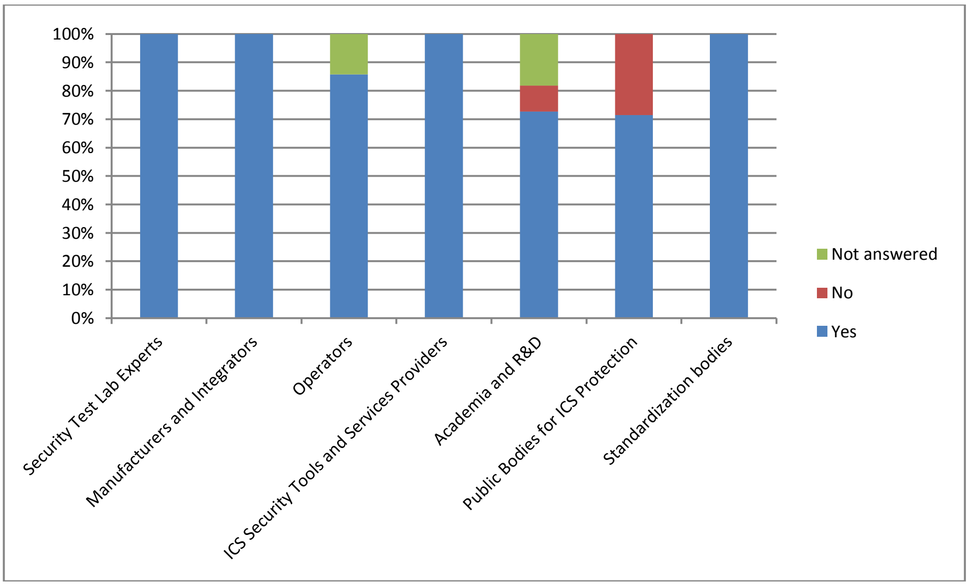


Figure 7: Percentage using risk management system by stakeholder type

During the interviews, some of the experts stated that a good way to implement a work plan for a test bed methodology is:

1. Create a General Methodology and
2. In following versions, branching work in a way that will specialise for different ICS sectors.

Regarding the methodologies used by stakeholders, they were adapted according to the stakeholder's specific criteria. Each company uses a set of controls taking parts of the documentation, according to their own judgment, to create their own methodology. For this reason, there is considerable variation in methodologies used for risk management in ICS. Most experts agree that a common methodology would be interesting or even necessary, as currently some companies state that 'as there is no mandate, I am not doing anything'. For these reasons the majority of experts support the idea of creating a test bed framework.

2.4 TEST BED BENCHMARKS

2.4.1 Are you aware of any initiative based on Test Bed Benchmarks for ICS technologies?

When asked if different stakeholders are aware of the existence of initiatives based on the creation of test bed more than 50% of respondents answered negatively. All the interviews show that experts are not aware of the existence of such initiatives, with just 15% of the set of experts who are actively involved knowing the state of the initiatives in which they participate. Responses seem to be independent of any stakeholder or sector perspective.

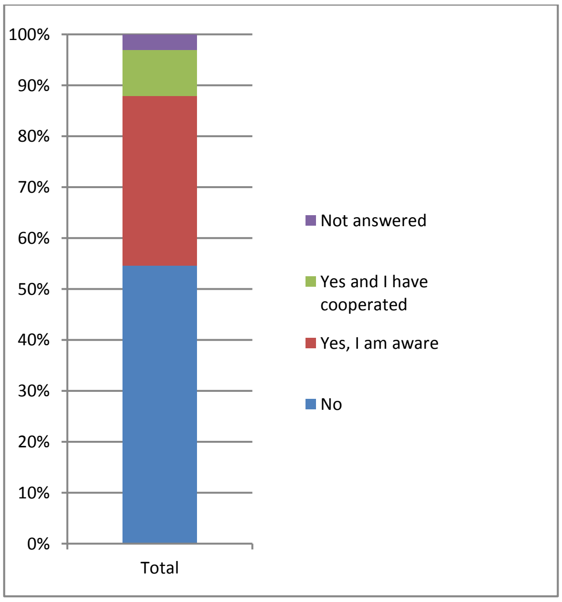


Figure 8: Degree of awareness of initiatives based on Test Bed Benchmarks

A list of initiatives that different experts have provided in answer to this question is shown in Annex II .

2.4.2 If proposed to do, would you like to cooperate in an additional one?

To the question about the offer to participate in a test bed initiative, 50% of the experts answered 'Could cooperate' and another 40% stated that they are 'Strongly Interested'. Even if not aware of such initiatives, many experts want to take part in testing activities.

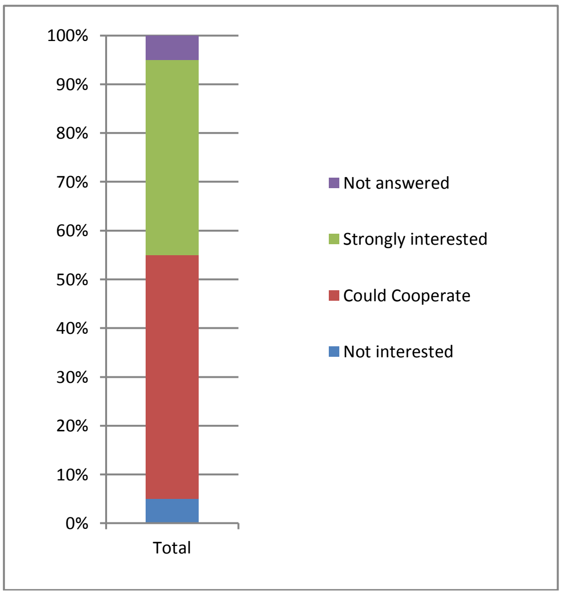


Figure 9: Degree of acceptance to cooperate in initiatives

Divided by sectors, 'Energy' is the only one in which some experts answered 'Not interested', even though this sector is one of the most involved and aware of security aspects. This could be explained by the fact that there are already many initiatives, especially in the Smart Grid field, that could be too time consuming for some.

2.5 INTEREST: Do you consider interesting the creation of a common Test bed/Framework for ICS technologies in the EU?

Experts were asked whether it would be advisable to create a common test bed or framework for Europe that would cover the capabilities of member countries. All experts indicated acceptance of this idea and they exhibited positive attitudes towards such initiatives.

Respondents were asked to rate their interest between '0' 'Against the creation of such Framework', which got no answers, and '5' 'Indispensable'. The graph below (Figure 10) shows the degree of acceptance of this idea in a numeric form. The average of data responses is close to 4, which translates to a 'Strongly Positive' opinion.

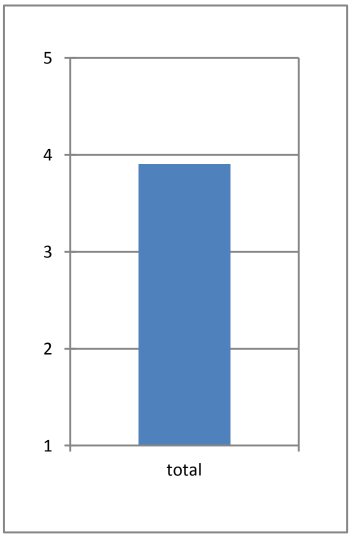


Figure 10: Degree of interest in the creation of a common Test bed/Framework

Checking from a Stakeholder Type perspective, 'Public Bodies for ICS Protection' and 'Standardisation bodies' are the ones that showed least interest, although many consider (see 4.2.1) they should be the leaders of such a body. In any case, they also support the initiative. It is also important to highlight that the 'Operators' group is one of the most involved, which reflects their interest in security.

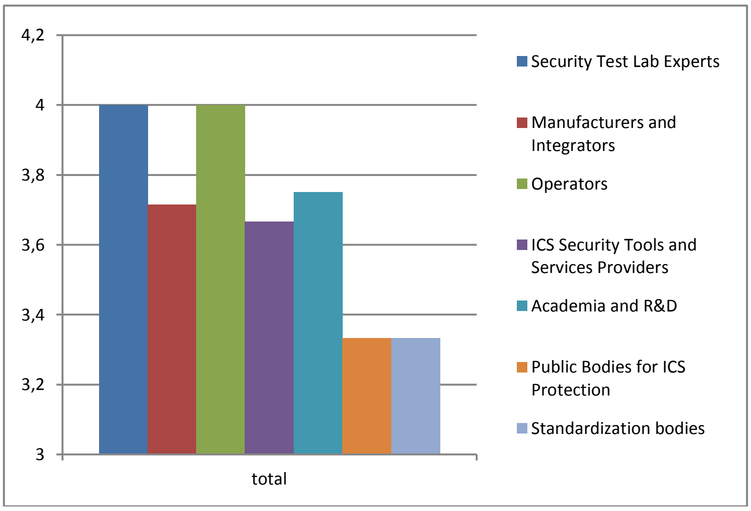


Figure 11: Degree of interest in the creation of a common Test bed/Framework by stakeholder type

3 Objectives

3.1 DRIVERS: Which do you consider the main drivers for such a Framework/Test bed?

In this question, for each of the provided answers respondents could rate their level of agreement between -2 points (Strongly Disagree) and +2 points (Strongly Agree). The results (Figure 12) were as follows:

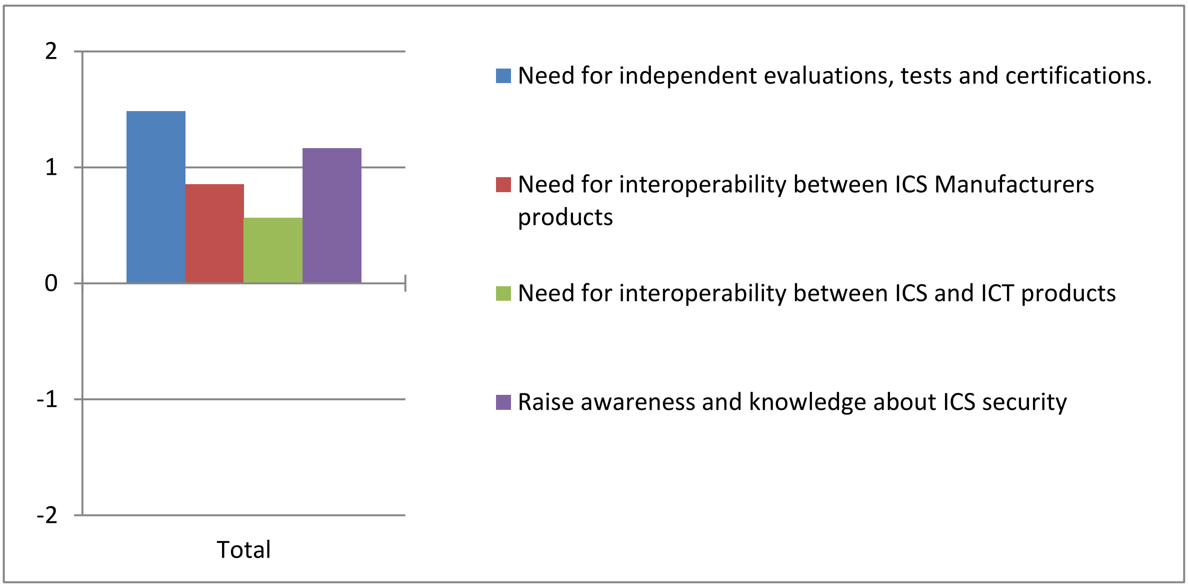


Figure 12: Main drivers for such a Framework/Test bed

So, it can be concluded that the Biggest Driver is 'Need for independent tests and certifications' (almost 1.5 points). Very few disagree or strongly disagree on this point. 'Raising awareness' is also considered very positively (1.16). Interoperability between different ICS manufacturers is in third position, but no respondent strongly disagrees with this one. The least important option is interaction between ICS and ICT, and also the most controversial as most people agree, but a significant minority disagree or strongly disagree. In any case, all reasons are rated positively on average.

Similar results were obtained when checking by Sector. But, when looking from a Stakeholder perspective we can see:

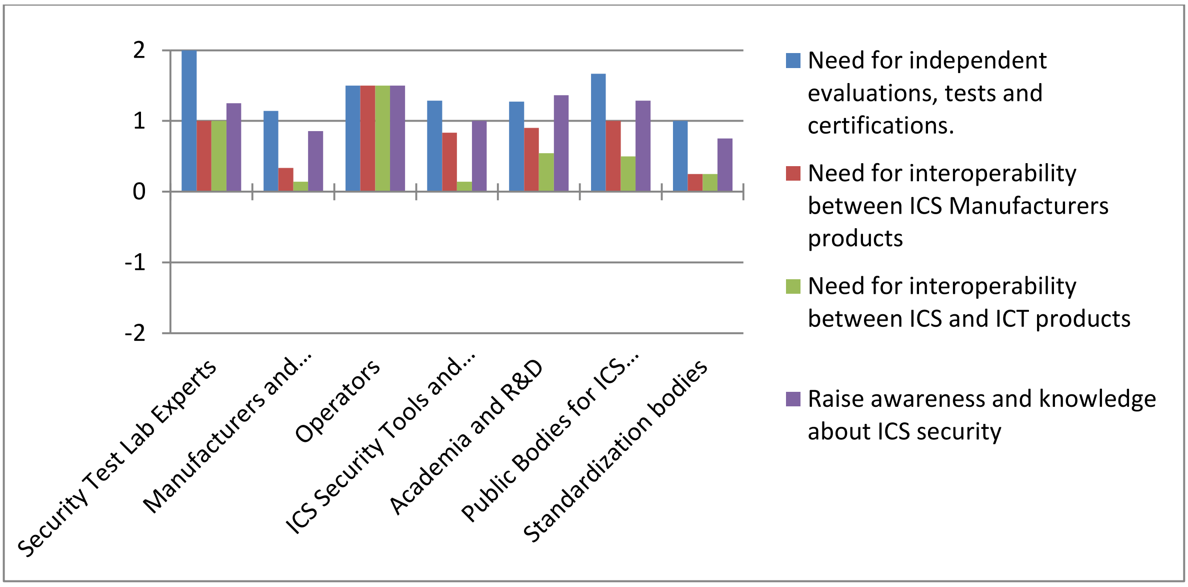


Figure 13: Main drivers for such a Framework/Test bed by stakeholder type

We can see that all Security test lab experts 'strongly agree' with reason A and, on average, agree or strongly agree with all reasons and Operators too. Academia and Public Bodies are not so enthusiastic.
Manufacturers, on the other hand, are the ones that have more differences between them. ICS Sec Tools & Service Providers and Standardisation Bodies present a similar profile to Manufacturers.

During the interviews or written responses some other reasons appeared in the form of 'open answers'. For example: the ability to measure real consequences of a disaster and implications for citizens. This is of high interest if combined with the fact that 'Political reasons are always a main driver', as some explained that INL NSTB was fostered after 9/11 and CSSC got necessary funding after the Japanese earthquake and Fukushima incident.

Other experts talked about the need to improve products or overall security in ICS systems in the EU. There is also a need to ease as much as possible the regulations to be followed, to lower the costs of implementing security for all involved stakeholders, harmonise standards, and provide an educational environment, currently lacking.
Several experts noted that interoperability cannot be seen as a driver by itself; the important thing is how interoperability affects security, otherwise the body could lose the target.

For some experts, especially those familiar with the situation outside the EU, 'Awareness' is already there, as it has increased during the last few years. This is particularly the case among technicians, but not so much in the senior management environment. One expert referred to a private study[2] showing that, in the last 3-4 years, operators are becoming less concerned about interoperability and more about security. They do not buy any product that is not interoperable.

Another expert explained the importance of telling the users how secure and compliant their security postures are. In fact, in the EU, at least two countries are working on this (UK and Germany) but as they are working independently their approach is not common.

[2] As the study is private, it is not possible to cite it here.

Many agree that interoperability tests are currently being done (in users' premises or organisations such as ODVA, OPC Foundation, PTO, Fieldbus Foundation and standards such as IEC61850) but for security 'wrong data' also has to be checked, and this is far more controversial.

3.2 MISSION: What should be the main mission for such a Framework/Test bed?

Several reasons were provided, rated in the same way as in 3.1, regarding the Mission that an eventual Testing Body in the EU should have.

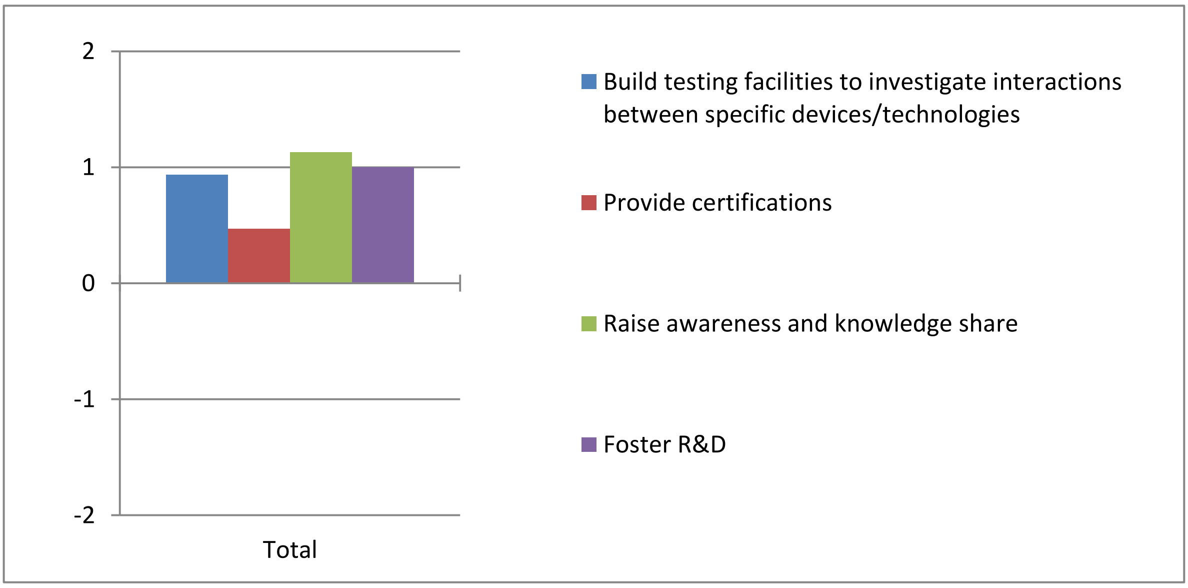


Figure 14: Main mission for such a Framework/Test bed

General results show that any of the provided reasons were considered positive on average, which is also true for every Stakeholder type and Sector.
The most valued reason was 'raising awareness and knowledge', but 'Foster R&D' and 'Investigate interactions between specific devices or technologies' also had good acceptance, albeit that many experts have responded 'neutral' to that one. The least accepted mission is 'providing certifications', which received an almost 'neutral' rating, with a significant group of experts disagreeing or strongly disagreeing about it.

