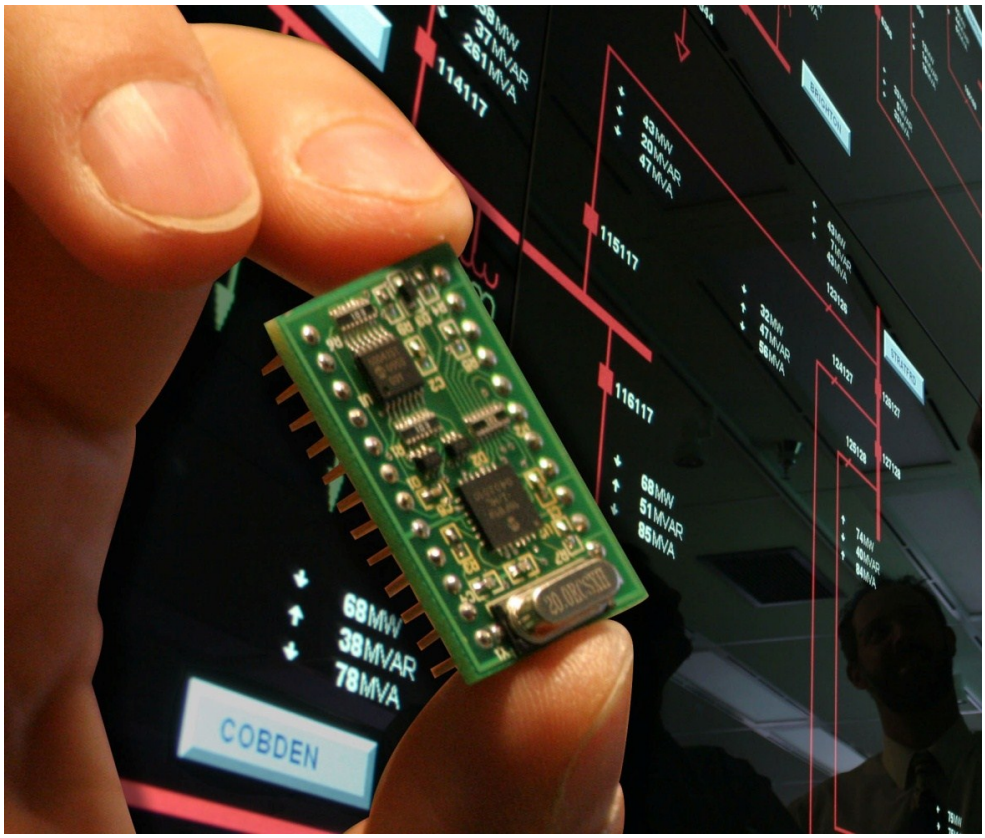


Good Practices for an EU ICS Testing Coordination Capability

Report

December 2013

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).

ENISA would like to express its gratitude to the speakers and participants in the validation workshop that took place on the 1st of October in Tallin , Estonia. Also we would like to thank Estonian Information System's Authority for the help provided in the organisation of the workshop.

Legal notice

Copyright Notice

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

Abbreviations

ANSI	American National Standards Institute
BEA	Battelle Energy Alliance
CCI	Committee on Critical Infrastructure
CCIRC	Canadian government created the Canadian Cyber Incident Response Centre
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Centre Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructures Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
COTS	Commercial off the shelf
CPNI	Centre For The Protection Of National Infrastructures
CSIRT	Computer Security Incident Response Team
CSSC	Canadian Strategic Software Consortium
DAE	Digital Agenda for Europe
DCS	Distributed Control Systems
DG JLS	Directorate-General for Justice, Freedom and Security
DOE	Department of Defense
DOE-OE	DOE Office of Electricity Delivery and Energy Reliability
EC	European Commission
ECI	European Critical Infrastructures
ESRIF	European Security Research and Innovation Forum
ENCS	European Network for Cyber Security
ENISA	European Network and Information Security Agency
EO	Executive Orders
EP3R	European Public-Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
ERNCIP	European Reference Network for Critical Infrastructure Protection
ESTEC	European Space Research and Technology Centre
ETSI	European Telecommunications Standards Institute
EU	European Union
EuroSCSiE	European SCADA and Control Systems Information Exchange
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
IACS	International Association of Classification Societies
ICS	Industrial Control Systems
ICSJWG	Industrial Control Systems Joint Working group
ICT	Information and communications technology
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute Of Electrical And Electronics Engineers
INL	Idaho National Laboratory
IPS	Intrusion Protection System
ISA	Instrumentation, Systems And Automation Society
ISO	International Organization For Standardization

IT	Information Technologies
JHA	Justice and Home Affairs
JRC	Joint Research Center
KF	Key Finding
LDPE	Low Density Polyethyl
NATO	North Atlantic Treaty Organization
NDA	Non-Disclosure Agreement
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Security Publication
NNSA	National Nuclear Security Administration
NSTB	National SCADA Test Bed
OT	Operational Technology
PLC	Programmable Logic Controllers
PPD	Presidential Policy Directive
PPP	Public Private Partnerships
R&D	Research & Development
RTU	Remote Terminal Units
SLN	Sandia National Laboratories
TDL	Trust in Digital Life
TNO	Netherlands Organisation for Applied Scientific Research
TOE	Targets Of Evaluation
UK	United Kingdom
US	United States
USA	United States Of America
VDE	Verband Deutscher Elektroingenieure (German Equivalent of IEEE)
VDI	The Association Of German Engineers
VDMA	Verband Deutscher Maschinen- und Anlagenbau e.V
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie e.V

1 Executive summary

Industrial Control Systems (ICS) are systems designed to support industrial processes such as gas and electricity distribution, water treatment, oil refining or railway transportation. They behave as command and control networks in a wide variety of environments, including many of the so-called Critical Infrastructures.

In the last few years, ICS technologies have evolved significantly. They have passed from isolated Operational Technologies (OT) to open architectures, highly interconnected with standard Information Technologies (IT) systems. This has lowered overall costs and enabled new functionalities, such as remote control, but at the same time it has led to a significant increase of vulnerabilities related to computer network attacks.

It is commonly accepted that providing testing capabilities for ICS stakeholders can effectively increase the security level across systems, enabling the detection of potential problems in a controlled environment, ensuring integrity and increasing the trustworthiness of certified/ tested solutions. Alternatively a security framework model adapted for ICS could be defined, so that stakeholders are supported when deciding which products/ services to buy or implement based on recognised efforts.

ICS security testing is now recognised to be so crucial that several countries within the European Union have already started to work in this direction in public or private initiatives[1]. Most of these initiatives have a geographic impact restricted to a single or a few Member States and with little or no coordination with other European programmes.[2] This has led to an uncoordinated and inefficient situation for ICS security testing. Some European initiatives, such as the ERNCIP,[3] work under the European Programme for Critical Infrastructure Protection (EPCIP), which aims to provide 'a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonize test protocols throughout Europe, leading to better protection of critical infrastructures[4] against all types of threats and hazards.' EPCIP does not, however provide a specific organisational or financial model, with homogenous goals and strategies.

This study aims to address some of these topics, and tries to identify existing resources and foreseen challenges in order to enable unified and consistent ICS security testing capabilities to be created across Europe. Although it can be argued that the impact of security testing can be slow in the installed base of EU infrastructure, many experts have been consulted in order to gather their knowledge and contrast their visions regarding this field, including the value it can provide and, moreover, the risks of inactivity.

[1] See "ICS Security Related Working Groups, Standards and Initiatives" for a full description and listed in : 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/ics-security-related-working-groups-standards-and-initiatives/view .

[2] In fact, some of the bigger countries have started their own testing capabilities independently, while smaller countries do not have resources to do so.

[3] See "ICS Security Related Working Groups, Standards and Initiatives" for a full description and listed in : 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/ics-security-related-working-groups-standards-and-initiatives/view .

[4] As the reader who is familiar with the topic should know, Critical Infrastructures and ICS technologies are related terms but not synonyms. Critical infrastructures is a term that comes from a governmental perspective and refers to the assets that are essential for the functioning of society. ICS, on the other hand, is a technological term. It is true that many CI are supported by ICS systems. But there are CI without ICS technologies and some ICS systems that are not used in CI.

The objective of this study is to explore how the European Union actions can be coordinated so to reach a level of harmonised, independent and trustworthy ICS testing capabilities, leveraging current initiatives. It represents a step forward from ENISA's 2011 recommendation for ICS protection,[5] offering guidance about how to design and operate these capacities from a wide perspective, including organisational, financial and technical aspects. The methodology included desktop research, an online survey and in-depth interviews with 27 experts from the European Union, the USA, Japan, India and Brazil.

The first part of the study aims to provide an overview of the current landscape of ICS security testing both in Europe and internationally, identifying initiatives, standards, methodologies, etc. Nevertheless, the main activities of the study were focused on proposing a feasible model to follow in order to enable ICS security testing capabilities in the European Union.

This research has led to 36 key findings and 7 recommendations, both for the public and private sectors, with special focus on the European Union institutions:

- Recommendation 1: The creation of a Testing Coordination Capability under public European leadership
- Recommendation 2: The establishment of a trusted and functional Executive Board to enforce leadership
- Recommendation 3: On the creation or involvement of working groups for specific activities
- Recommendation 4: Definition of a financial model appropriate to the European situation
- Recommendation 5: Carrying out a feasibility study for a Distributed Model of Operation
- Recommendation 6: Establish collaboration agreements with other organisations dealing with ICS security
- Recommendation 7: Establish a knowledge management programme for ICS testing

[5] 'Protecting Industrial Control Systems – Recommendations for Europe and Member States'; Recommendation 5: '*Creation of a common test bed, or alternatively, an ICS security certification framework*'.

Contents

2 Introduction

2.1 The need for a study on ICS security testing for the European Union

According to NIST SP 800-82, an 'Industrial Control System' (ICS) is

> *a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted programmable logic controllers (PLC) often found in industrial sectors and critical infrastructures*.

ICS and SCADA systems are used in many of the so-called 'critical infrastructures'. The European Commission in the document *Critical Infrastructure Protection in the fight against terrorism*, COM (2004) 702 defined critical infrastructures as

> *those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States*.

Nowadays, traditional IT technology is being widely adopted by most ICS and SCADA systems to improve the efficiency and the automation of the controlled process and related services[6] and, as a result, to achieve cost savings. Unfortunately, this adoption often comes with poor planning, lack of information, security misconfigurations, etc. Moreover, the adoption of IT technology incorporates well-known vulnerabilities and new zero-day vulnerabilities into ICS/SCADA systems. ICS systems may have a lifetime of over 20 years and have traditionally been designed without security requirements and to work as independent systems. Therefore, current control and automation systems are not prepared to deal with current threats. Legacy technologies must be improved to overcome current security gaps. Doing so requires firstly having a full understanding of the security case (i.e. vulnerabilities, their origin, frequency, etc.) for which security assessments by means of specialised tools and methodologies are necessary.

Although the industry is moving in the direction of developing security through the use of standards, recommendations and guidelines established by certification bodies and/or public–private initiatives, there are still several areas where there is room for improvement: poor software development practices, fast testing and objective measuring, official security certifications, current status of new security standards development, etc. All these needs could be addressed by a common test bed framework, which allows for testing ICS-SCADA systems, processes and components against specific security requirements. This is clearly stated in ENISA's 2011 document *Protecting Industrial Control Systems: Recommendations for Europe and Member States*, Recommendation 5 – creation of a common test bed, or alternatively, an ICS security certification framework:

> *The Common ICS security strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership that leverages existing initiatives (e.g. EuroSCSiE). This test bed would make use of realistic environments with the appropriate resources for conducting independent verification and validation tests. These tests should include, at least:*
>
> - *Check the compliance of applications and systems with specific security profiles.*
> - *Verify and validate that programming good practices and methodologies are being applied.*

[6] Such as remote control systems.

- *Certify that ICT security tools and services are compatible with specific ICS systems, applications and specific setups.*

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

2.2 Purpose and scope of the study

2.2.1 The aim of the study

There are two main objectives for this study. One is to present a clear overview of the current status of ICS security testing activities. In order to do this, it is necessary to identify the state of the art, the national, European and international initiatives, as well as threats, risks and challenges faced by these infrastructures.

Secondly, based on that analysis and the contribution of multiple interview and questionnaire answers from ICS security experts worldwide, the study intends to propose a series of recommendations to develop and implement a security testing framework that best suits the European Union's needs.