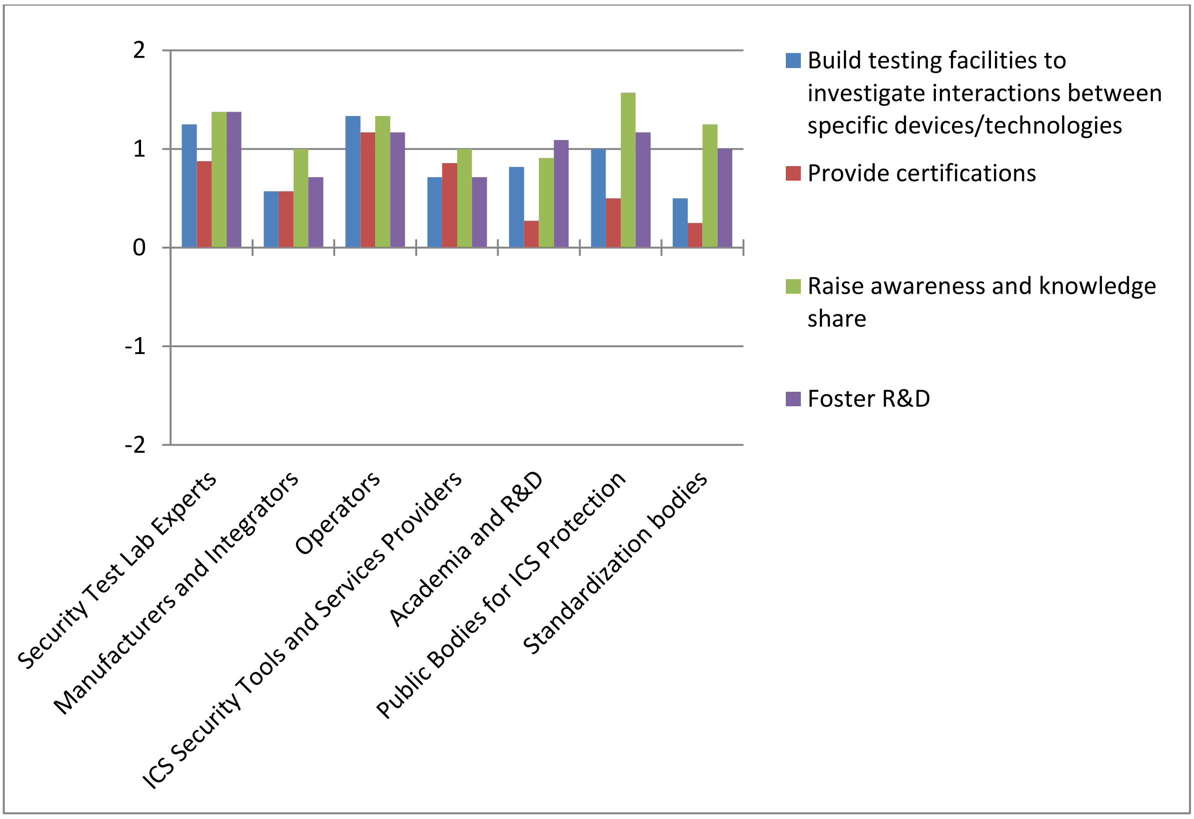


Figure 15: Main mission for such a Framework/Test bed by stakeholder type

There are no great differences in terms of Sector. However, when reviewing by Stakeholder type it can be concluded that Operators are the ones that agree most with all suggestions, including the controversial ‘providing certifications’, and close to them are the ICS Security Test Labs Experts. Manufacturers are the ones that agree least, but it can be said that there is no great debate among them, as most of their answers are between ‘neutral’ and ‘strongly agree’. The biggest internal confrontation is in academia, especially concerning the point ‘provide certifications’.

During the interviews some other points arose. For example, it was stated that the Mission should be assured in a more generic way. For example, the ENCS mission is ‘Foster security to a higher level in customer assets’. Some others missed options like ‘Define for customers what is a good level of testing quality’, generate and share information about ICS security testing, generate references and guidelines to classify products and evaluate compensation measures, etc.
Several experts believe that certifications have to be aligned with other industry standards (ISA Secure) but consider it unnecessary, or even harmful, to create a new one as the market is already too fragmented. Concerning this, some say that the ultimate solution is not to certificate the products themselves, as there are so many alternatives, but the development lifecycle. The way security is built in and taking into consideration in their procedures and way of working. Many technical experts agree that it is important to ‘stop making compliance and start building security’, because certification can give a wrong security impression.

3.3 TASKS: Which tasks should be performed by this Framework/Test bed?

A set of tasks was listed in order to rate them in the same way as in previous questions.

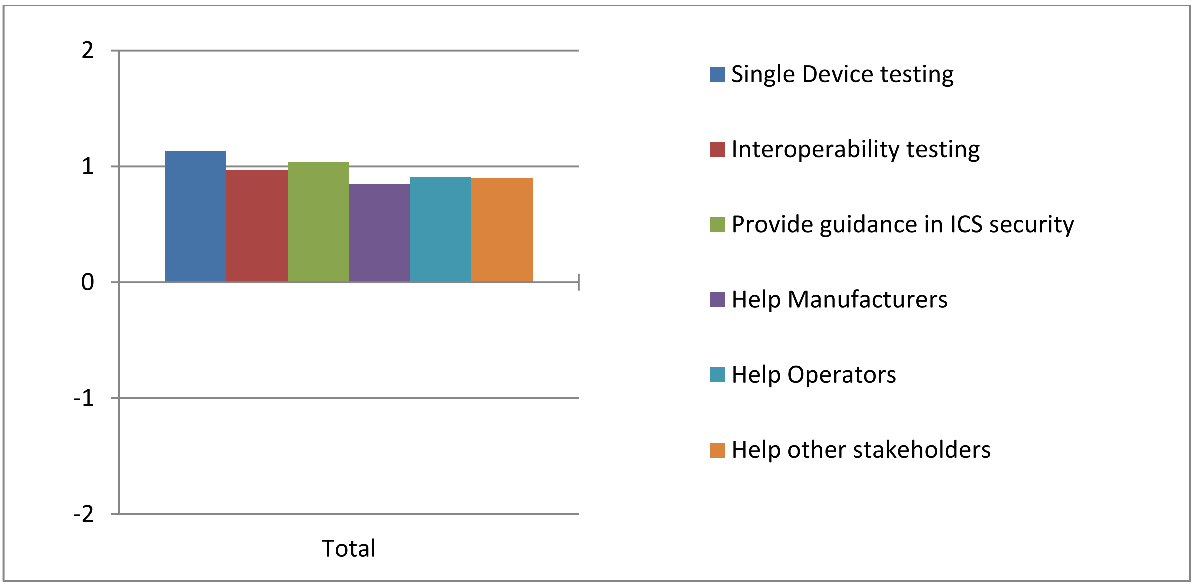


Figure 16: Task to be performed by the test bed

All described tasks enjoyed a high degree of agreement (between 0.84 and 1.12 points), with 'Single device testing' the highest, 'Provide guidance' the second and 'Helping manufacturers' the lowest. But, there was always some level of debate.

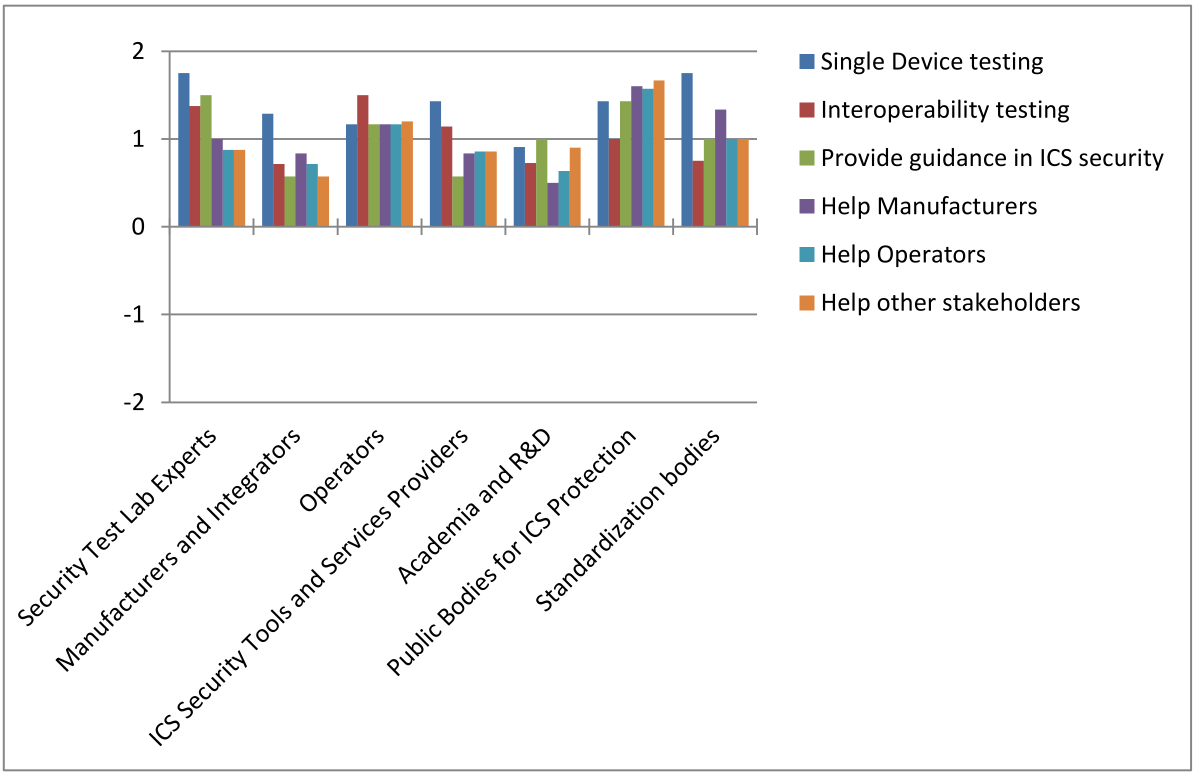


Figure 17: Task to be performed by the test bed by stakeholder type

Checking by stakeholder type, Public Bodies, Operators, Standardisation Bodies and Security Test Labs Experts are the more interested in any of the tasks, while Academia, Security Tools and Service Providers and Manufacturers are the least interested.

During the interviews some said that even if 'Help Manufacturers' could be interesting, especially in R&D and a way to provide them some value, it would be difficult due to privacy issues.

Regarding ‘Single Device Testing’, even if well rated, many problems were put forward:

- There are too many devices to test. It is not possible[3] to test all of them, and deciding which ones to choose is difficult even for mature organisations such as the NSTB at INL.
- Some experts think that single device testing is already being done in several places across the world (INL, CSSC) and that it could be enough.
- Europe has the option to focus on something else. In this respect, many talked about performing a holistic approach, considering pre-production environments, passive techniques or controlled penetration tests.

Other tasks considered missing have been ‘Cooperating with CERTs’, ‘Cooperation with Academia to foster Research and Education’, ‘helping government to set a balance between commercial interest and consequences to society in case of failures’ or ‘Providing security postures and metrics’.

3.4 ASSETS: What kind of assets do you think are of most interest to be tested by such an ICS Testing framework?

In this question different elements of the systems had to be rated: ‘0 – Not interesting’, ‘1 – Added Value’, ‘2 – Important’ and ‘3 – Critical’. The results were as follows:

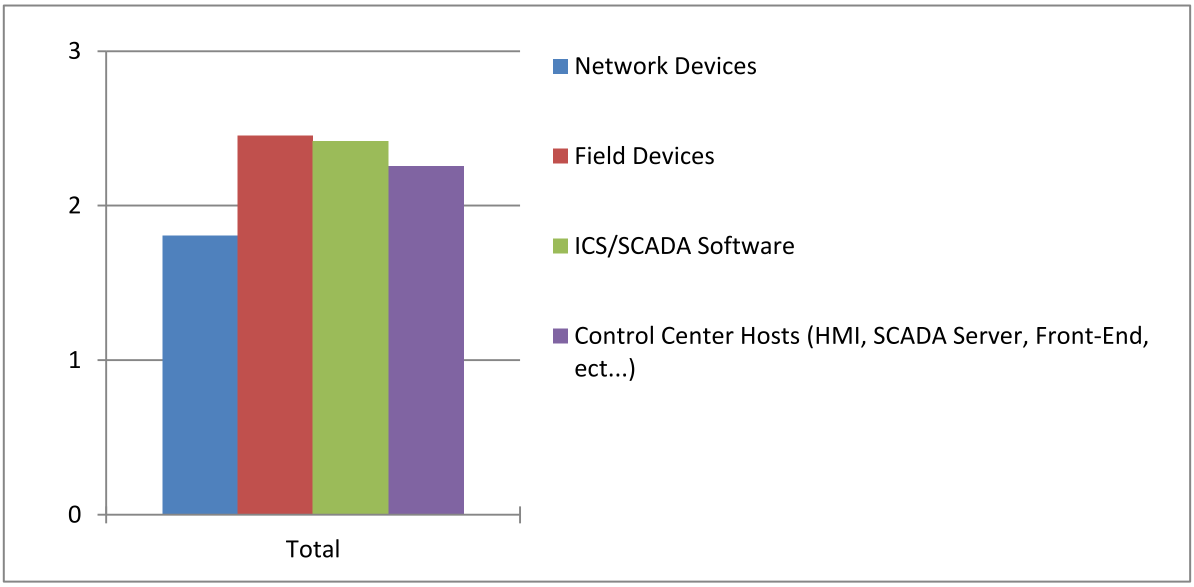


Figure 18: Degree of interest of the kind of assets to be tested

As can be seen, all devices are considered, on average, between important and critical, except network devices which are also considered ‘important’. This can also be understood as a need to think in a holistic way as explained in 3.3.

Reviewing the results by Stakeholder type (Figure **19**) it was found that PPBB are the most interested in any technology and Academia the least. Field Devices and ICS Software have the highest scores overall especially because of the contribution of STLE, ST&SP and PPBB.

[3] Because of the amount of resources

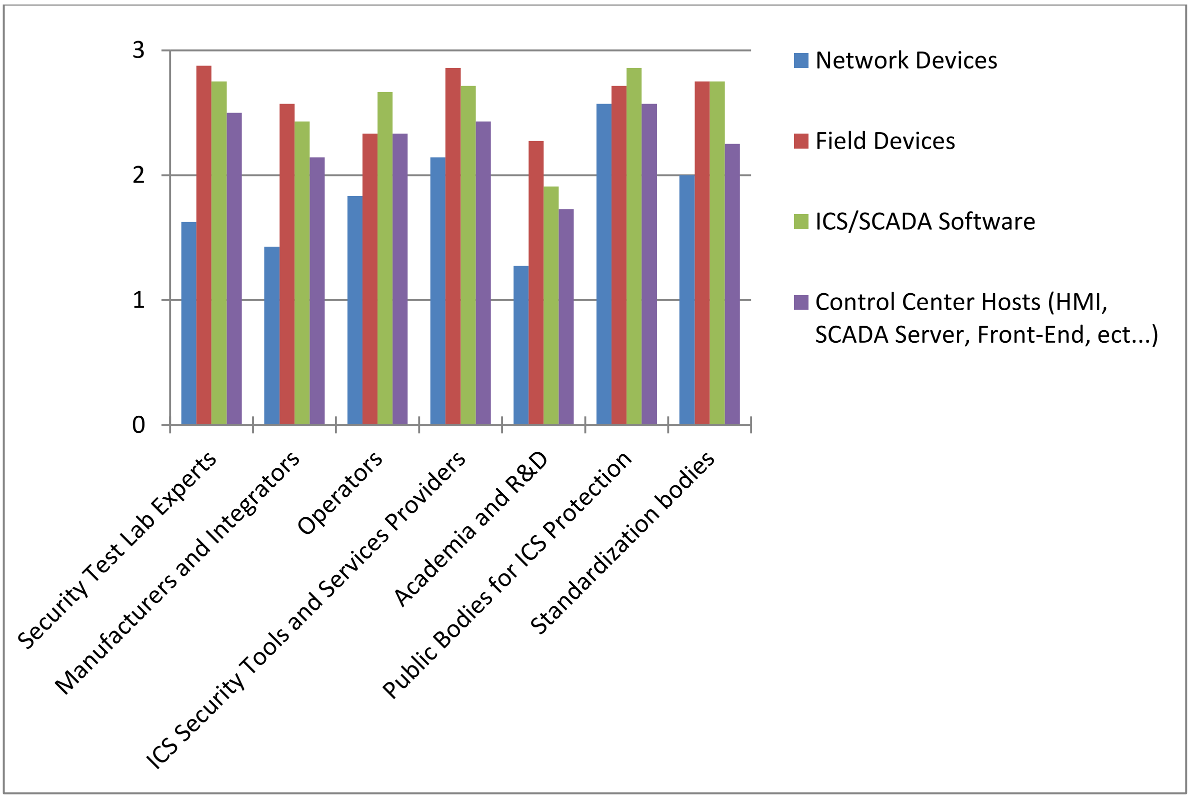


Figure 19: Degree of interest of the kind of assets to be tested – by stakeholder type

During the interviews some stated that they missed 'Remote access technologies' as they are one of the greatest vectors of infection. A few experts also said that it is difficult to assign criticality, because it will depend on the system and, currently, there are no good risk assessment methodologies. Related to this, an expert pointed out that even though there are many testing tools, there are no mature ones for field devices.

Some very technical experts noted that most often failures are architectural, that legacy systems and '*things*' that are not in network diagrams are often the weakest link. The best approach, in their opinion, to really understand the security level of a system is not through 'network diagrams' or Databases, but 'in the binaries, the source code and the traffic on the wire'. This also recalls the 'holistic approach' mentioned in 3.3.

3.5 MANDATORY VS OPTIONAL: Do you think that this Framework should be mandatory for any new technology or product?

This question was discussed especially in the interviews, but some options were provided by questionnaire responders.

It is interesting to see (Figure 20) that the answer which gets the greatest share is negative, 'No, just QA Certification', but more than half of the total are positive answers such as 'depending on business' or 'not yet but in the future' or, simply, 'yes'. So, it can be concluded that there is considerable debate in this area.