The study also aims to help the stakeholders concerned to recognise the importance of European test bed foundation, of cooperation between public and private sectors, and for developing norms and standards related to testing activities.

The recommendations resulting from the study will also allow ENISA to pave the way for future actions and studies on ICS/SCADA test beds.

2.2.2 The scope of the study

Most of the content used for the desktop research deliverable is based on highly reputable sources of information, such as official good practices, technical reports and standards produced by organisations such as CPNI UK, NIST, IEEE, ANSI/ISA, IEC, ISO and others.

However, the second part of the study, obtaining the opinion on the subject of all relevant stakeholders, is considered to be more interesting. Most of the material used to create the recommendations comes from the contribution of a group of experts. These individuals, from various fields (security test lab experts, ICS operators, manufacturers, academia, security tools and service providers, public and standardisation bodies, etc.) cooperated in this part of the study by providing their knowledge regarding existing initiatives, known good practices, standards and policies, as well as other topics already addressed and, even more important, experiences, opinions and suggestions. Relevant representatives of the public and the private sector were engaged (by means of a survey and personal interviews) to provide their opinion on critical aspects of ICS security test bed framework.

This study identifies common points and differences among stakeholders' replies and contributions to propose recommendations for these same stakeholders. These recommendations provide useful and practical advice aimed at improving current initiatives, enhancing cooperation, developing new measures and good practices, and reducing barriers to information sharing with the strategic goal of improving ICS cyber-security within the European Union through testing and certification activities.

2.3 Target audience

This report constitutes a source of the most recent information on the topic of ICS testing which might be useful to anyone involved in the domain of industrial control systems' security or interested in obtaining a security test in ICS devices and broad overview of the current situation in ICS security testing. An important part of this document is devoted to outlining the current situation in ICS testing, including initiatives, existing documentation (guidelines and regulatory documents) and standards related to ICS security test bed frameworks. It is assumed that the readers of the study will have security and ICS background knowledge. This section is intended for:

- Security test lab experts
- Manufacturing and integrators
- ICS engineering
- Industrial Control Operators
- ICS security tool and services providers
- Managers
- Security auditors
- Experts of certification schemas
- Business leaders with technical backgrounds

In addition, the core sections of this document contain a number of key findings, recommendations and conclusions regarding ICS security testing, resulting from the analysis of the opinion of a variety of experts in the field and from desktop research. These sections are not written in technical language. The key findings describe the main ideas, proposals and suggestions of experts for developing future strategies, methodologies and standards for ICS security testing at different action levels: political, technical, financial, etc. For this reason, this part of the study is more appropriate for:

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

2.4 Approach

The study comprised two main phases. The first phase was intended to gather all the data that would make up the work base for the study. The second phase was based on the analysis of the data in order to develop recommendations for the different types of stakeholders involved with the creation and use of ICS security testing framework.

The activities carried out during the first phase of the study included the so-called 'desktop research', which refers to the analysis of all available documents relevant to the topic of the study. This included existing documents (guidelines, recommendations, reports etc.) from organisations, companies, consortiums, initiatives or research centres, as well as the most influential

documentation in the field, and the latest news (e.g.: subscription to forums, discussion groups, LinkedIn expert groups, etc.).

The second part, the 'stocktaking', aimed at obtaining experts' opinions on the most important ICS testing subjects through questionnaires that included 26 different questions. At the same time other experts agreed to be interviewed to explain certain concepts in a personalised way and provide deeper insight. The information provided by the experts has been classified according to the main background of the experts. This classification is made both by sector and by type. The sector has been further divided into the type of work carried out by the expert (energy, manufacturing, chemical, water, etc) and the type by the role assigned in the sector (security test lab expert, manufacturer, operator, R&D, public body, etc.)

It is worth mentioning that over 100 experts were contacted for the study, of whom 32 participated in the poll. Additionally, 32 experts were asked to perform interviews, which led to 23 conferences with 27 different experts.

The second phase of the study was based on the qualitative analysis of the findings and the development of recommendations for different categories of stakeholders. The first stage of the study built up a large data source comprising diverse information. These data were consolidated and normalised into a structured set of information that can be easily and thoroughly processed. The basic element of it is a 'key finding', which is a relevant and influential observation from the desktop research, the survey and/or the interviews. Key findings may show an emerging issue, an initiative taken or believed to be taken, an agreement/ disagreement level between stakeholders, values or tendencies in the answers, a relevant line of opinion or any other piece of elaborated information that might have any impact in the field of security test bed focused in ICS environments. Key findings were finally combined in order to ultimately derive the recommendations presented in this study.

3 Key findings of the study

This section presents the key findings of the desktop research and the analysis of the results of the survey and interviews. For these tasks, questions were tailored to make it easier to obtain key findings that would give rise to clear recommendations. As an output, several topics have arisen regarding the status, challenges, gaps, resources, objectives and concerns related to the creation of a European Testing Coordination Capability.

In this section, the most relevant ideas have been structured into six specific categories identified as necessary to address the recommendations. The logic behind those categories was to start by describing the current situation of the ICS security testing environment, trying to identify its needs and requirements. Then, it was intended to sketch which models could best address these needs, considering existing resources and trying to foresee the biggest constraints and limitations. The final part is intended to clarify how the eventual testing coordination capability should relate to the rest of the organisations that make up the ICS security community.

- Current status of ICS testing:

There is growing interest in ICS security testing in Europe. This has led to the current situation in which several initiatives have emerged. Unfortunately, they are mostly considered immature, with poor or no coordination between them and room for improvement in methodologies, standards and educational resources. Most experts consider that leveraging these efforts under a coordinated programme could help to raise the status of ICS security testing.

- Objectives for a European ICS Testing Coordination Capability

In order to provide ICS security testing capabilities in the European Union, it is important to understand the needs of the community, and the main objectives that must be taken into consideration. An independent testing coordination capability, aligned with current standards, supported by public institutions and able to provide value to all involved stakeholders is required, but some other topics, such as the importance of making testing mandatory, are still under discussion.

- Consideration about the model and operations

In this section the discussion is about how to model a Testing Coordination Capability to best address those needs. Testing facilities are considered necessary but opinions regarding a certification framework are divided. In any case, most of the experts consider that the acceptance of the results is a key issue for the entity success and consider that a distributed model of operations, engaging centres across the European Union would be adequate for the current and future scenario.