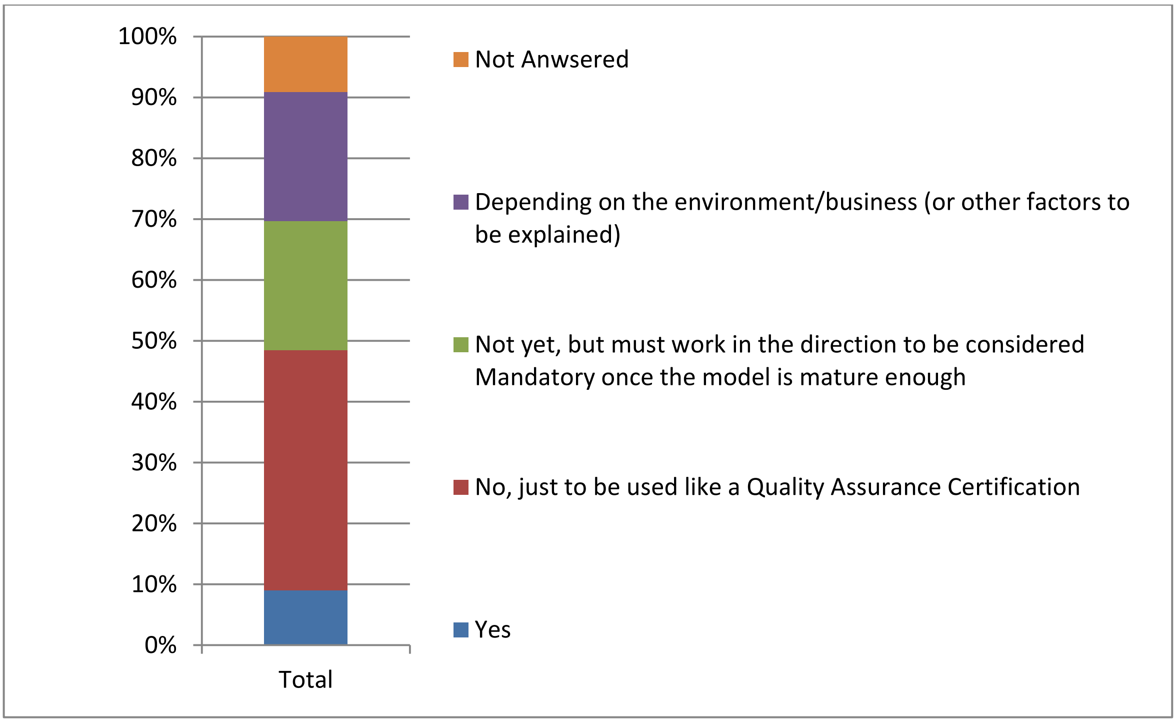


Figure 20: Acceptance percentage of mandatory of the framework for any new technology or product

Most of the simple 'yes' answers come from Operators and Security Test Labs Experts. Exactly 50% of Manufacturers are against, but many would prefer it under certain conditions or in the future. Regarding Sectors, the Water one is the most reluctant but Chemicals and Energy are 'for' it.

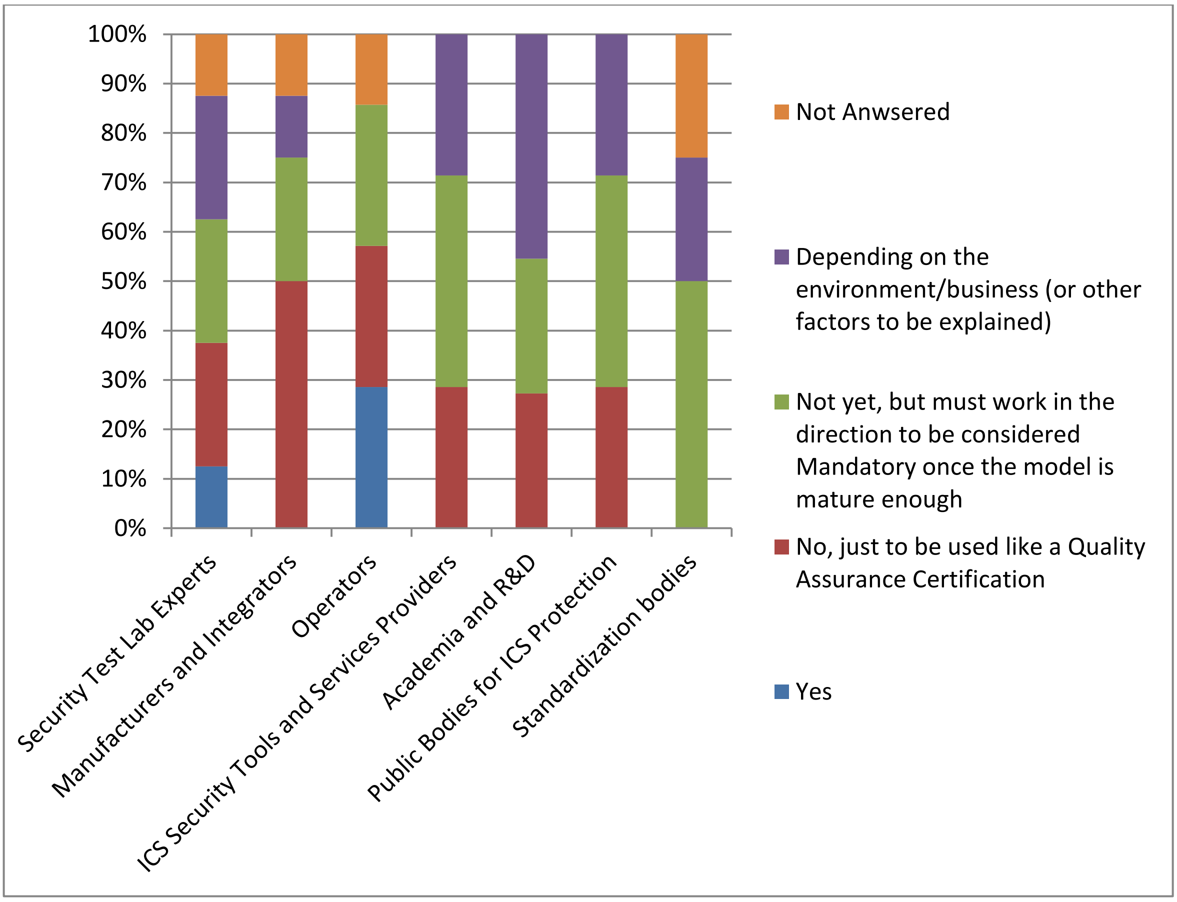


Figure 21: Percentage approving mandatory nature of the framework for any new technology or product by stakeholder type

During the interviews many debates arose:

- Some experts believed that test bed framework should be mandatory for CI or those that have an impact in society, but some replied that it is still no clear definition of what a CI is.
- Many experts think that it has to be mandatory, otherwise no one will follow, but some others think it might not be possible to do it. Specially taking into account that some stakeholders would be very reluctant.
- Some said that there are already 'safety' regulations that can be modified[4] to include this, and that, if mandatory, the investment in security would be 'acknowledgeable' somehow to be justified as Return Of Investment. In it, it is reasonable and a fact that cyber security issues in ICS environments could lead to real 'safety' problems.
- Several technical experts believe that there is a problem when similar experiences[5] had problems to effectively increase the security level, making it more a compliance issue than a real security driver.
- Some say that, more than a regulation, a certificate would work easily as it can be seen as a market advantage. One said that a reasonable approach could be to develop certifications according to robustness levels against different types of threats.
- Another option has been followed in Germany, where some operators have joined to publish a common set of requirements, so that they can push their providers in a more

[4] In fact, the Japanese CSSC is following this line of work.
[5] Like NERC-CIP in the US.

effective way. Furthermore, a common framework for the EU can help organisations to harmonise both their requests and offerings.

- A few Security Test Labs Experts have considered that, in any case, the eventual Testing Body should, at least, have some ability to force bug fixing under certain circumstances.

4 Model

4.1 CERTIFICATION FRAMEWORK VS TEST BED: Comparing a Certification Framework Model (such as Common Criteria or FIPS) with an ICS Testing Framework, which one do you consider a more appropriate approach?

This question has been intended to answer which Model is preferred for an eventual Testing Body, if a Test Bed is preferred or a Certification Framework. Both possibilities have been considered separately (Figure 22), as they can coexist and even rely on each other.

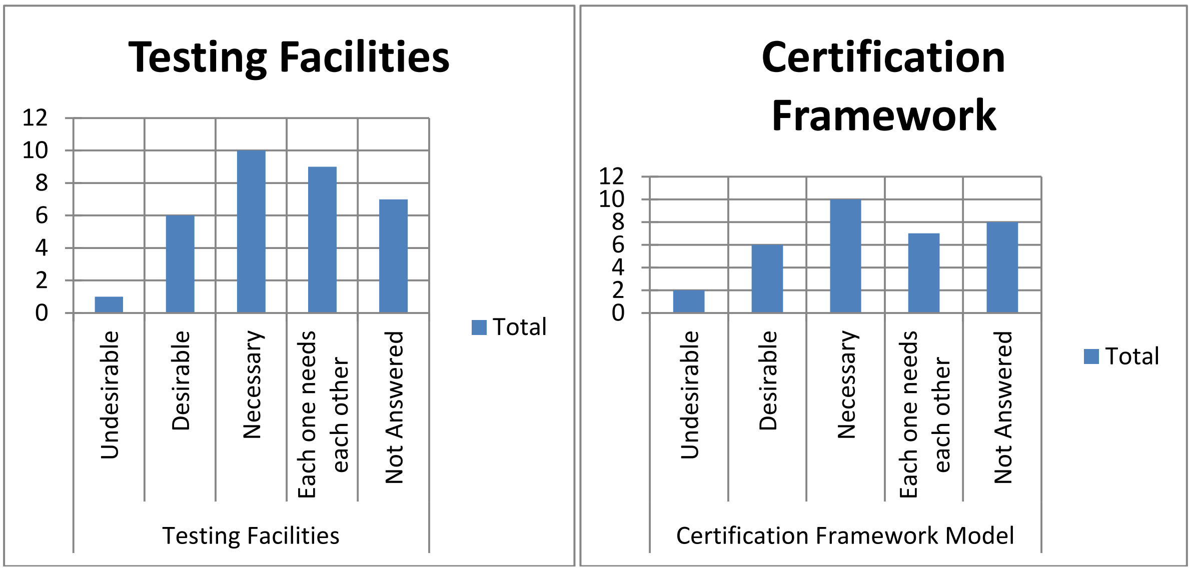


Figure 22: Certification Framework Model vs. ICS Testing Framework

From a general point of view, both options are positively considered, being 'necessary' or 'desirable' the options with more answers. It can also be highlighted that, for many, 'Each one needs each other' was the preferred option.

From a stakeholder perspective (Figure 23), the 'Certification framework model' is considered 'necessary' for almost all respondents from the 'Operators' group. Testing Facilities are also considered desirable or necessary for them. But, all other Stakeholders types consider more interesting the Testing facilities as their most chosen answer is 'necessary'. Security Test Labs Experts are the ones that consider more that 'each one needs each other', but still prefer testing facilities than certification frameworks.

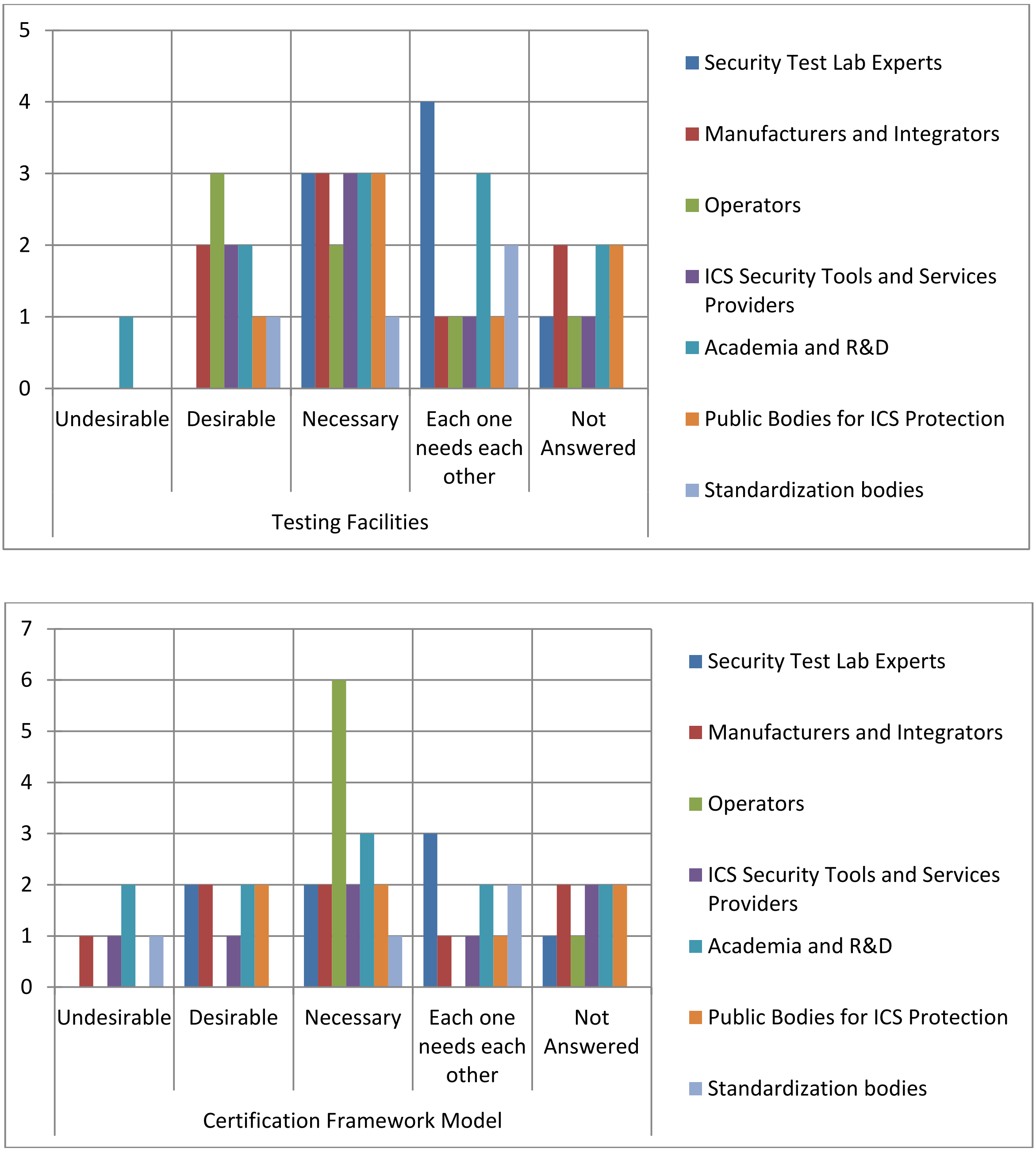


Figure 23: Certification Framework Model vs. ICS Testing Framework by stakeholder type

4.2 STAKEHOLDER ROLES FOR DEFINITION: How do you consider the different Stakeholder Types should cooperate in the following tasks regarding the ICS Test Bed / Framework duties?

This question is referred to the process of Definition and Creation of the Testing Body. The intention is to identify the roles and responsibilities that each stakeholder type is willing or expected to take. In order to leave it as clear as possible, the question was divided in a group of sub-questions, regarding the Definition of the: Objectives (Figure 24), Operational Model (Figure 25), Financial Model (Figure 26) and Technical Resources (Figure 27).

It should be noted that, in general, there are no great differences of share between 'cooperating' and 'consulting' participation for any given stakeholder or duty, so not many conclusions can be obtained in this regard.

4.2.1 Objectives

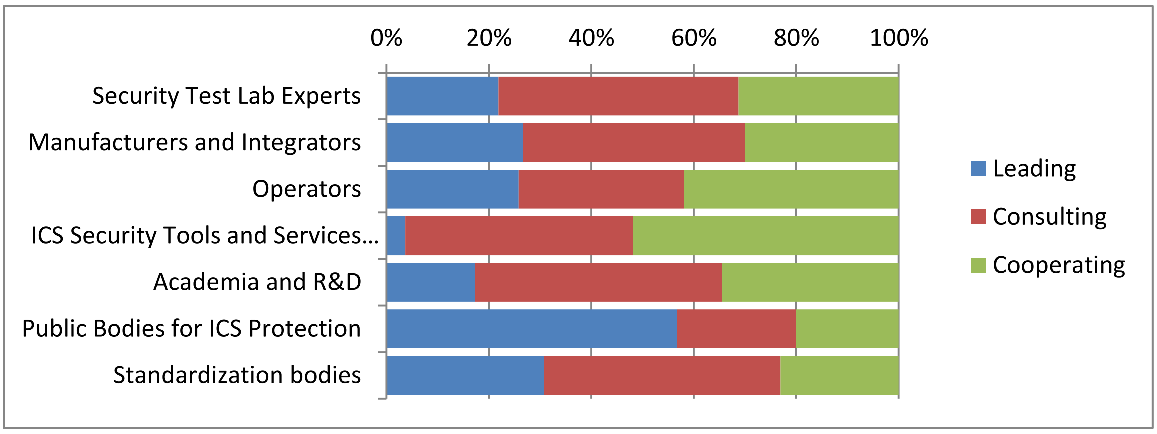


Figure 24: Stakeholder roles for objectives

In order to define the Objectives of the eventual Testing Body, most respondents (almost 60%) have considered that the Public Bodies should lead the actions. And then, in a second level 'Standardisation Bodies', 'Manufacturers', 'Operators' and 'Security Test Lab Experts'. 'ICS Security Tools and Service Providers' are considered mostly for consulting and cooperation tasks, but almost never for leading.

It is interesting to note that 'Public Bodies' are the only ones that voted differently. They do not consider themselves as appropriate to 'lead' these fields as 'Operators', 'Academia' or even 'Security Test Lab Experts'. On the other hand, 'Standardisation Bodies' mostly voted for themselves in order to lead the definition, while the rest of the respondents mostly consider that they should be consulted.

4.2.2 Operational model

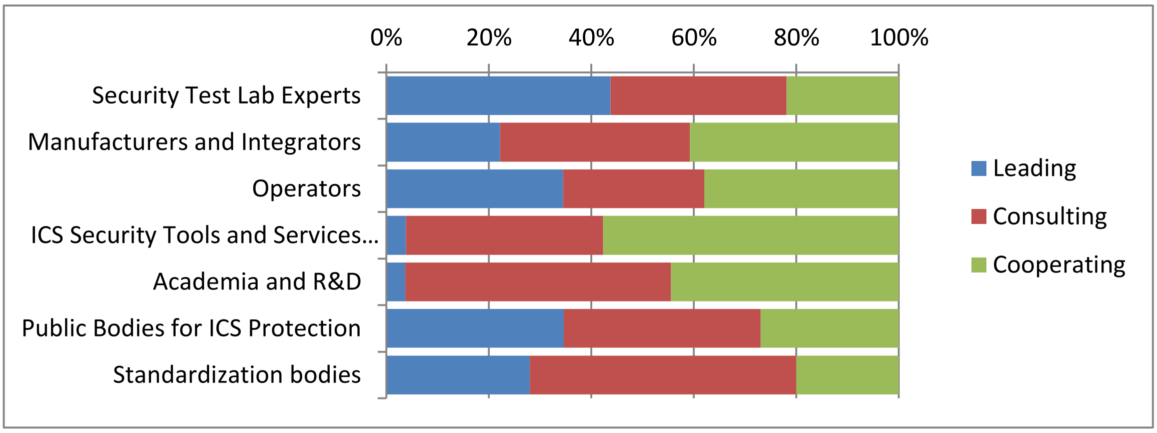


Figure 25: Stakeholders roles for Operation Model

When being asked to define which stakeholder fits better for the Definition of the Operational Model, the most ‘leading’ stakeholder is STLE, closely followed by Operators, PPBB and a step further by Standardisation Bodies and Manufacturers. Academia and ICS ST&SP are mostly considered for consulting and cooperating.

4.2.3 Financial Model

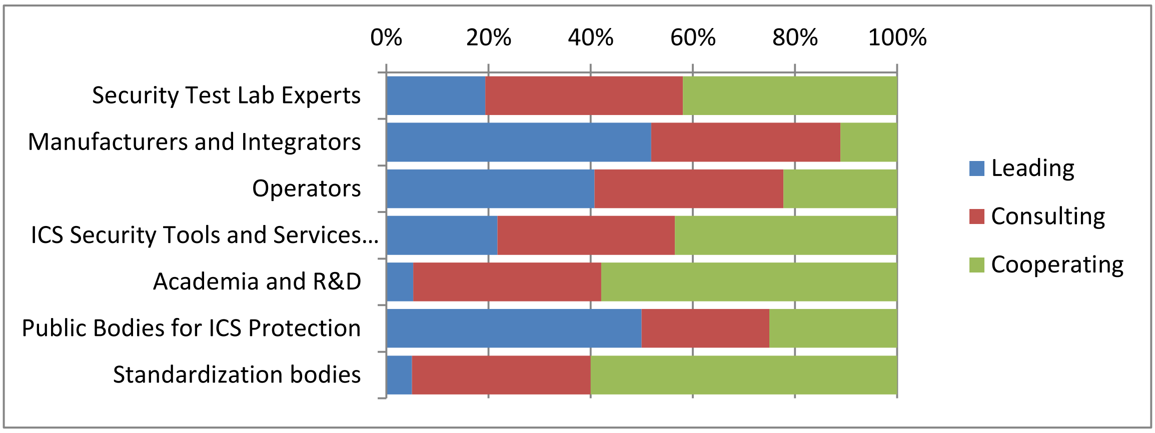


Figure 26: Stakeholders roles for Financial Model

Regarding the financial model the profile of the answers have strong variations. Manufacturers, PPBB and Operators (in this order) are considered to be Leading with rates between 40%-50%. This could be explained because those stakeholder types are usually the ones with more resources, the ones that can perform bigger investments and, hence, take decisions. STLE, ICS ST&SP, Academia and SB, on the other hand, are just considered for cooperating and consulting at this respect.

4.2.4 Technical Resources

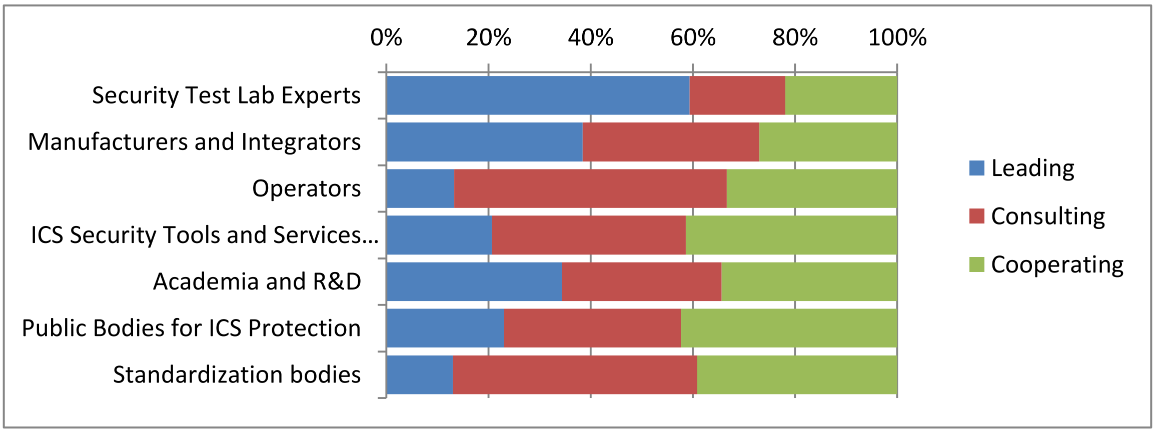


Figure 27: Stakeholders roles for Technical Resources

When being asked about the Technical Resources to take into account, the leading stakeholder is considered to be ‘STLE’, followed by ‘Manufacturers’ and ‘Academia’. ‘Public Bodies’, -unexpectedly- ‘Operators’, ‘ICS Security Tools&Services Providers’ and ‘Standardisation Bodies’ are behind them. In fact, 'Operators' are mainly considered for consulting tasks. This could be due to the fact that Operators are often very biased to focus in the technologies that are using, but do not have a wider vision of the market.

4.3 STAKEHOLDER ROLES FOR OPERATIONS: How do you consider the different Stakeholder Types should cooperate in the following tasks regarding the ICS Test Bed / Framework duties?

In contrast with point 4.2, the intention here is to identify the roles and responsibilities that each stakeholder type is willing or expected to take during the Operation lifetime of the Testing Body. It was also divided into a group of sub-questions, regarding the tasks of: Testing and Result Interpretations (Figure 28), Communications (Figure 29) and Lifecycle and Improvements (Figure 30).

4.3.1 Tests and Results

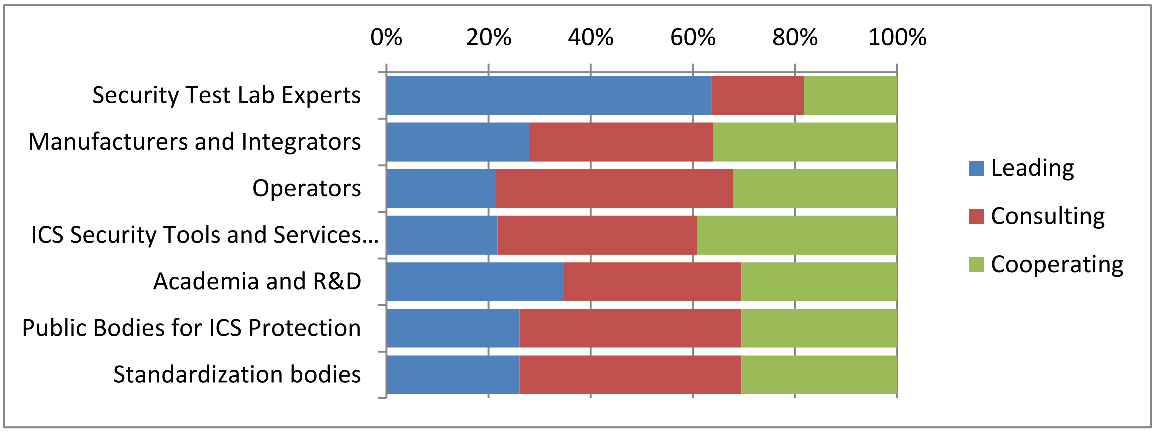


Figure 28: Stakeholders roles for Tests and Results

There is a high agreement for considering STLE as the leading stakeholder for this task. But all others have a significant part on it (more of 20%) and all are taken into account for consulting or cooperating.

4.3.2 Communications

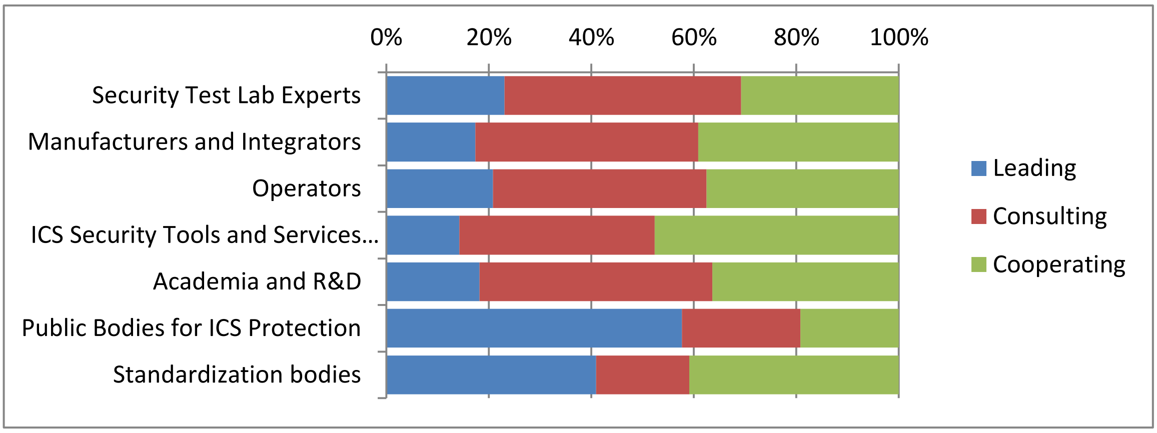


Figure 29: Stakeholders roles for Communications

Regarding communications, the most recognised stakeholders are Public Bodies, with almost 60% of the votes, and followed closely by Standardisation Bodies. All the rest are considered for consulting and cooperating tasks.

4.3.3 Lifecycle and Improvements

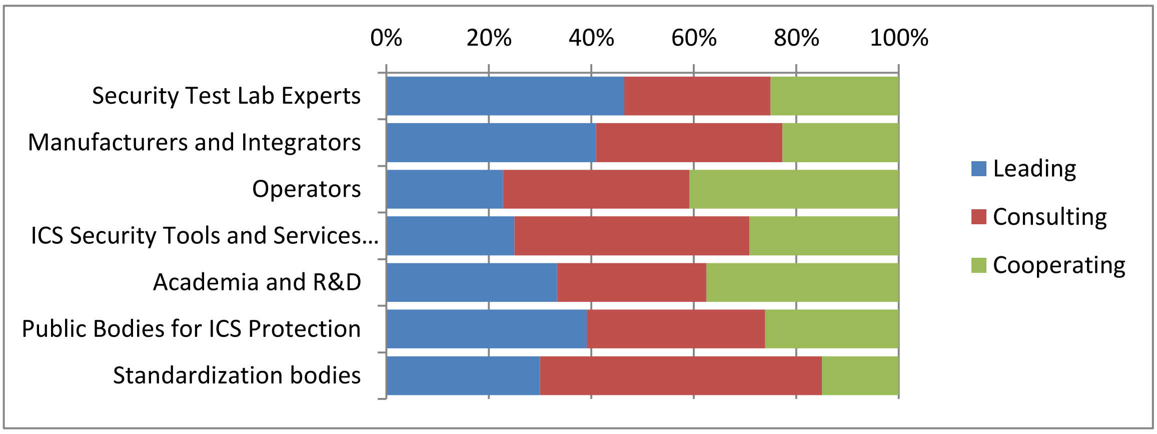


Figure 30: Stakeholders roles for Lifecycle and Improvements

In this case, results show more balance. STLE is still considered to be the ‘leading’ group, but Manufacturers and Public Bodies are considered to be much implicated. In fact, every Stakeholder type is expected to keep some degree of leading or cooperating responsibility.

4.4 SLAs: Which ones do you think are the most necessary SLA metrics to consider between the Test bed and their Customers?

Experts were In order to get some metrics related to the Service Level Agreement that could be interesting for the stakeholders, two options were provided ‘Time to get results for specific matter’ or ‘Time to Certificate’ (Figure 31), but some other possibilities were expected through open text fields and interviews.

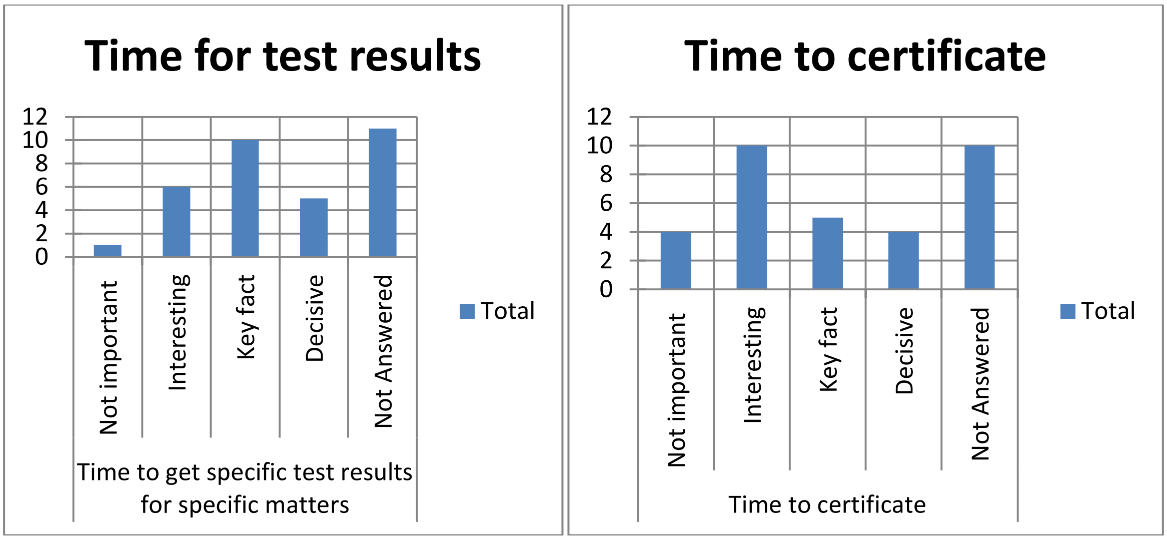


Figure 31: Most necessary SLA metrics for test results and for certification respectively

Regarding the default answer, 'Time to get test results for specific matters' is mainly considered a Key Fact, or 'interesting' rather than decisive. This is the opinion shared from most stakeholders, being the only ones to find it decisive the ones from STLE or Academia.

The 'time to certificate' is considered mainly 'interesting', and just as many experts find it 'decisive' as 'not important'.

In the open answers, several other points arose such as, being 'technical validity', 'relevance' and 'actionable findings based on results' as the most important points.

4.5 MEASURES FOR SUCCESS: Which ones do you consider should be the Measures of Success for this Framework / Test Bed?

Some measures of Success for the Testing Body have been intended to be sketched with this question. Three possible answers have been provided 'Acceptance of the results', 'Speed of the results', and 'Comprehensiveness of tests'. Respondents have been prompted to rate each one from '0 – Not important' to '3 – Decisive'. Total results are as given (Figure 32):

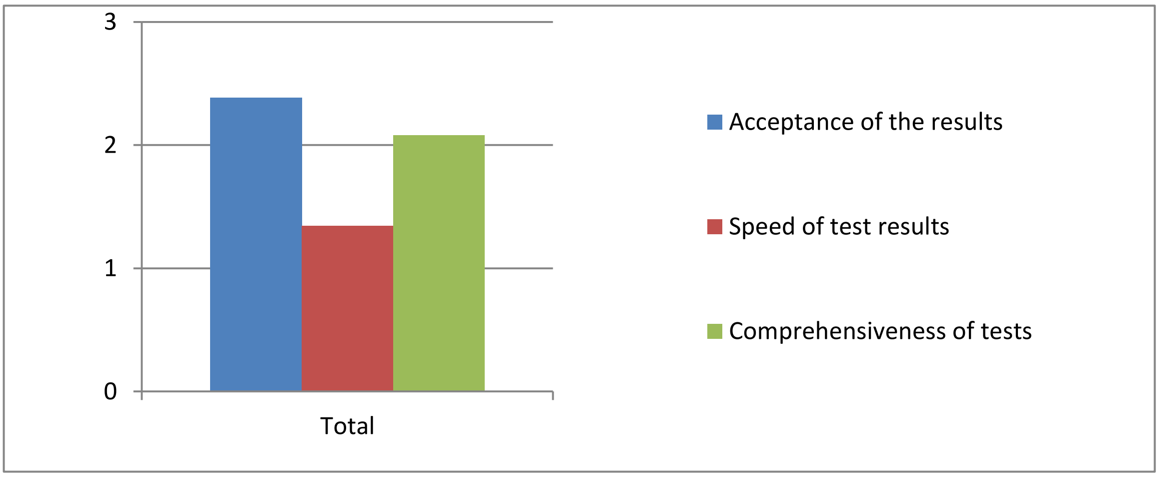


Figure 32: Measures of success

This means that ‘Acceptance of the results’ is considered the most important measure of success, followed closely by ‘Comprehensiveness of test’. How fast the results are provided is considered far less important than the aforementioned.

Checking the results by Stakeholder Type (Figure 33), it is clear that the profile of the answer is similar in almost all cases (except ‘Public Bodies’, that consider ‘Comprehensiveness of tests’ as the most relevant one). But it is interesting to highlight that, for ‘Operators’, all three topics are almost equally important.