- Overview of available resources

The next point is to identify the available resources that could be used to facilitate and speed up the process. It has been pointed out that funding could come through a public–private partnership and knowledge could be engaged from the industry and some European and international experiences.

- Major constraints, risks, threats and limitations

The experts have warned about their biggest concerns regarding the creation of a Testing Coordination Capability in the European Union. Building trust among the stakeholders was one of

the most recurrent topics, but also the enormous diversity of technologies involved, they way they are used, the heterogeneous regulatory environment and the need for a clear funding model.

- Relationships with other stakeholders

This section outlines how the Testing Coordination Capability should relate to the rest of the ICS security community. Taking into account all stakeholder types through representation in the Executive Board and other tasks, recommendations were to maintain fluid communications with CERTs and other institutions, to be especially careful concerning vulnerability disclosures and taking advantage of the Testing Coordination Capability for educational purposes.

3.1 Current status of ICS testing

3.1.1 ICS security testing is uncoordinated

The situation of ICS security testing in Europe is unanimously seen as fragmented, not harmonised and immature. During the last few years, the interest in security for ICS has increased. This has led to several national initiatives in a number of European states,[7] with little or no coordination at higher level. Most consulted experts believe that it is necessary to foster cooperation as the way to achieve a better security status along with a more efficient use of resources.

3.1.2 No real 'ICS security educational environment' in the EU

Many experts noted that there are two types of professionals working in ICS security testing. Some come from the IT environment and some from OT. The differences between their backgrounds can cause serious communication and interpretation problems. As far as can be determined, there is not a mature 'educational environment' for ICS security needs in the European Union. Some specific courses may be offered in future in response to market needs, but as yet there are no official efforts, as in other countries.

3.1.3 Low maturity level of ICS security testing methodologies and initiatives in Europe

The current ICS test bed initiatives in Member States are not mature enough in terms of technical versatility and fluency of work to assume immediate leadership of tasks testing in Europe. For some aspects, some initiatives have arisen such as the ERNCIP, the ENCS, CCI, or NATO Test Bed; these must be taken into account. But at the date of this publication, there is no initiative with the completeness of vision and the specificity required for European needs.

In addition, ICS environments are often tested following methodologies that were conceived for the IT environment. The implications of bugs and failures in both situations are very dissimilar, so most experts agree that they are not well focused. In fact, many of the professionals in charge of these tests are aware of these limitations, so they just use the parts or controls of these methodologies that apply better to their needs under their best judgement. There are just a few exceptions to this, like the ISA/IEC-62443 (Formerly ISA-99) or ANSI/ISA TR99.00.01-2007. In any case, they recognise that there is also much space for improvement for most industry-specific cases and also regarding

[7] See "ICS Security Related Working Groups, Standards and Initiatives" for a complete review of studied initiatives and listed in: 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/ics-security-related-working-groups-standards-and-initiatives/view .

risk management processes. Most of them consider that clear guidance in all these matters would be interesting, if not necessary.

3.1.4 Interest in a certification framework

Many experts consider the creation or adaptation of a certification framework for ICS environments to be necessary in order to ensure a minimum level of security for ICS infrastructures across the European Union, at least, within some conditions. In fact, some countries, as Germany and England are currently working on a Common Criteria adaptation for ICS environments.[8] This interest is highly dependent on the stakeholder type, with operators and security test lab experts most interested (see Figure 1). However, the adaptation of a certification framework is a matter of debate (see section 3.3.2).

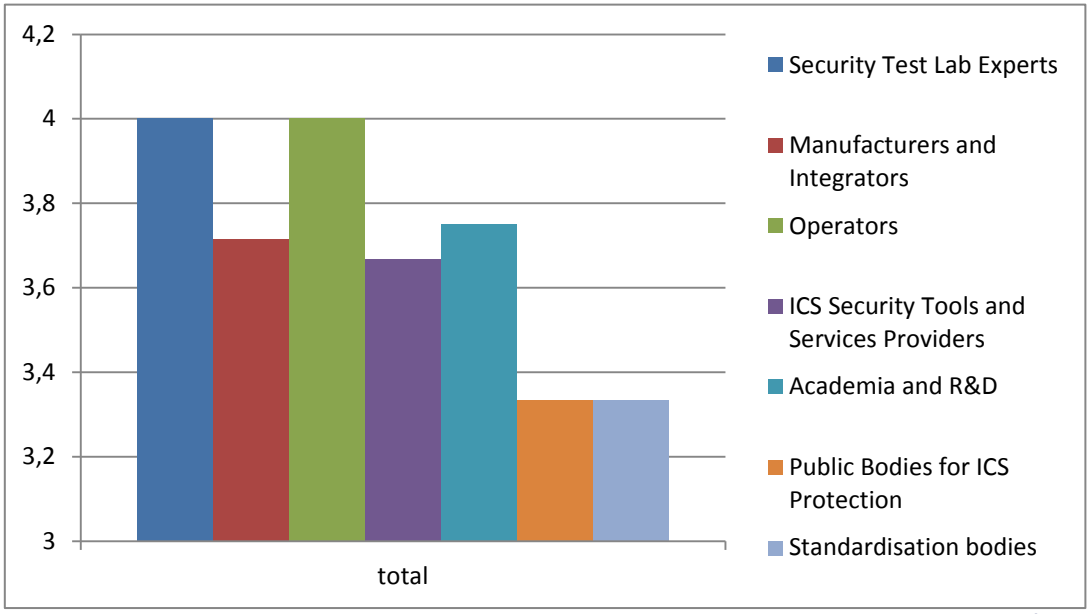


Figure 1: Degree of interest in the creation of a common Test bed/Framework by stakeholder type[9]

3.1.5 Operators are key to a change in the status-quo

Many experts believe that ICS operators, as well as other organisations that acquire ICS technologies (i.e. integrators, engineering companies, etc.), could act as the main agents of change. Moreover, if asset owners can join forces to demand high-end cyber security capabilities for the products and services they need, they could dramatically influence today's common practices.

In this regard, during the workshop some experts pointed out that there are great differences among sectors in the maturity level of the cyber-security measures and initiatives targeting the protection of operational technologies, including ICS. The nuclear industry and the

[8] Although they are doing it independently and, according to some experts, their approaches are not mutually compatible.