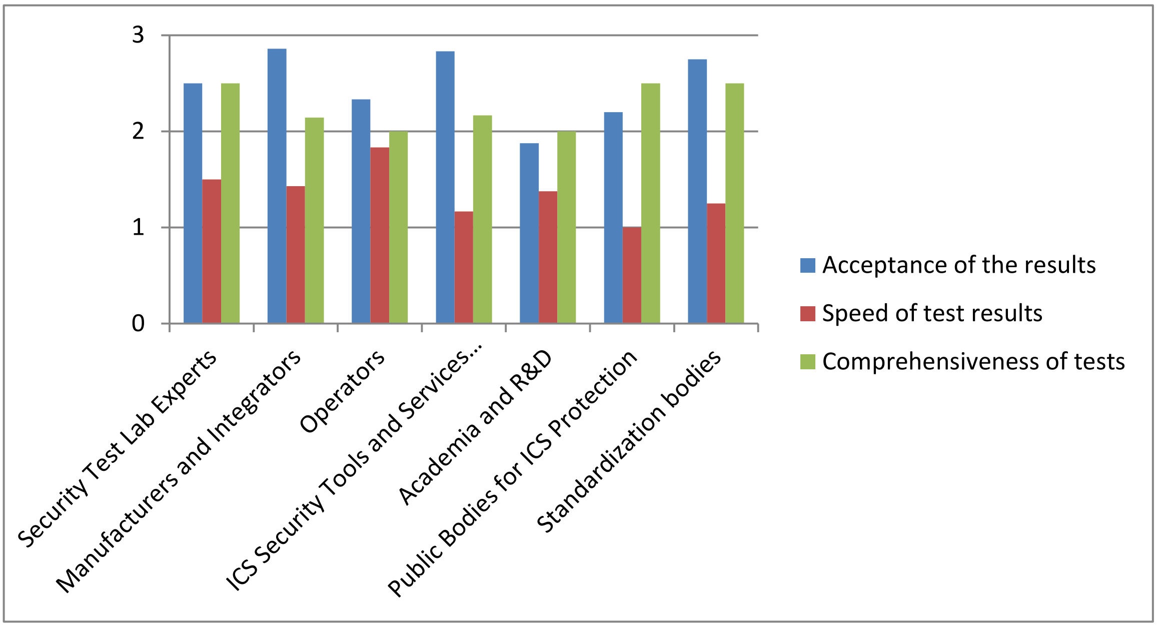


Figure 33: Measures of success by stakeholder type

During the interviews and open answers, many experts have emphasised the importance of ‘trust’, and some also have explained that there must be a compromise between comprehensiveness and speed. Automating the most repeatable controls can help to maximise the quality and decrease time.

4.6 CENTRALISED vs. DISTRIBUTED: Regarding Centralisation vs. a Distributed model, how do you consider the Test bed should be put into place?

This question is intended to understand if a centralised or a distributed model is more interesting for the eventual Testing Body (Figure 34).

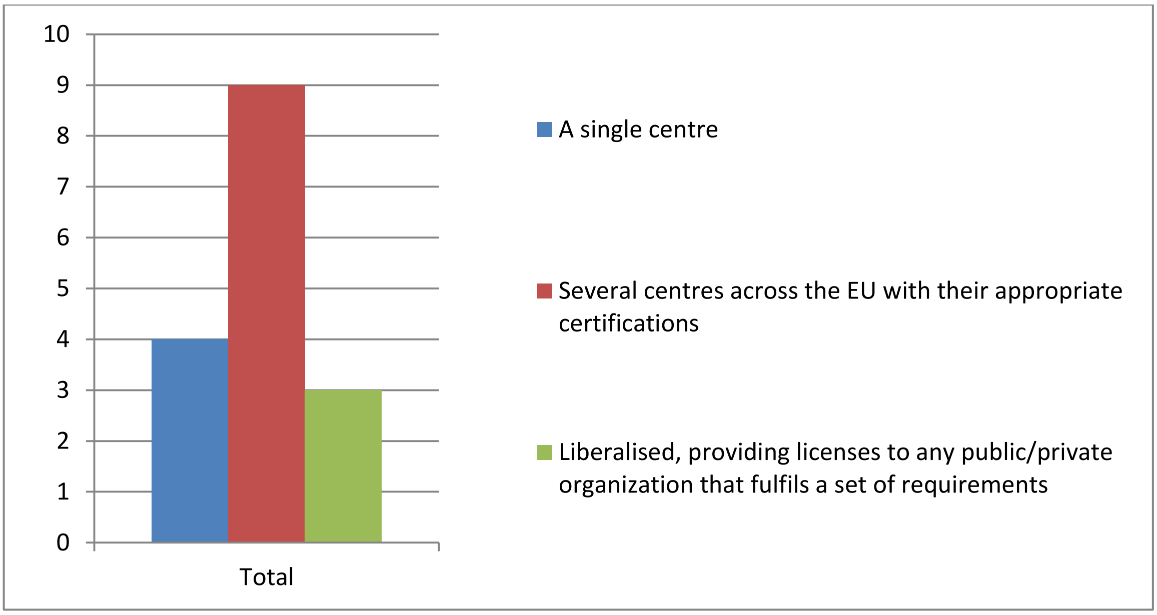


Figure 34: Degree of acceptance regarding Centralisation vs. a Distributed model

The most repeated answer was ‘Several Centres Across the EU’ with more than the 50% of answers. ‘A single centre’ has had some votes (from ‘Manufacturers’, ‘ICS ST&SP’, ‘Operators’ and ‘Standardisation Bodies’) and only a few ‘Security Test Labs Experts’, ‘Manufacturers’ and ‘ICS Security Tools&Services Providers’ consider that it should be liberalised by providing licenses (Figure 35).

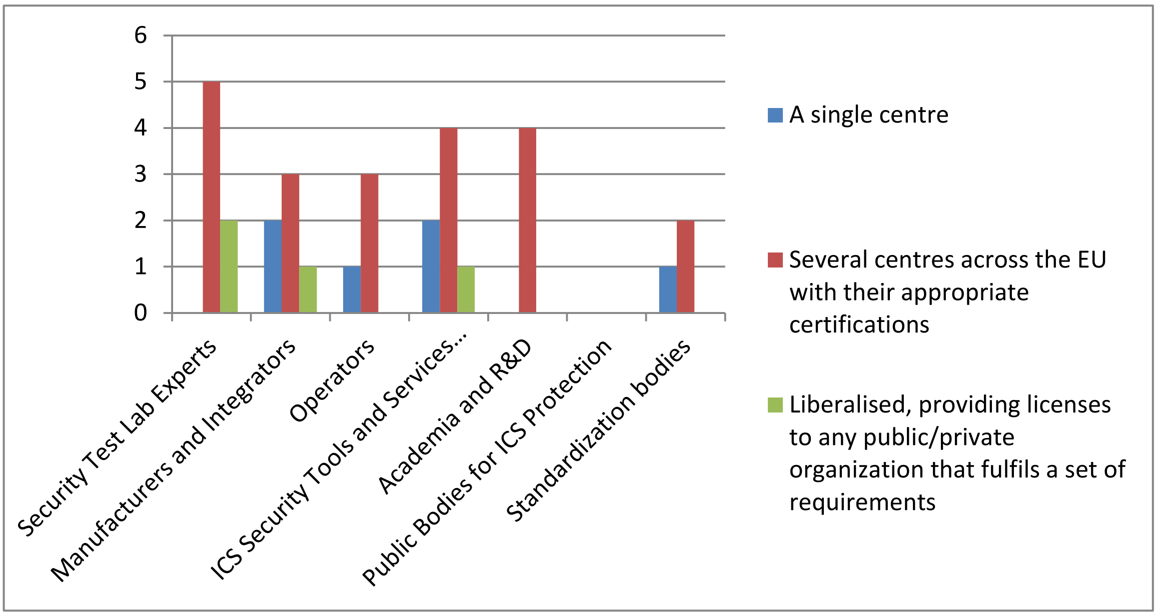


Figure 35: Degree of acceptance regarding Centralisation vs. a Distributed model by stakeholder type

To understand the reasons it is necessary to focus on the interviews. A wide majority of experts have stated that a Distributed Model will be much more adequate for the EU complexity that could take advantage of its own size.

Different reasons have arisen, such as:

- closeness to the industry,
- differences in legislation or specific needs,
- possibility of developing 'centers of excellence' for concrete purposes

In almost every speech, they have warned about the need for 'synchronizing' already existent efforts, making 'consistent tests', not lowering standards and, for foreign experts, having a clear 'gateway organisation' as interlocutor.

In most cases this is linked directly to an 'Accreditation Model' in which a superior body (some even referred to ENISA) could accredit centers to perform the tests, as it is already been done in other industries.

4.7 SEGMENTATION: If the test bed could be segmented into a series of tasks, stages, workflows or others, what kind of criteria do you think would be more useful?

This question has been set in order to determine if some kind of segmentation model could be used in order to specialise between different centers. Very few experts have answered to this question, so the validity of the results is doubtful.

In any case, it seems that there is some preference, in case of segmentation, of doing it by business (Figure 36).

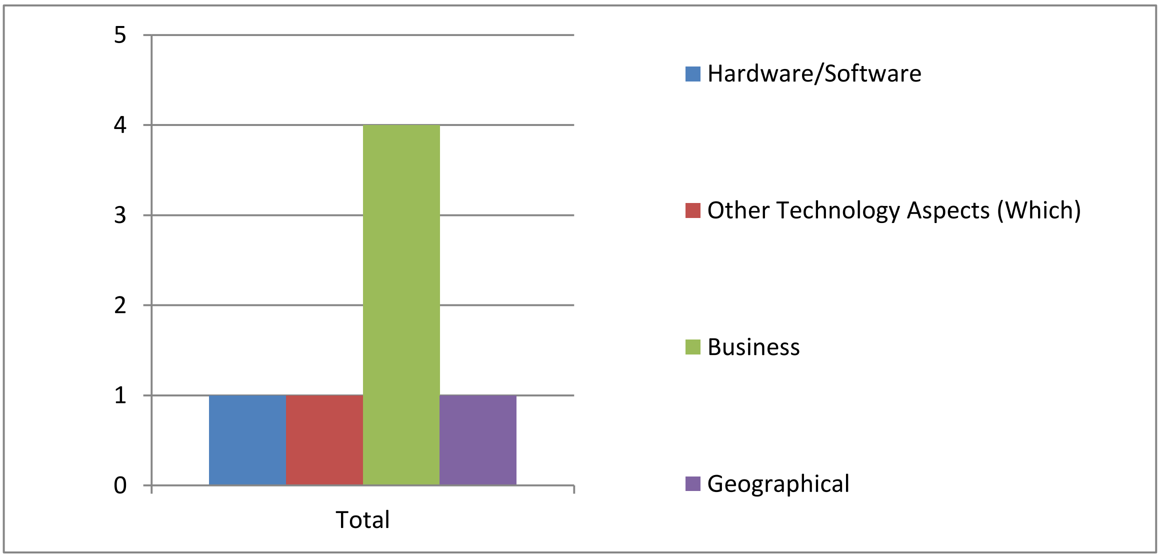


Figure 36: Degree of utility of the different criteria to segment

5 Resources

5.1 FINANCIAL MODEL: In your opinion, what should be the economic model for this eventual Test Bed?

This question asks about four different economic models to support Test beds: ‘100% Public’, ‘100% Private’, ‘Public Entities invest in creation and Private Parties pay for use/certification’, ‘Public Private Partnership in both creation and operation’, to be rated from ‘Strongly disagree’ to ‘Strongly agree’.

According to the ratings (Figure 37), the financial model that fits better with the current social-economic conditions is the public–private partnership (PPP), in both the creation of test bed infrastructure and use of its methodologies such as usage services offered by it. The average rate of this response was above the ‘Agree’ level. The answer ‘Public Entities invest in creation and Private parties pay for use/certification’ also had a good level of acceptance. ‘100% Public’ had a slightly positive rating, but it can be considered that it has as much support as opposition. It is important to say that all respondents consider ‘100% Private’ option as the worst, with an overall rating equivalent to ‘Disagree’.

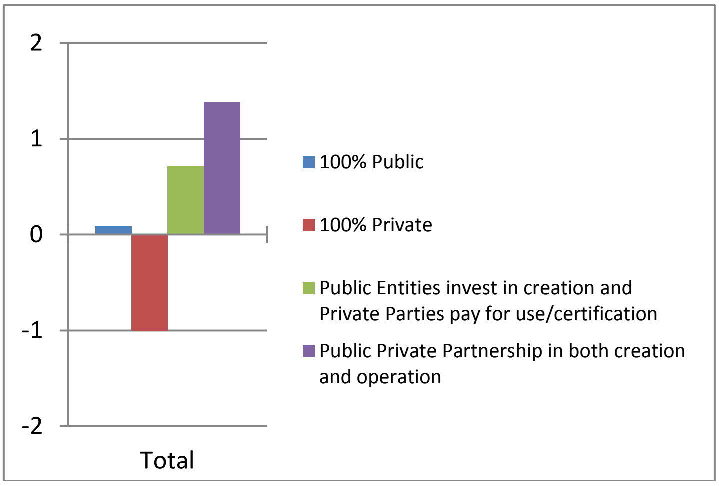


Figure 37: Financial model

Below are shown the graphs of the acceptance of each financial model regarding Stakeholder Types and Sectors (Figure 38).

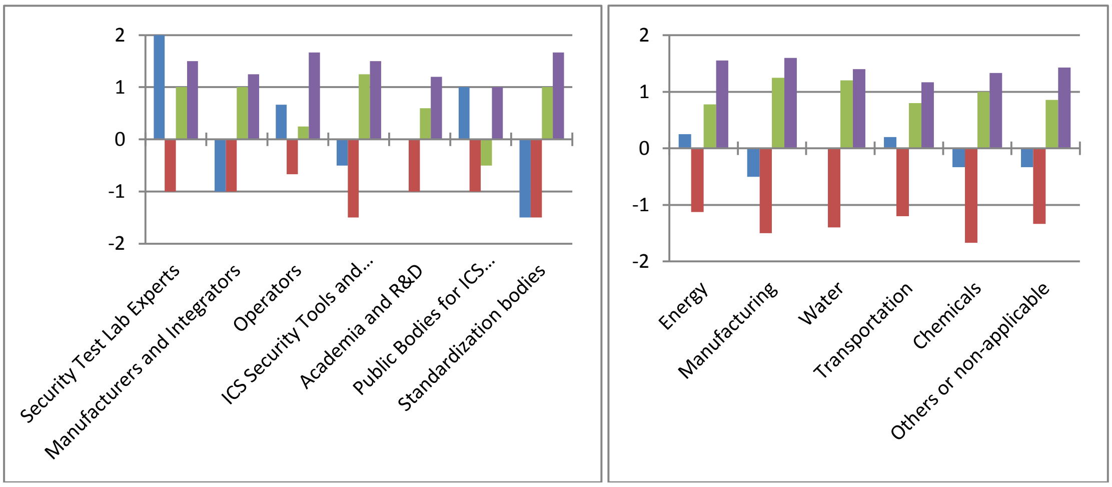


Figure 38: Financial model by stakeholder type and by sector respectively

In terms of stakeholder type, in general terms they all have the same opinions regarding the economic viability of the PPP model. It should be noted that the controversial '100% Public' suggestion has full support from the 'Test labs security experts' and also positive ratings from 'Publics Bodies', and 'Operators', while 'Manufacturers', 'ICS Security Tools&Services Providers' and, especially, 'Standardisation Bodies' are 'against' it. If the results are divided by sectors, they are very homogeneous, without important differences between them.

It is noteworthy that some of the experts asked about the economic model feasible for creating a test bed, reiterated that the use of these test beds must be imposed by mandate because if a complex test bed is created and its use is optional, the money invested will be wasted. Some others consider that it is not realistic to expect private investments to fully build such utilities, so that public funding is necessary, but there is no reason not to involve private parties when it makes sense, provided that integrity and impartiality is assured.

A few experts explained how the model works for the NSTB-INL in the USA or the CSSC in Japan. The financial model of the first has changed over time and is now less dependent on public funding[6] as the results of the tests are provided only to those that pay for them. The CSSC started out, as the NSTB did, with a massive participation of public funding and it is likely to shift to a more balanced PPP model over time. In fact, some experts consider that, to guarantee stability, public participation in the early stages of the initiative is critical.

5.2 EXISTING FRAMEWORKS

Questions about this topic were asked only of interviewees, so the amount of raw data is lower and most of the information is unstructured but deeper.

5.2.1 Do you have any knowledge about existing ICS Test Beds such as INL or SANDIA Labs (US) or the ICS Sandbox (Montreal/Brazil)?

All interviewees were, at least, aware of existing Test Beds. Some have had closer connections with them and five of them are members of one of them. This question was interesting in order to understand the perspective from which interviewees were talking, but no conclusions can be drawn from it.

[6] Although it still belongs to the Department of Homeland Security of the USA.

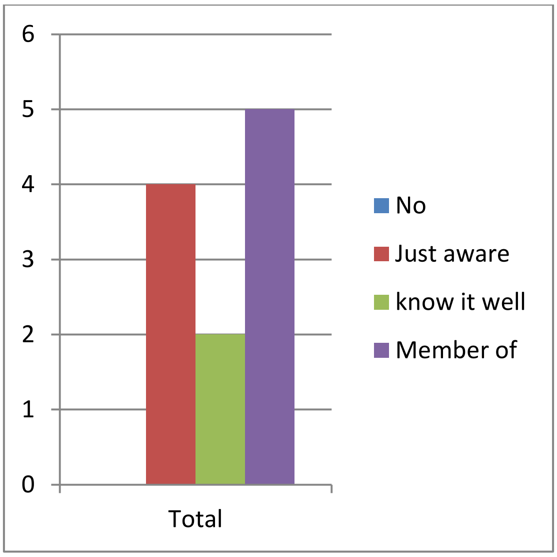


Figure 39: Degree of knowledge about existing ICS Test Beds

5.2.2 Which aspects do you think are 'reasons for success' and which could be improved?

Interviewed experts consider that, nowadays, the most mature and relevant Test Bed in the world is the National SCADA Test Bed from Idaho National Labs in the USA. When experts were asked about the reasons for its success several points were raised, although there was no consensus among them all:

- The NSTB has great financial and technical resources. This is mainly due to the considerable support that they had from the government at the beginning and, even now, there are people committed to the point of taking 'political risks'. Many experts relate this to the 9/11 incident.
- For some experts, even more important than that, is the fact that they have some of the best experts in the world, with great understanding of their problems, and the ability to share this knowledge through education (both internal and external).
- It has been able to gain confidence from all relevant stakeholders for several reasons:
  - Their results are valuable for their customers (whether public or private organisations).
  - They handle sensitive information carefully, for example through vulnerabilities disclosures.
  - They try not to become a market driver by publishing 'security classification' of products or any kind of comparative chart.
  - They are considered 'independent' from private interests.
- They meet the expectations regarding certification. The cost and time-to-market is reasonable considering the complexity and value of the results.
- The previous reasons make stakeholders (especially vendors) very cooperative. At the beginning of their activity, some stakeholders (especially vendors) were reluctant to cooperate because they thought they would lose sales if bugs were detected. This did happen, at the beginning. But, later on, consumers started to ask others why they were not being tested and the market driver worked in the opposite direction.