[9] This figure shows the degree of interest that every stakeholder type had in the creation of a Certification Framework, rated from 0 – Against the creation of such Framework to 5 – Indispensable. As can be seen, most answers are close to 4 – Strongly Positive, but some other consider it just 3 – Interesting. A complete discussion is included in section 2.5 of the "Survey and interview analysis" and listed in: 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/survey-and-interview-analysis/view .

telecommunications sector are most advanced in this respect. Nevertheless, if coordinated, other sectors could probably benefit from these efforts in the future.

3.2 Objectives for a European ICS Testing Coordination Capability

3.2.1 Need for independent evaluations, tests and certifications

During the survey several drivers were considered interesting for the creation of a Testing Coordination Capability. The need for interoperability testing within different OT vendor products and with IT products, and raising awareness and knowledge, were rated positive; and some others arose during the interviews such as the need for coordination, or the interest in having 'a single authority' to contact for national or international organisations. But the main driver was identified as the 'Need for Independent Evaluations, Tests and Certifications'.

When asked about the tasks that the Testing Coordination Capability should perform, the questionnaires revealed minor differences in the tasks suggested, with 'single device testing' and 'providing guidance in ICS security' the most valued ones. But during the interviews, many experts expressed their doubts about the interest in performing single-device testing.[10] As this is something already being done in many centres across the world, they recommend differentiating somehow from that model and finding smarter and more cost-effective ways to work.

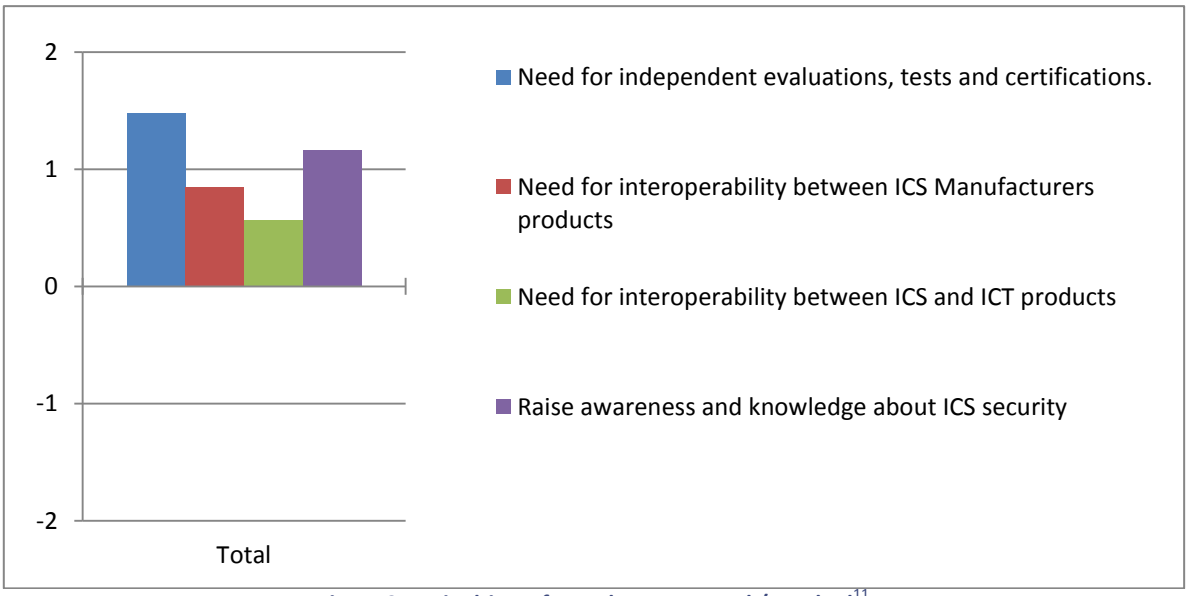


Figure 2: Main drivers for such a Framework/Test bed[11]

[10] Providing guidance is considered a theoretic approach about how to address security, while single-device testing involves performing a set of tests to an specific, isolated piece of equipment. A discussion of other alternatives can be seen in "Survey and interview analysis", section 3.2 and listed in: 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/survey-and-interview-analysis/view .

[11] This figure shows, in average, the degree of agreement with some proposed drivers between -2 points (Strongly Disagree) and +2 points (Strongly Agree). A complete discussion is included in section 3.1 of "Survey and interview analysis" and listed in : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-

3.2.2 Political will has been necessary in similar experiences abroad

Some respondents explained that political will has been the main agent of change for the most significant similar experiences addressed in the past. The NSTB/INL in the USA was boosted after the 9/11 attacks, and the process of creation of the CSSC in Japan begun after Stuxnet, but was significantly speeded up after the 2011 earthquake and tsunami. Securing critical infrastructures, which often include ICS systems, is usually considered a Homeland Security matter that is likely to be seen as more relevant after a disaster with dramatic consequences has occurred.

3.2.3 Aligning with existing standards is better than developing new ones

Most experts expressed their concerns about including more certifications in a market that is already too diverse and fragmented. When asked for alternatives, they usually recommended aligning with existing standards and regulations (i.e. ISA/IEC-62443, ANSI/ISA TR99.00.01-2007 or ISO/IEC 15408) and including those cyber-security aspects that must be taken into account. This vision is reinforced by the fact that, in this field, cyber-security risks can lead to physical damage.

3.2.4 Offering value to all stakeholders is key to success

In order to build a successful initiative, all involved stakeholders must be interested in cooperating with the Testing Coordination Capability. If some of them are privileged over the rest this could lead to conflicts and lack of trust. Eventually, if this happens, the initiative will fail as a trusted and effective security enhancer. Operators may find interesting guidance and audits regarding their own infrastructures. Many security products and service providers, vendors and researchers could take advantage of independent testing facilities during development phases of their products, etc. Communications could be held with all involved parties in order to understand their needs and find adequate frameworks of mutual interest for cooperation.

3.2.5 A systemic or holistic approach is recommended but is more difficult to standardise

Trying to identify any type of device as 'most critical' for testing has provided no conclusive results. As many experts have said during the interviews, any link in the security chain can potentially include breaches that compromise the whole system, so a holistic/systemic approach for security has often been recommended.

Some of the most technical experts, noted that some 'creative' testing methods, such as 'penetration testing' or 'sniffing and analysing' techniques are more effective in understanding the real security level of a given infrastructure than checking devices under laboratory conditions or under virtualisation. The main limitation of these techniques is that they are highly dependent on the knowledge of the tester, so they might not be consistent enough to provide consistent results.

3.2.6 Debate regarding the adequacy of making testing mandatory

When asked about making ICS security testing mandatory the most common answer was that it should not be. Nevertheless, more than a half of the answers were positive if testing were to be mandated under certain conditions such as 'depending on business' or in the future, once the testing methodology is mature enough. In fact, many of the experts interviewed expressed disbelief in performing any tests if they are not mandatory. Some considered the option of including these controls in existing regulations (see 3.2.3). On the other hand, some others appealed to experiences

---

infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability/survey-and-interview-analysis/view .

like the US NERC-CIP to explain the negative effects of regulations in order to increase security (see KF 3.3.2).

There is considerable debate over this topic at many levels. For example, some have suggested that testing should be mandatory for critical infrastructures or for those that have an impact on society, but others have replied that nowadays it is unclear – or, more precisely, 'nation dependent' – exactly what constitutes a critical infrastructure.

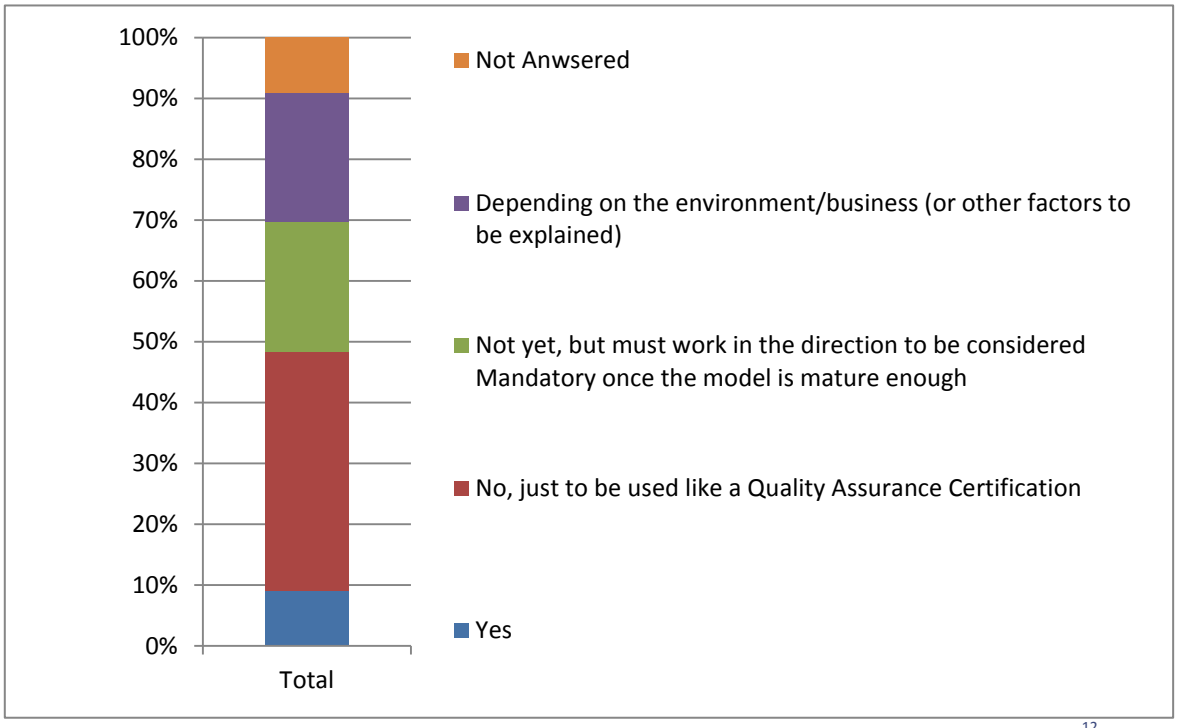


Figure 3: Acceptance percentage of mandatory of the framework for any new technology or product[12]

3.2.7 Consider ways of enforcing vulnerability resolutions

Some experts, especially those from the group 'Security Test Lab Experts', noted the importance of keeping some capacity to enforce vulnerability resolution once they have been found and notified. Some experiences around the world have shown that, sometimes, companies do not resolve specific problems, because, for example, they do have economic reasons to do so. This means that some vulnerable systems may stay in production for long periods of time although they have known problems and resolutions, but very closed NDA agreements disable any possible correction enforcement. It has been recommended to keep some level of independence to apply measures. Suggestions for dealing with this vary from applying economic penalties to performing vulnerability disclosures after a reasonable period of time. In any case, it is admitted that any measure would be controversial and could meet resistance.

[12] From the set of proposed answers in the legend, respondent votes showed this distribution. A complete discussion is included in section 3.5 of the "Survey and interview analysis" and listed in : 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/survey-and-interview-analysis/view .

3.3 Consideration of the model and methodologies

3.3.1 Need for both testing facilities and a certification framework

According to the experts, both the creation of Testing Facilities and a Certification Framework are mainly considered as being 'necessary'. In fact, a common answer was that, for this environment, it is necessary to provide both services to the community. They consider that testing without obtaining a certification will decrease the attractiveness of testing, as there would be less marketable value. On the other hand, providing certifications not based on real tests is not considered adequate by most experts.

Of particular interest is the fact that the idea of a 'Certification Framework' is mainly supported by Operators (see Figure 4). During the interviews this was explained as their need to show themselves compliant regarding specific standards, especially taking into account that many of them perform their own tests before setting devices in the production line.