Some caveats about this model are:

- The funding model has changed a lot in the last few years, and is now more dependent on private money; the organisation's independence is starting to be questioned by some customers and experts. Many would like to have alternatives.
- In terms of cooperating with the EU, it is important to understand that the Department of Homeland Security of the USA has its own agenda and will not share some of their knowledge.
- As there are so many ICS technologies in the market, it is not always easy to determine which has to be tested to improve overall security.
- They are still dependent on the ability of the expert that conducts the tests, for example in penetration testing. Results are not homogeneous even within the same team.
- They lack the ability to enforce resolutions when organisations are aware of them and take no measures to solve the problems.

Members from two other emerging bodies have been contacted:

- The ICS Sandbox in Brazil and
- The CSSC in Japan.

Regarding the ICS Sandbox in Brazil:

- It is a PPP in cooperation with the ICS Sandbox in Montreal that has just started, so there is no much information regarding 'success' or 'problems'.
- It is not only about simulating vulnerabilities and risks, but also about everything else to be protected. What would happen (in society, in number of lives, in the economy) if a Critical Infrastructure suffers a successful attack. This is something innovative.
- Their economic model is such that private companies (usually vendors) are the 'sponsors' that pay for some particular 'testing setup'. Not all stakeholders are equally involved in their Organisational Board. In order to preserve the body's independence, vendors are just sponsors that provide knowledge but do not take part in the ICS Sandbox decisions. This is considered to be a difficult balance.

And regarding the CSSC in Japan:

- The CSSC has a very deep connection with the INL. They get a lot of support from them. Researchers follow the INL training (in the near future, the idea is to have their own training, with the same scheme). They have the same policies to design facilities.
- Also, like the initial INL, it gets most of its funding from public budget as they have from MEPI in order to keep independent. Private organisations want to invest in testing because the costs of R&D in cyber-security are very high if they do it on their own. Having a public, common, Testing Infrastructure helps them economically. But it is always the Government that promotes the activities and retains leadership.
- The project started after the Stuxnet issue because Japan has similar nuclear facilities to the Iranian ones. But the budget increased after the Fukushima disaster. Some of the reconstruction budget was used to create the CSSC.
- They have tight links with the JP-CERT and the AP-CERT (Asia Pacific).

In the answer to this question several other initiatives were described; they are discussed in 'Annex II: ICS Security Testing Related Initiatives'.

5.3 ASSETS: What kind of assets or infrastructures do you think are necessary for testing environment?

This question was only put to the interviewees, and not all of them, so number of answers is lower and conclusions to this question could be biased or partial. In any case, experts who did answer are relevant enough to consider their opinions (Figure 40), as they have a clear vision of building a test bed, and testing environments to keep as real as possible. Interviewed stakeholders highlighted that no environment must be tested in production systems if avoidable. Preproduction and, with some concerns, virtualised environments are more desirable. Due to the criticality of these environments, doing tests with exactly the same elements[7] as those actually used is the best option.

When stakeholders were asked about assets that should be taken into account on test bed infrastructure and their importance level, they tended to consider every element as 'Decisive' or 'Added value'. According to the interviews, this is understandable because some experts consider that it is dependent on the criticality of the device in the system (as seen in 3.4). The only exception to this are the 'Virtualisation environments' that, as explained, cannot be always suitable for testing.

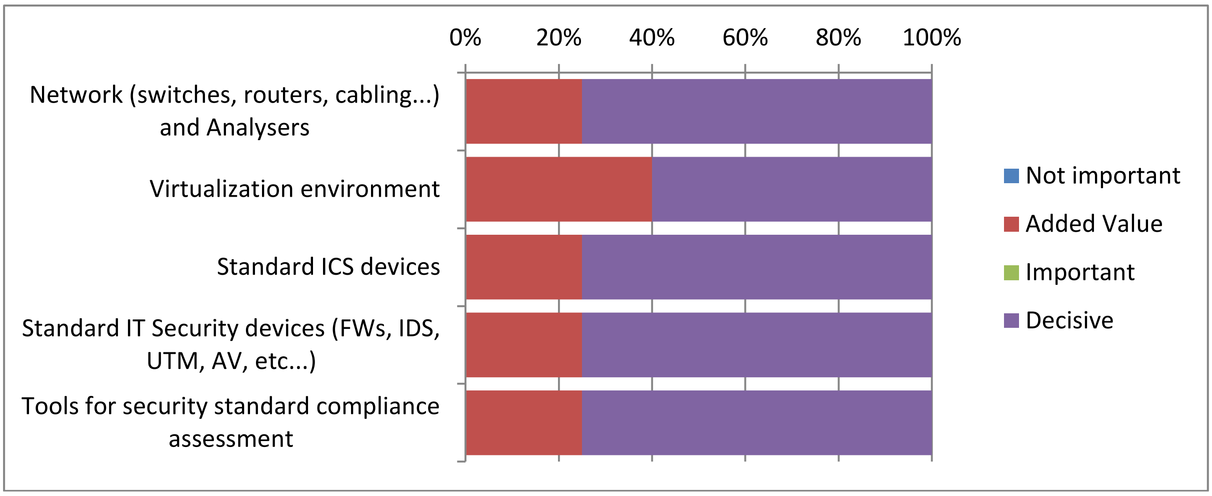


Figure 40: Infrastructures necessary for testing environment

During the interviews, many experts pointed in the direction of performing 'Holistic' approaches as discussed in point 3.3 checking for the whole ICS infrastructure implanted. Something probably smaller and designed for versatility is more realistic than big investments.

It is interesting to see that experts who prioritise 'single device testing' are usually the ones more concerned about security certification in the debate explained in point 4.1.

It is also noteworthy that, when stakeholders were asked about the assets needed for the creation of the eventual Test Bed, a large number of them emphasised that human assets and their knowledge of the ICS security subject is the most important in this environment.

[7] Including configuration, firmware, etc.

5.4 SKILLS: What kind of skills must have the staff in this eventual testing environment?

In this question, posed only to interviewees, they were been asked about which of the skills are more important (Figure 41): ‘Vulnerability Assessment’, ‘OT Technology Expertise’, ‘IT Security Expertise’, ‘Ethical Hacking skills’ or ‘Skills in very specific OT technologies Manufacturers/Business’.

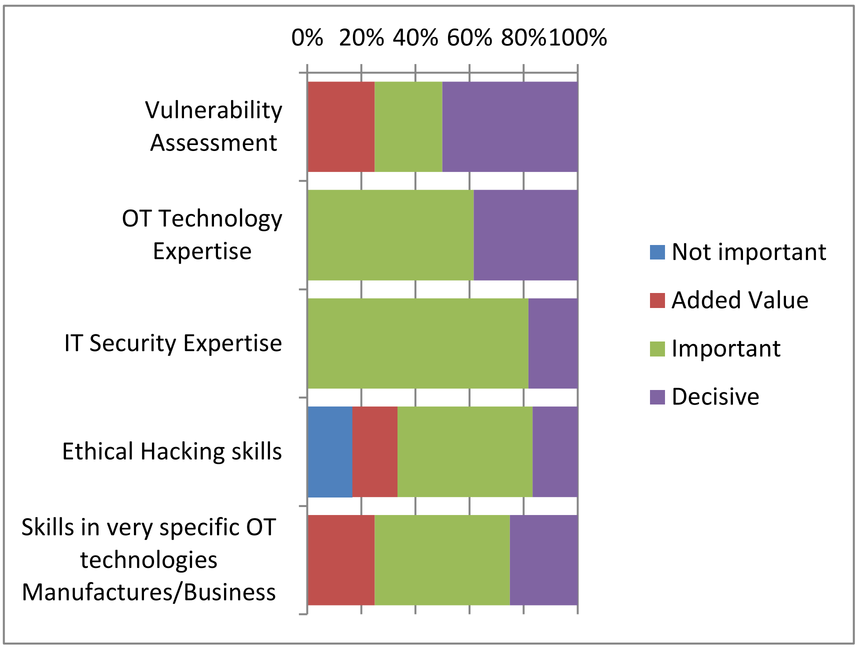


Figure 41: Staff skills

All experts stressed that the most desirable staff skills fell somewhere between ‘IT security expertise’ and ‘OT Technology Expertise’. Some experts felt it was unlikely to find enough individuals owning such knowledge in both fields, so they prefer the creation of talented groups; each person making up the group has certain skills and adds to the other members. If these groups of experts were given independence in their work, they would end up soaking up the skills of their peers and they could do a risk analysis and vulnerability job much more effectively.

There is also a debate regarding ‘ethical hacking’ and other ‘creative’ abilities. Some experts consider that, if the Testing Body has to grant acceptance of the results, they should be homogeneous and reproducible.[8] But, as specially STLE state, security risks are changing continuously and some level of creativity and variety is indispensable. To reach an agreement between both approaches could be one of the keys for success.

6 Constraints

This group of questions were asked in both questionnaires and interviews, with a high rate of participation. Several ‘areas’ of constraints were defined and, for each one, three or four aspects were proposed, to be rated from ‘Trivial’ (0) to ‘May not be possible’ (5). All questions had a free text space for respondents to explain other options or to give more detail on answers. Some respondents just answered by checking options, without providing clarification in ‘open fields’, but the answers received during the interviews were valuable enough to get conclusions.

[8] Especially in a Distributed Model of organisation.

As a general rule in all questions of this group, all presented options were evaluated at least at the 'Difficult' level by stakeholders, both respondents and interviewers. The conclusion to these results is that the creation of such a Testing Body has to overcome many challenges.

6.1 ORGANISATIONAL: Which limitations do you consider would be the most challenging from an organisational point of view?

This question asks about four different topics to specify the level of challenge to apply to each one (Figure 42). In general, all stakeholders identified 'Differences between how technologies are applied in different ICS environments or Businesses' and 'Building trust among every kind of Stakeholder' with, at least, 50% 'Very Difficult' rates or high. The last topic is the most challenging to stakeholders, as more than 80% consider this option to be 'Difficult' or more. In fact, it is the only one with some votes on the 'May not be possible' option. It is also interesting to note that for all topics some stakeholders marked the 'Trivial' option.

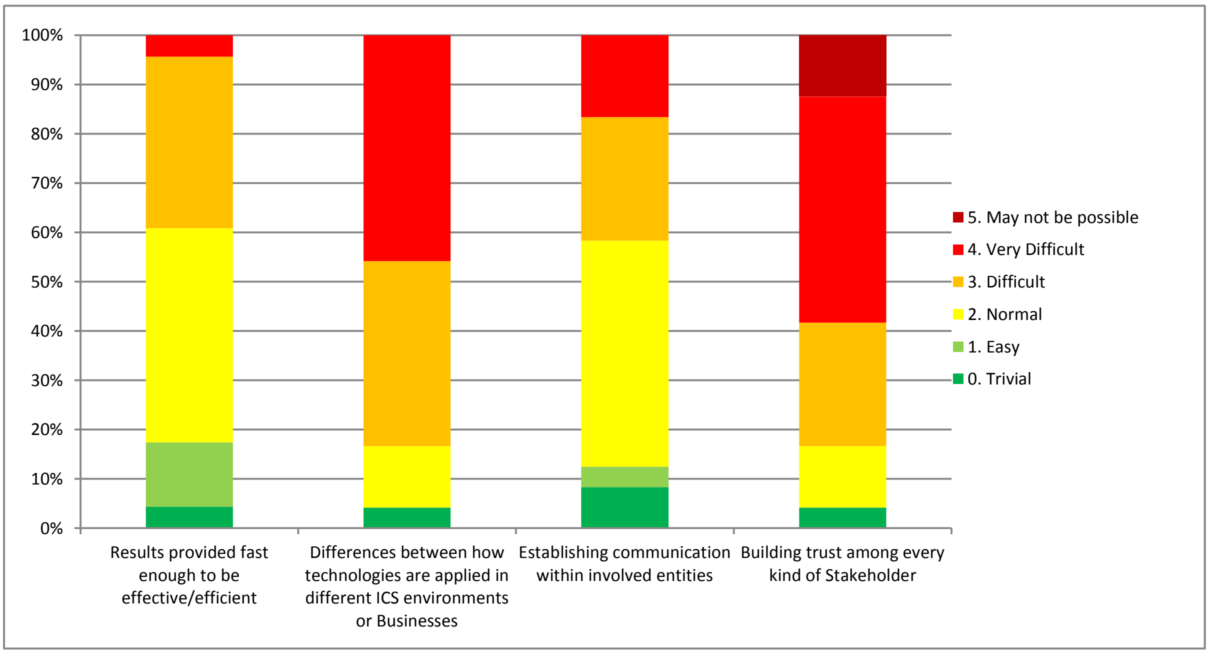


Figure 42: Most challenging limitations from an organisational point of view

'Providing results fast enough' was mainly considered of 'normal' difficulty, and 'Establishing communications within involved entities' was perceived, in general terms, as just slightly more difficult.

'Establishing communication within involved entities' was the topic showing most differences by stakeholder type (Figure 43). 'Security Test Labs' experts and 'Academia and R&D' rated it as 'Trivial' or 'Normal', meanwhile other stakeholder type rated it 'Normal', at a lower level, but with many responses in 'Difficult' and even 'Very difficult' options.

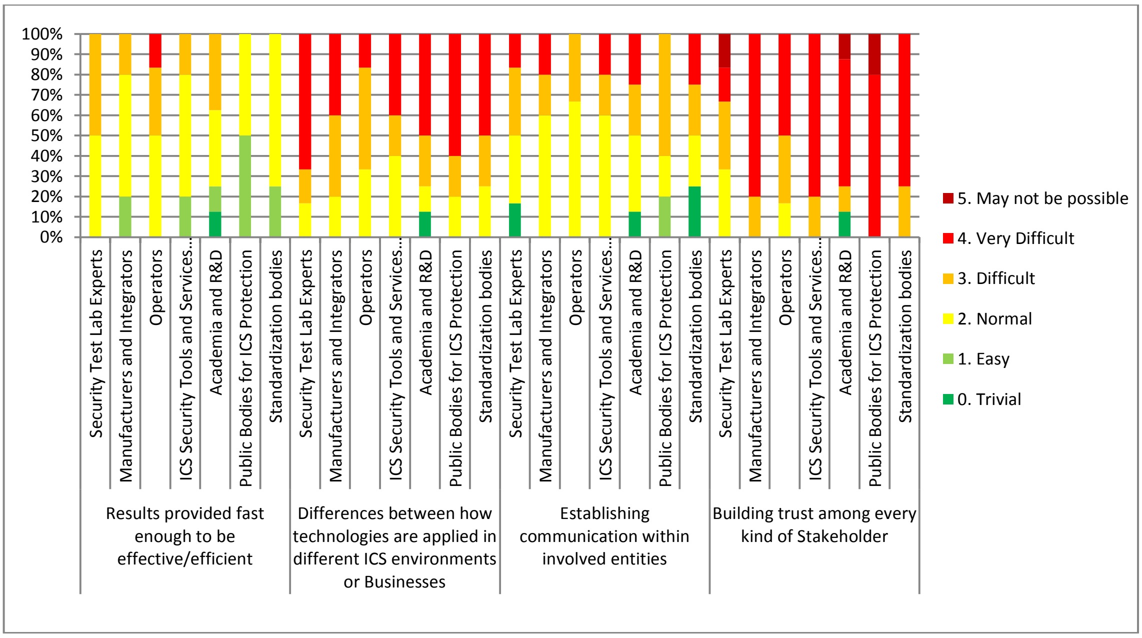


Figure 43: Most challenging limitations from an organisational point of view by stakeholder type

Interviewed manufacturers and Integrators exposed their reticence about the feasibility of building trust, especially concerning Vulnerability Disclosures. Their opinion is that vulnerabilities must be published with a delay, of a few months for example, and that some kind of 'arbiter'[9] must be in charge of building trust using their authority and legal agreements.

Some experts are optimistic about the potential for building trust because some experiences have already achieved it (see 5.2.2), there are NDAs and, also, because stakeholders need each other. In such a complex environment as the EU such an organism could help to make the situation simpler. A few experts think that understanding will be easier among technicians than at senior management levels, where strategic goals and competition have more importance.

A few experts explained that there are about six big vendors worldwide. According to some, these Big-6 companies are indispensable to the project and it is essential to make them feel part of it. If one company gets too much influence, the others will stand apart. On the other hand, some other experts with experience in cooperating initiatives say that it is very risky to allow independent companies to be included directly in the Testing Body decision organisms. They strongly recommend allowing participation only from representatives of groups, consortiums or initiatives, as they will have less economic interest.

One expert noted that there is a risk because if the activity performed by labs is perceived as 'a set of tests', then things could be made for the minimum, somehow 'lowering' the standards of quality.

Another expert do not consider it so important whether someone or something was certified or not; he believed that it is more interesting to indicate when it is reasonable or not to use a product; because safety conditions can be different and security capabilities can vary depending on countermeasures.

[9] Usually they speak about Public Bodies and CERTs.

6.2 TECHNICAL: Which limitations do you consider would be the most challenging from a technical point of view?

For this question, the questionnaire had four proposals: 'Diversity of technologies involved', 'Differences between how technologies are applied in different ICS Business/Environments', 'Vulnerability databases accuracy or time to update' and 'Limitations in virtualisation technologies'.

Respondents coincide in rate responses (Figure 44), finding the first one the most challenging with more than 80% of responses at the 'Difficult' or 'Very difficult' level; decreasing to the last one, with almost 60% of responses at the 'Normal' or lower level, and 10% regarding the issue as 'Trivial'.

It is interesting to note that the first option, 'Diversity of technologies involved', recorded these results due mainly to 'Security Test Lab Experts' answers. 'Operators' and 'Public Bodies for ICS Protection' answered the different options in very similar percentages. The 'Academia and R&D' experts group is the group that accounts for most of the 'Trivial' and 'Easy' answers, except for the last option.