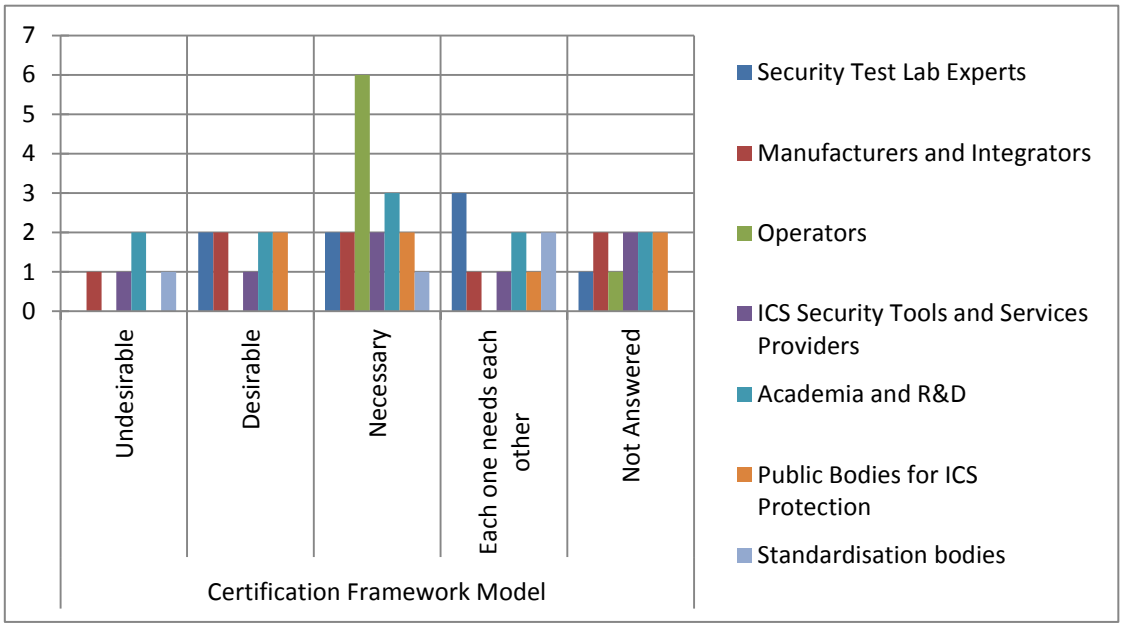


Figure 4: Interest in a Certification Framework model by stakeholder type

3.3.2 Debate over whether Certification and Compliance are adequate for improving security

There is considerable debate regarding Certification and Compliance as an effective and valuable method for improving the real security status of the ICS environment.

- On the one hand, experts with a business-oriented perspective like the idea of having certifications. In fact, a few of them believe that some type of certification is unavoidable; otherwise, there is no point in testing. In general, they like the idea of having a reference, a list of controls to be compared with, not as in more 'creative' testing (see 3.2.5). They also think it is easier 'to sell' to operators and that vendors would appreciate having just one reference for all of Europe. They also admitted some problems, like the fact that the

information can also be used by attackers and that it can be very costly if the objects of certification are single devices[13] and have to be re-certificated after any change.

- On the other hand, technical experts do not like it as they think it could lower standards from a security perspective. NERC CIP or Common Criteria are often referred to as a misleading influence for security building. For economic reasons systems are made to meet minimum compliance standards only, not taking into account that security needs change over time, that some standard controls are not applicable in ICS but others are more critical, etc. The technical experts' view can be summarised as 'Stop aiming for compliance and build security'.

Some point of agreement has been found with the proposal that the Certification Framework could be the point to reach once testing facilities have been operating for a period of time and are mature enough. This model can operate while awareness and interest is raised and is improved over time, so it can start with an accepted model to be adapted in further iterations for businesses or needs.

3.3.3 Deciding what exactly should be certified

Several options have been expressed by experts about 'what should be certified' in case a certification framework is set, including:

- Devices: This is interesting for stakeholders, but is already being done in several test beds and can be too costly for companies with many different products.
- The development process: It could be more efficient than 'single device', and already existent certifications may be adapted.
- Security postures: This is the direction that some Member States[14] are already working in.
- The whole architecture of the systems: Including devices and mitigation measures, in a real and controlled environment in case it could endanger citizens.
- The test beds: Many experts consider that in addition to any certification, a European body should be able to accredit those centres that are mature enough to perform appropriate testing (see 3.3.6).

3.3.4 Stakeholder roles for definition and operation will require common agreement and public leadership

Several questions were intended to identify the most desirable roles for each stakeholder in the process. In general terms, it can be concluded that all stakeholders would have to be taken into account for all tasks, so they can share their knowledge and vision, but their degree of involvement differs significantly.[15]

For starters, public bodies are considered as the most appropriate organisations to lead some of the most critical definition tasks, such as objectives (Figure 5), financial model and communications (Figure 6). Operators and vendors were also considered for high-responsibility roles in any kind of task, including the financial model definition. Security test lab experts were pointed out as the most

[13] The adequacy of single-device testing is discussed in 3.2.5.
[14] For example the United Kingdom.
[15] A complete discussion of tasks and responsibilities can be found in "Survey and interview analysis" and listed in: 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/survey-and-interview-analysis/view .

suitable stakeholders in order to define and operate in technical and methodological (Figure 7) activities.

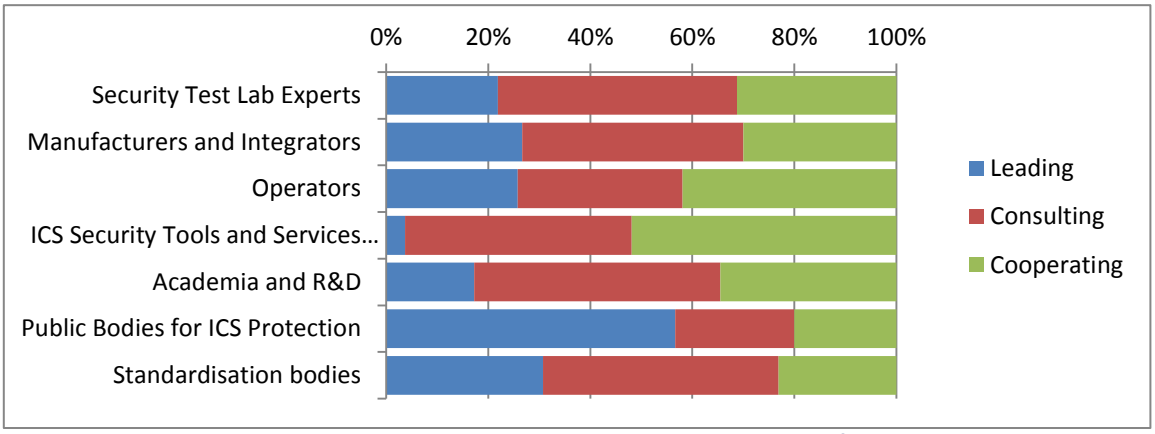


Figure 5: Stakeholder roles for Objectives Definition[16]