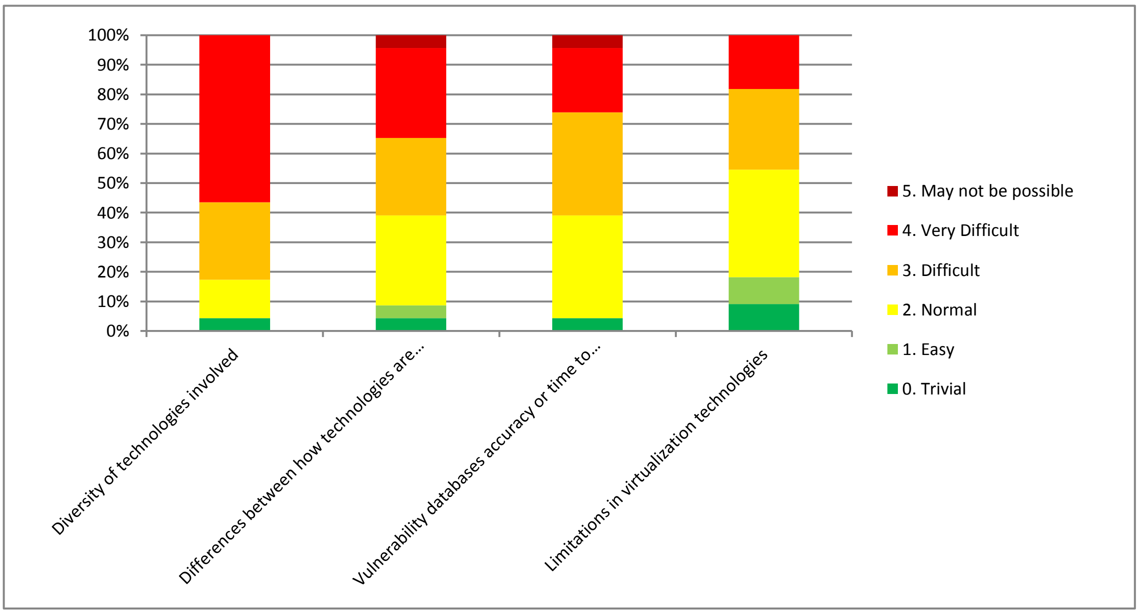


Figure 44: Most challenging limitations from a technical point of view

Interviewees highlight that the variety of products is an important problem and a challenge from a technical point of view.[10] They say that there are many manufacturers but just four to six really big vendors that provide services to any operator, and they have to be involved (see 6.1).

6.3 METHODOLOGICAL: Which limitations do you consider would be the most challenging from a methodological point of view?

In this case, respondents qualified all options (Figure 45), 'Limitations of existing methodologies', 'Difficulties to develop cross-environment methodologies' and 'Agree about the security criteria'; with very similar values. All of them had about 30% of responses at 'Normal' level or lower, more or less another 30% as 'Difficult' and about 40% 'Very difficult' or higher. Last topic, 'Agreement about security criteria' was considered the most challenging, with 20% of responses in 'May not be

[10] Although, as one expert noted, 'all technical problems can be solved with time and money'.

possible' option, but the percentage of results with 'Normal' difficulty or below was very similar in all topics at about 40%.

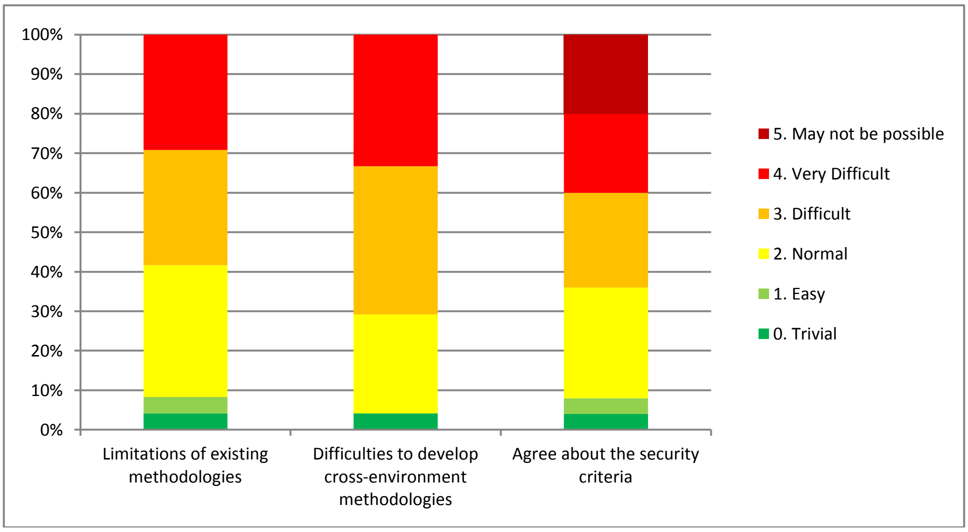


Figure 45: Most challenging limitations from a methodological point of view

If Sector and Stakeholder division is taken into account (Figure 46 and Figure 47), only members from 'Academia and R&D' rated topics as 'Trivial', and these people are classified in 'Others or non-applicable' sector. There were some responses at 'Normal' level, but they are very few. The rest of respondents considers all topics at least with 'Normal' difficult level.

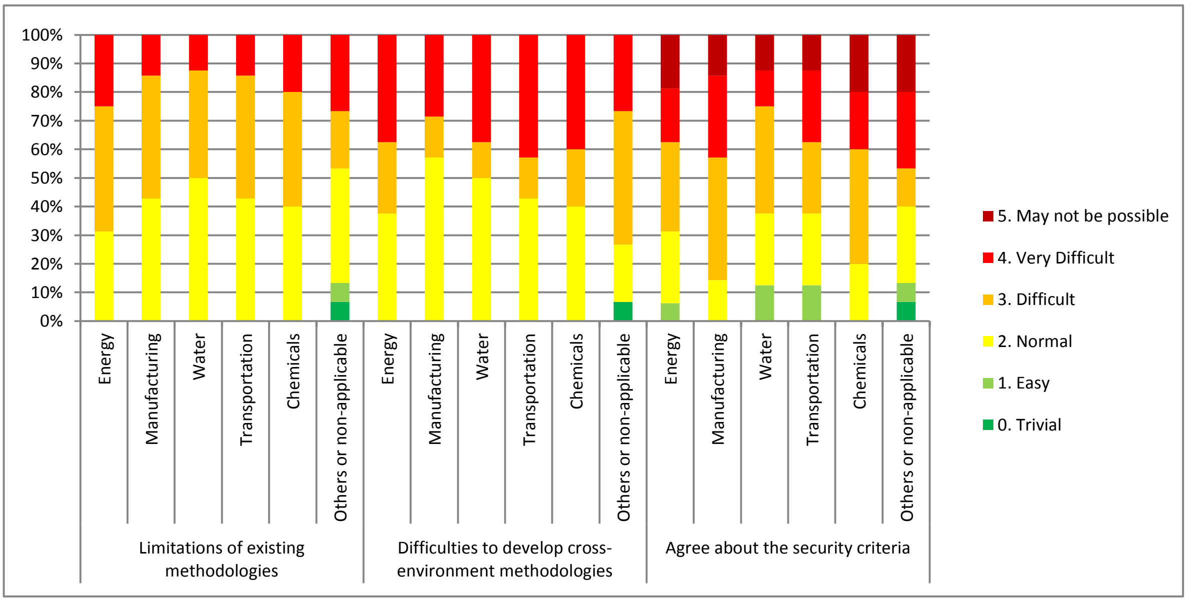


Figure 46: Most challenging limitations from a methodological point of view by sector

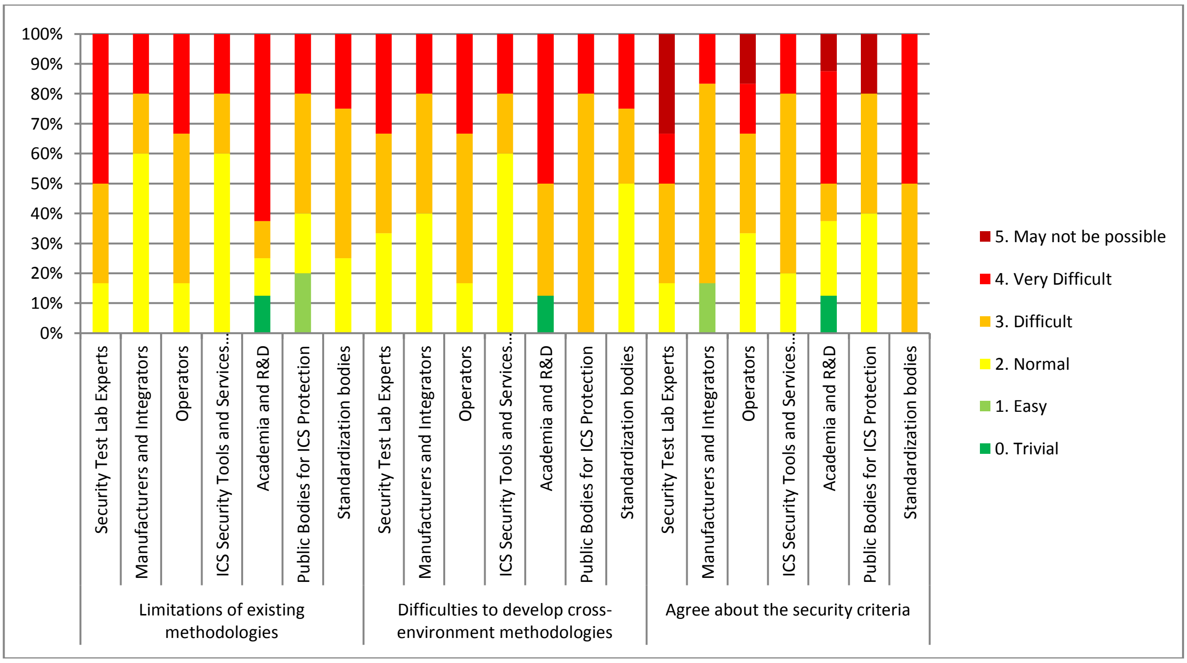


Figure 47: Most challenging limitations from a methodological point of view by stakeholder type

Interviewers gave greater detail in their responses and their general opinion was that 'Agree about the security criteria' was the most difficult criterion to meet. An expert highlighted that getting full agreement cannot be an objective of important standards, and he explicitly said 'We never did it in the ISA-99'.[11]

6.4 LEGAL & REGULATORY: Which limitations do you consider would be the most challenging from a Legal and Regulatory point of view?

In this question, stakeholders were asked about four different topics about laws and practices carried out in Europe. Results (Figure 48) obtained for 'Differences between countries' and 'Differences between environment legislations' topics are quite similar. These two questions are very similar and many stakeholders could have interpreted the questions in the same way. 'Laws and regulations too open for interpretation' is the option most rate as 'Normal', with 50% of responses in this level. 'Unclear limits of legal/illegal testing practices across Europe' was the option with more 'Easy' votes. These last two topics received similar votes too.

[11] Which is, in fact, the main reference within the interviewees as seen in 2.2.

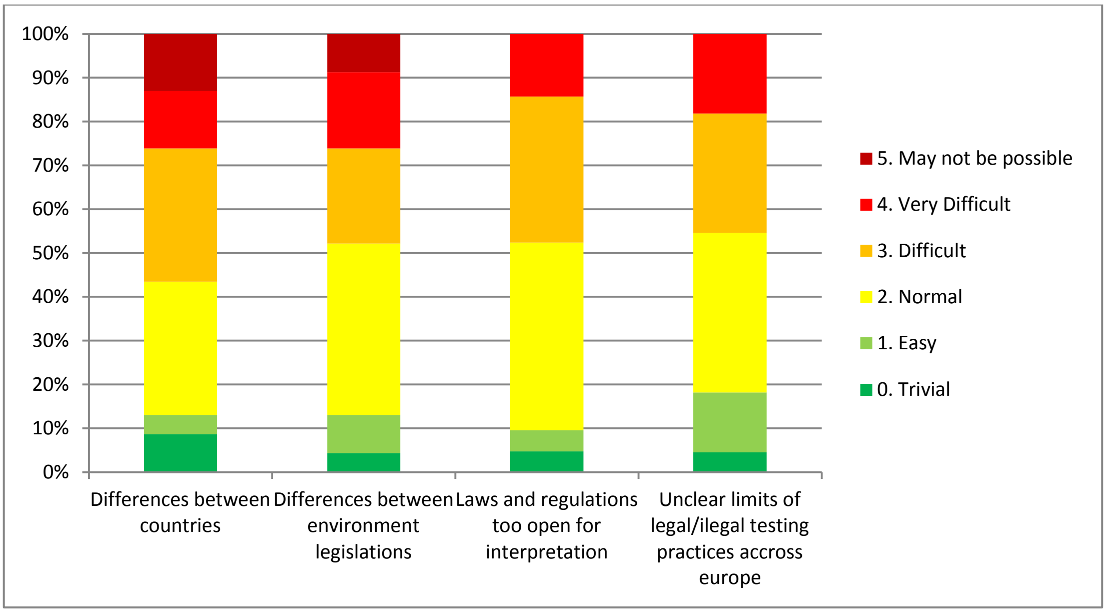


Figure 48: Most challenging limitations from a legal and regulatory point of view

Taking into account responses given by stakeholders, the most challenging from a Legal and Regulatory point of view are the differences that can exist between sectors or countries in their legislation.

Opinion among the interviewed stakeholders was that the Legal and Regulatory framework is a big challenge of testing process and they rated its solution as 'Very difficult'. Some important comments made by different stakeholders are:

- '*the problem has to be resolved at political level*',
- it can be done '*by segmentation*' or
- if a legal framework and laws at European level are created, then '*in about 10 years or so, it is going to work*'.

6.5 ECONOMIC & FINANCIAL: Which limitations do you consider would be the most challenging from an economic/funding point of view?

Concerning Economic and Financial limitations, the questionnaire offered three options to rate (Figure 49): 'Public Budget limitations', 'Private Sector Budget Limitations' and 'Difficulties to reach an agreement between Public and Private'.

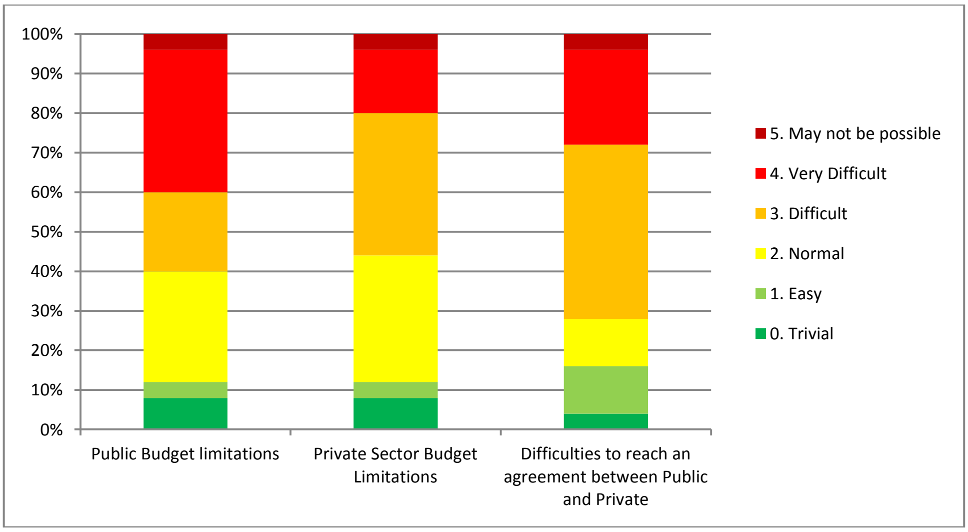


Figure 49: Most challenging limitations from an economic/funding point of view

On the one hand, some questionnaire respondents rated these options with at the lowest possible level; on the other hand, there were many high rate responses too. If the average of data responses is done, the rate of challenging of the three responses is close to 'Difficult' (3) level.

Comparison between Public and Private Budget seems to indicate that the private sector will have less problems or it will be an easier challenge to solve.

Manufacturers and Integrators interviewed consider that the initial funding should be public, and, when the initiative works correctly, many private companies will want to collaborate with the funding. On the other hand, they highlighted that public funding gives more independence because 'the private sector is investing only by emotions, so they could be pressured by external elements' (see also 4.2.3 and 5.1).

One interviewer highlighted that, in the case of certification model, the cost of it can be assumed by small manufacturers or manufacturers with a few products but for big vendors, the cost and complexity of certifying every product could be excessive.

7 External relationships

This group of questions was presented in the questionnaires and some of them were also asked in the interviews. Each question asks about some topics which must be rated from 'Strongly disagree' (-2) to 'Strongly agree' (2) except one question, in which for each topic a number between one (lowest) and five (highest) has to be set. Some of these questions are open, so experts can add whatever they want to say.

7.1 ROUTINE COMMUNICATIONS: How do you consider that communications between the ICS Test bed/Framework and other organisations should be modelled?

The proposed options to answer this question were 'Stakeholders presence in the Organisational Board', 'Periodic Meeting and events', 'Publications' and 'Communication protocols defined with other entities’. All answers were well accepted by stakeholders (Figure 50), with a rate close to ‘Agree’ (1) option. ‘Periodic Meeting and events’ was the most accepted option to model communications between the ICS Test bed/Framework and other organisations.

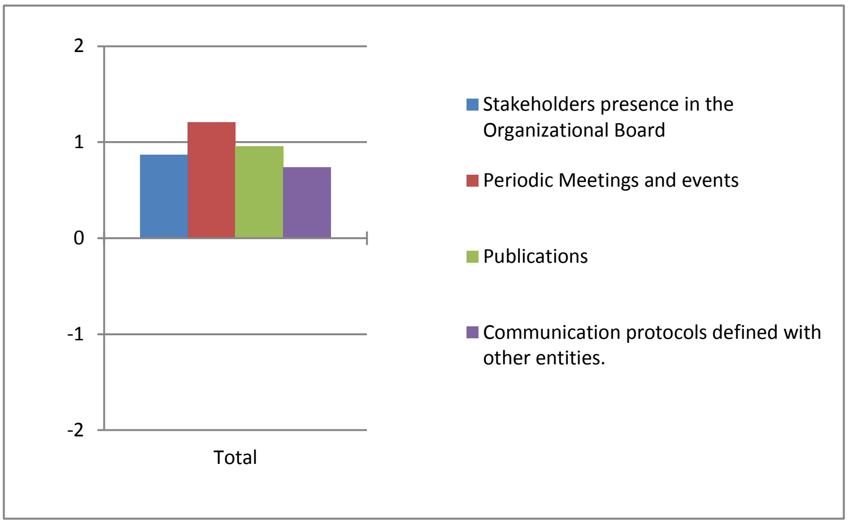


Figure 50: Routine communications type between the ICS Test bed/Framework and other organisations

Some experts added more information to this question with new possible models such as sharing information through a platform which allows stakeholders to publish the information they want.

Results by sector division do not show significant differences, but when looking at Stakeholder type (Figure 51), it can be seen that the ‘Academia and R&D’ group give lower ratings than the rest. ‘Manufacturers and Integrators’, ‘ICS Security Tools and Services Providers’ and ‘Standardisation bodies’ are the groups that have more agreement with ‘Publications’.