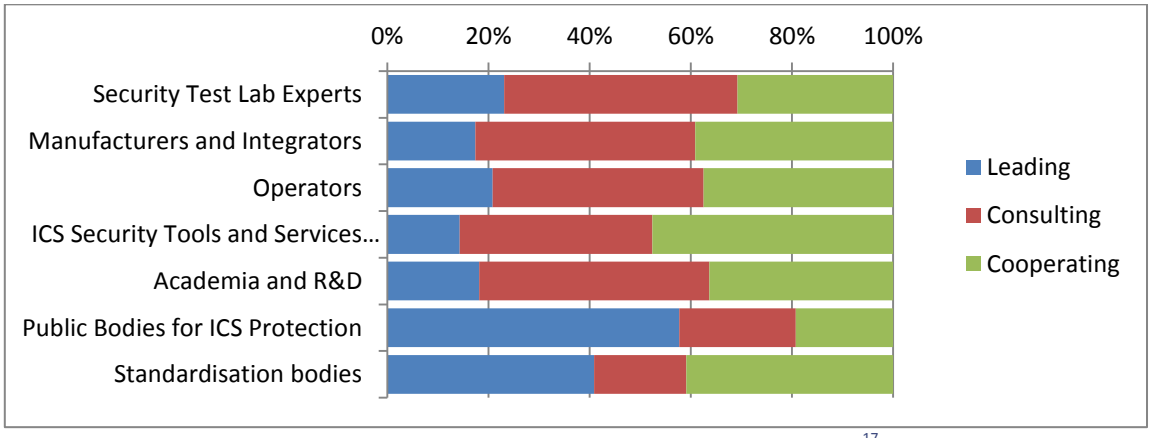


Figure 6: Stakeholders roles for Communication operations[17]

[16] This graph shows, for every stakeholder type, the percentage of votes they received for each level of responsibility (Leading/Cooperating/Consulting) in the Objectives Definition task. A complete discussion is included in section 4.2.1 of "Survey and interview analysis" and listed in: 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/survey-and-interview-analysis/view .

[17] This graph shows, for every stakeholder type, the percentage of votes they received for each level of responsibility (Leading/Cooperating/Consulting) in the Communication Operation task. A complete discussion is included in section 4.3.2 of "Survey and interview analysis" and listed in: 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/survey-and-interview-analysis/view .

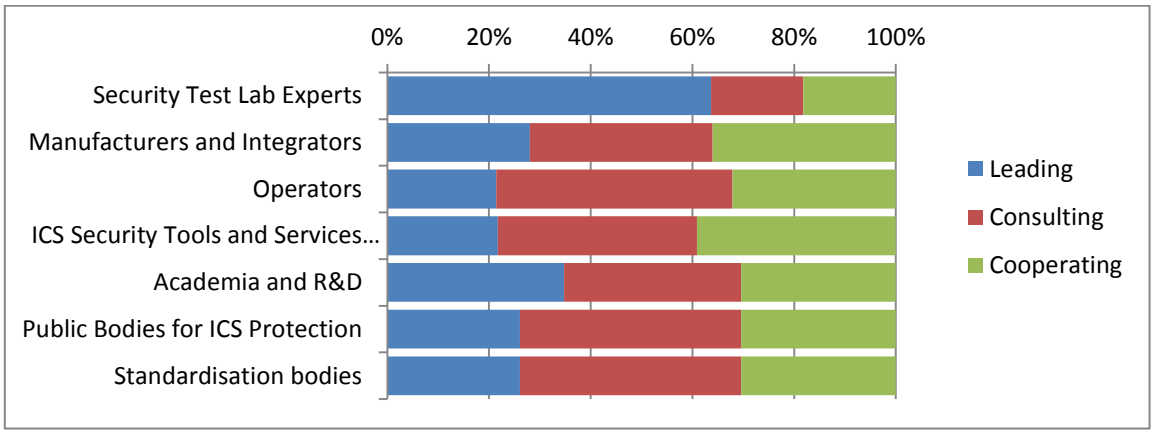


Figure 7: Stakeholders roles for Tests and Results operations[18]

3.3.5 'Acceptance of the results' and 'Comprehensiveness of tests' are the best measures of success

According to the experts, 'Acceptance of the Results' is considered the most important measure of success. Being able to provide impartial and competent results, technically valid, relevant and including actionable findings is the best way to make them widely accepted and, ultimately, a decisive point for the success of the initiative. This has to be understood from a multi-stakeholder perspective, in which conflicts of interests can affect trust (see 3.5.1).

Comprehensiveness of tests was also highly rated, and it can be considered more important than speed, but some experts cautioned that both factors have to be kept into balance (see 3.5.3).

3.3.6 EU complexity makes desirable a 'Distributed Model' with an Accreditation Organisation on top

During the interviews, a wide majority of experts stated that a Distributed Model of operation would be the most appropriate, considering the EU's complexity, and the way in which Europe could take advantage of its own size. Different reasons such as closeness to the industry, differences in legislation or specific needs and the possibility of developing 'centres of excellence' for concrete purposes were often quoted.

In almost every interview the respondents spoke about the need for 'synchronising' existing efforts, making 'consistent tests', not lowering standards and, for foreign organisations, having a clear 'gateway body' that could act as an interlocutor. In most cases this links directly to an 'Accreditation Model' in which a main body could accredit centres to perform the tests, as has already been done in other industries.

3.3.7 Segmentation by business is the most recommended course

Regarding the best way to segment activities between centres, segmenting 'by Business' was the preferred option based mainly on two reasons: every industry has specific needs, and the cost of the

[18] This graph shows, for every stakeholder type, the percentage of votes they received for each level of responsibility (Leading/Cooperating/Consulting) in the Test and Results Operation task. A complete discussion is included in section 4.3.1 of "Survey and interview analysis" and listed in: 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/survey-and-interview-analysis/view .

equipment. Some experts thought that starting from a generic model and adapting it, in future iterations, for every industry could be helpful.

3.4 Overview of available resources

3.4.1 Public–private partnership(PPP) as the most accepted financing model

Many of the stakeholders consider that exclusive public funding models are insufficient to achieve self maintenance of the Testing Coordination Capability and that there is no reason not to include private investments if mutually beneficial. Experts believe that it would be worth carrying out a feasibility study in this regard, considering some kind of PPP funding model. In any case, public funding can be necessary in the early stages (as explained in section 6.4.2).