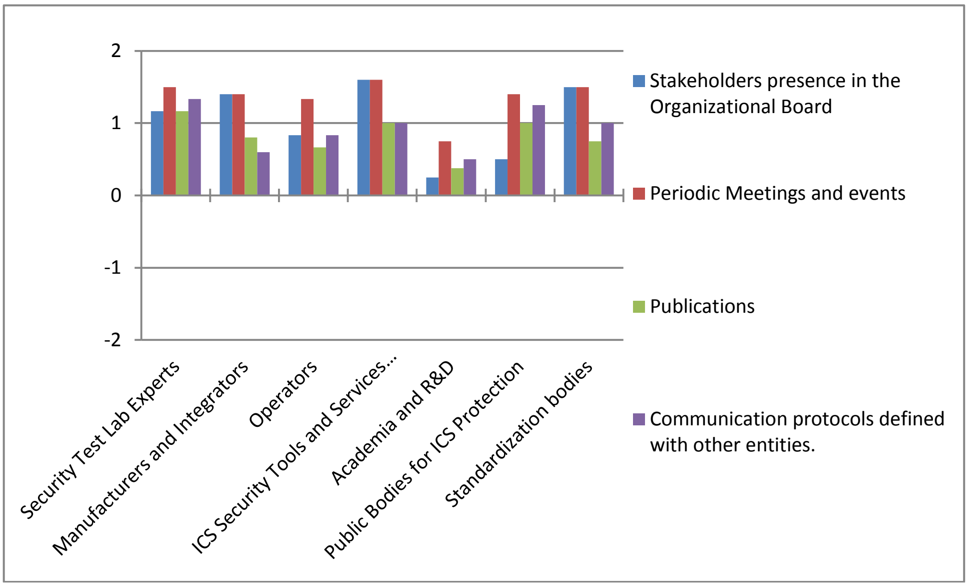


Figure 51: Routine communications type between the ICS Test bed/Framework and other organisations by stakeholder type

Regarding ‘Stakeholders presence in the Organisational Board’ there were different opinions between the experts interviewed, so this issue is specifically addressed.

- Some interviewees think that all type of stakeholders have to stay in the Organisational Board because it is very important to let people cooperate and to have as much information as possible on the right way to perform. For example, although there is consensus regarding the importance of involving all types of stakeholders in the entities concerned, as explained in 6.1, many experts believe that independent companies should not be a part of the Organisational Boards or other decision making bodies, and that they should delegate in consortiums of bigger groups.
- Some experts agree that vendors should have representation on the Organisational Board but not with decision-making power, only to provide knowledge . The reason for this is to retain independence and to reduce the risk of a single manufacturer, for example, gaining too much power on the Organisational Board. This can happen when for example there are people in the Organisational Board that are just there representing a single company, trying to block the debate or moving it to one direction.

The common feeling about communications between the different parts is that they will be very difficult to achieve, because everyone has their own vision and interests. Some rules and principles were also stated as necessary regarding information sharing, such as the way to present results, the standardisation of tests, constraints regarding procedures, etc.

7.2 CERTs/CSIRTs: When do you consider communications should be carried out between the ICS Test bed and existing or future CERTs/CSIRTs?

For this question, the questionnaire proposed two answers: 'In case of detected (potential) problems on existing Infrastructures', 'In case of emergencies' and an open option 'Others'.

Experts who completed the questionnaire thought that (Figure 52), in general, communications between the ICS Test bed and existing or forthcoming CERTs/CSIRTs should be carried out in both cases, with a rating over 1, so there is agreement about it, and even more clear in case of emergencies. Only one expert strongly disagreed (-2) with the answer 'in case of detected (potential) problems on existing infrastructures' and only two were 'Neutral' (0) with communications 'in case of emergency'.

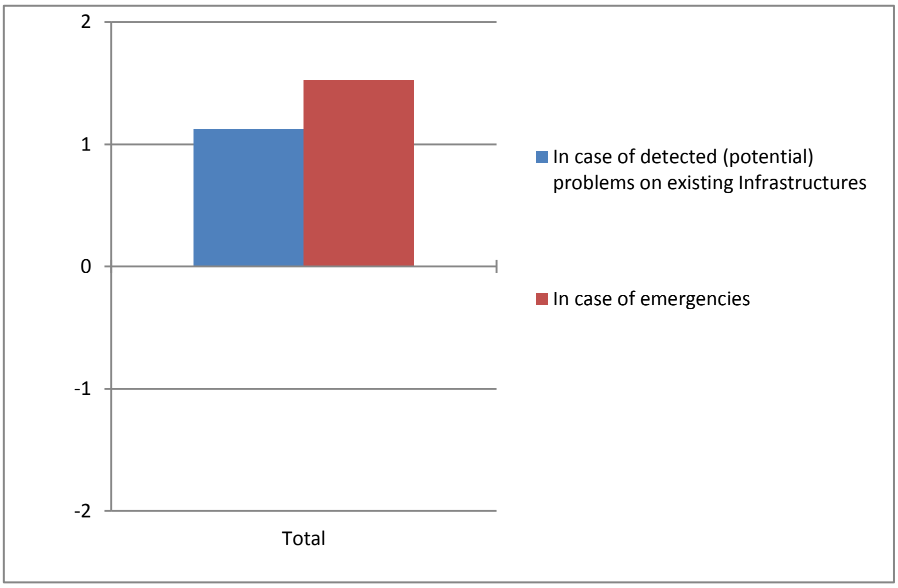


Figure 52: Communications between the ICS Test bed and existing or future CERTs/CSIRTs

Results by Stakeholder type (Figure 53) show that ‘Public Bodies for ICS Protection’ group ‘Strongly Agree’ (2) with both options and only the ‘Operators’ group prefers ‘In case of detected problems on existing Infrastructures’ rather than ‘In case of emergencies’, which is exactly the opposite of the ‘Manufacturers and Integrators’ answer. This could be explained considering that Operators would prefer to be informed as soon as possible about a potential risk, while Manufacturers might prefer to behave more discreetly.

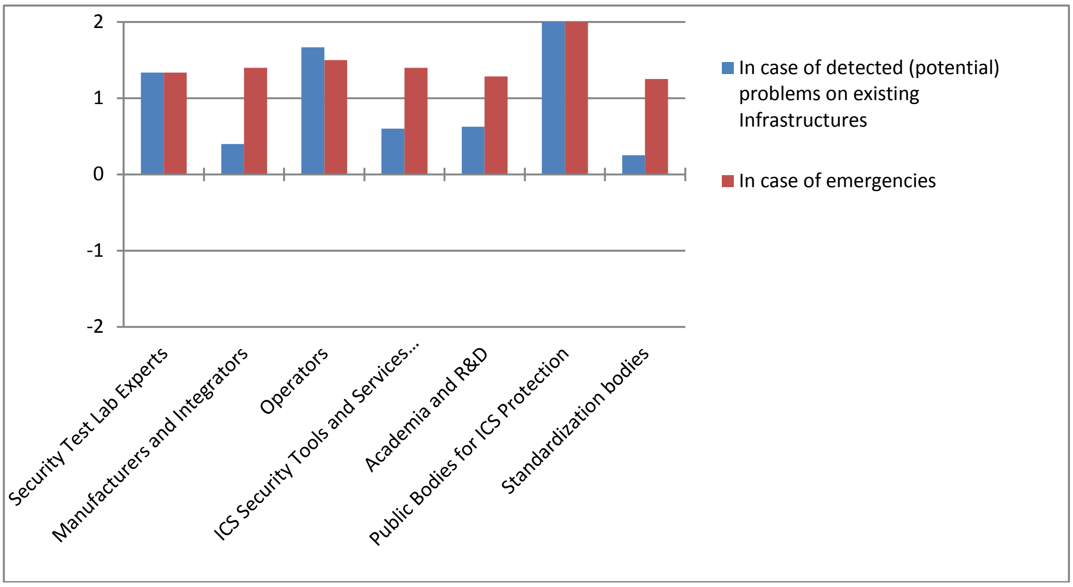


Figure 53: Communications between the ICS Test bed and existing or forthcoming CERTs/CSIRTs by stakeholder type

During the interviews most of the experts explained that, in their opinion, it is necessary to cooperate with CERTs as they are the ones who handle real risks, day-to-day, in production conditions. CERTs are trusted organisms that can handle the attacks, so trust can be improved through them. One expert recommended publishing reports that summarise general knowledge about the security status, while others believed more specific information should be communicated to the appropriate audience following a ‘case-by-case’ analysis.

Some also think that CERTs are prepared to take responsibilities in vulnerability disclosures and act as an arbiter in certain cases, which is a critical task that the eventual testing body could delegate to them. In fact, this is how it works in the USA.

7.3 VULNERABILITY DISCLOSURE: How do you consider vulnerabilities should be disclosed?

Note: The original intention of the question, as it was written in the questionnaire, is to build a path, selecting the order in which involved entities should be informed. But the high level of contrast between the opinions shared in the interviews and the numeric results strongly suggest that, instead of a ‘path’ (which means, the lower number, the bigger the priority), most respondents[12] ‘rated’ the priority (which would mean, the higher the number, the smaller the priority) that each Stakeholder should have. This means numeric results not reliable enough and it was decided to rely on the interviews, as this topic appeared often and was discussed in detail with most experts.

[12] But not all of them.

Most vendors had a strong position in this topic. They considered that they should be the first ones informed, as they are the ones that can fix the problems and take the responsibility of informing their customer and propose solutions.

But, in general terms, interviewed stakeholders did not agree with these terms. They think that this information can be of critical importance for many stakeholders and that, in fact, the problems will be easier to solve when there is information sharing and cooperation.

It is understandable that there are reasonable technical arguments to justify any of the positions, but also economic reasons. For example, vendors fear losing their reputation, but ICS Security Tools vendors prefer to propose their countermeasures rather than wait for bug-fixing.

As noted before (7.2), one interviewee said that communication mechanisms depend strongly on the information's content. It is possible '*to publish summarizing reports about general findings using as many channels as possible, but specific findings must be considered case-by-case depending of the specific circumstances and they will determine an ideal communication approach*'.

Some experiences in this regard, another expert explains, have made vendors become more collaborative. An interviewee said that vendors might start claiming that there are no issues within their products, or that everyone has security problems; but, if Government shows them vulnerabilities and how to solve them, then it is seen as a support and it will work as a door-opener. Vendors would talk to each other, and they would also want to have their products as secure as possible because they know that if there is an incident their reputation will suffer.

So, as they increase their interest in security, they need to learn and get more information about it. But they are still reluctant to provide much of their 'critical information' to current Test Beds, and even more reluctant to publish their results.[13]

Most interviewees think that trust (see 6.1) is one of the most decisive factors to achieve success for a European ICS Testing Body. With it, companies and individuals would be more open and cooperative. Regarding this:

- Some experts claim that certain organisms 'facilitate' trust, mainly Public Bodies, and/or mechanism like legal agreements and strict participation rules.
- Another interviewee suggested that: '*trust increases with committees in which there is a "core" of people that does not change, as it often happens, that someone cannot go to the meeting and they send someone else, so it is not so easy to remain confident*'.
- Another expert explained that trust is not something that can be built through companies (even if NDA contracts are written), because trust works at a more human level.

Many interviewees have expressed their opinion about signing non-disclosure agreements (NDA):

- On one hand, most experts agree about the need to use this formula, as a legal and professional mechanism to increase trust and cooperation. Contracts, one said, are as strong as the parties that sign them. So, if a big company and a European organisation agree about an NDA, it is something reliable, and this is something important for them.
- But other expert warns about an effect in the other direction. They explain that, in some cases, the biggest companies can force the other parties to sign such strong NDAs that the Testing Body has no means to assure that their results are being used to improve security. This is specially important regarding vulnerability disclosures; they recommend including clauses regarding responsibility for bug fixing, time before publishing vulnerabilities and ways to enforce resolutions such as disclosing vulnerabilities or applying sanctions to vendors that do not fix it. But this is a controversial topic, and may have an undesirable

[13] Especially if there is something wrong – which makes sense in the case of exploitable vulnerabilities.

effect in trust terms. It is necessary not to forget that, in some situations, vendors may claim that they are unable to help during long periods (months or more than a year) in which systems will remain vulnerable. Reasonable timings and responsibilities have to be agreed.

7.4 DISSEMINATION & AWARENESS: What do you consider to be the most appropriate way to perform Dissemination and Awareness activities?

For this question, the questionnaire had five proposals: 'Forums', 'Publications', 'Meetings for High Level Management', 'Educational courses and certifications' and 'Others'.

Stakeholders thought that all proposed methods were appropriate dissemination and awareness activities, as shown in the graph (Figure 54), with a preference for 'Educational courses and certifications' and 'Publications'.

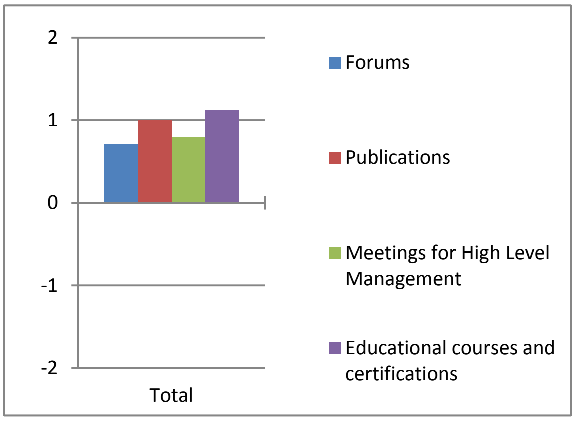


Figure 54: Most appropriate way to perform dissemination and awareness activities

During the interviews, a few experts commented that periodic meetings and events can be useful once the body is mature enough, but they are not a high priority for starters. Some also advised caution regarding publications, as they can be used to raise awareness but they can also give clues to attackers. Again the NSTB INL model, publishing just statistical, anonymous information is considered a better option. Regarding meetings, another expert considered that they are interesting, but more expensive in time and money, and not as clear as a good document.

Some stakeholders proposed other ways to perform dissemination and awareness activities such as:

- Using existing initiatives, mainly those which are fully dedicated to Dissemination and Awareness activities in the Industrial Cyber-security ambit, such as the Industrial Cyber security Center.
- Involve existing stakeholders in the creation of commonly agreed testing methodologies and guidelines, provided that the Testing Body can have recourse to some authority in case of disagreement. This would also help the Testing Body to meet stakeholders' expectations.
- Ask for cooperation in the review of publication, as it involves more experts and the results are less likely to increase risk for security owners.
- Another expert suggested that developing and using an alert or notification system similar to US ICS-CERT would be a good way to achieve dissemination objectives.

Regarding awareness, some experts think that senior management is not interested in the details of vulnerabilities and test bed results. With them, real use cases, demonstrations, and stories work better. On the other hand, medium-level specialist staff are interested in technical details. Therefore, meetings should be focused on the audience. Some consider that it is interesting to help medium-level staff to increase high-level management awareness.

7.5 EDUCATION: If you consider that such a lab should also perform an educational role, how would you suggest it should be provided?

The proposed options to answer this question were 'Through courses and certificates', 'Providing facilities for professionals to increase technical knowledge' and 'Through publications' and 'Answering specific questions for Stakeholders'.

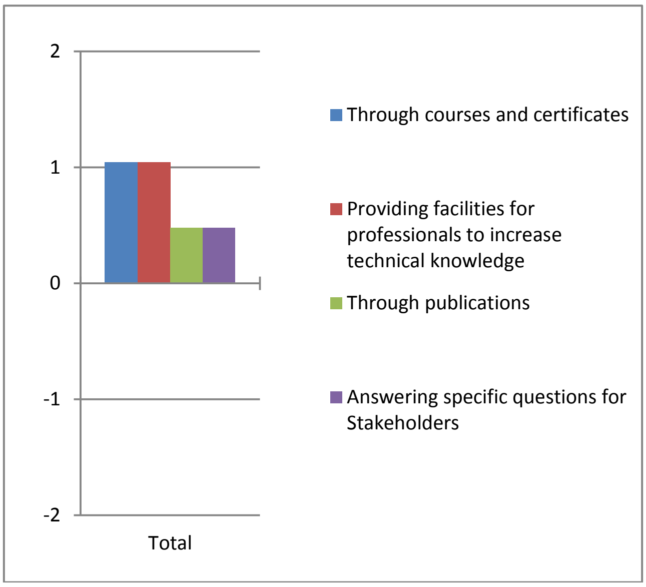


Figure 55: Educational role

Regarding stakeholders division by type (Figure 56), it is important to highlight that the average result of 'Answering specific questions for Stakeholders' rated by 'Manufacturers and Integrators', 'ICS Security Tools and Services Providers' and 'Standardisation bodies' is negative, indicating 'Disagree' (-1) value. The reason for this could be the lack of trust between all stakeholders and, as most stakeholders believe, the fact that these groups are more reluctant to share information. 'Public bodies for ICS protection' are 'Strongly Agree' (2) with 'Providing facilities for professionals to increase technical knowledge' option.

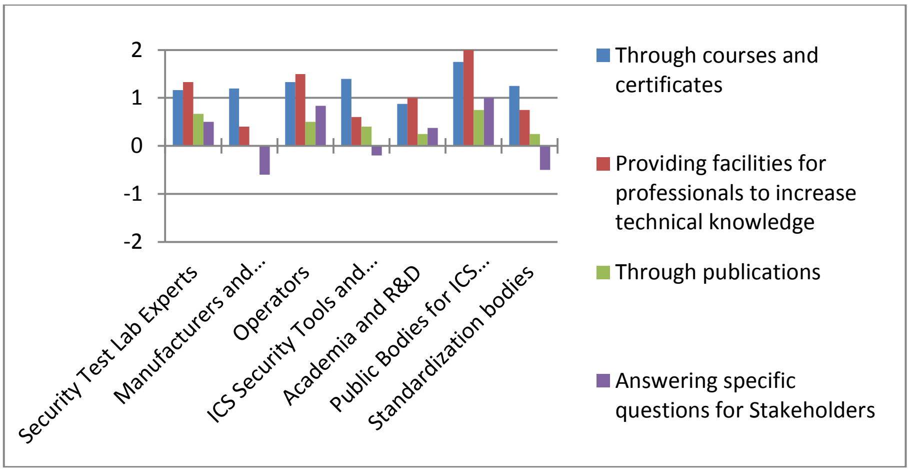


Figure 56: Educational role by stakeholder type

Regarding the interviews, one expert noted that some stakeholders are disappointed with academic publications, because they tend to publish all details, and that increases the risk as attackers can exploit this information. A few experts suggested drawing up agreements and provide seminars and lectures to stakeholders in cooperation with universities.

TP-02-13-769-EN-

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-074-1
9 789292 040741
doi: 10.2824/26451

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu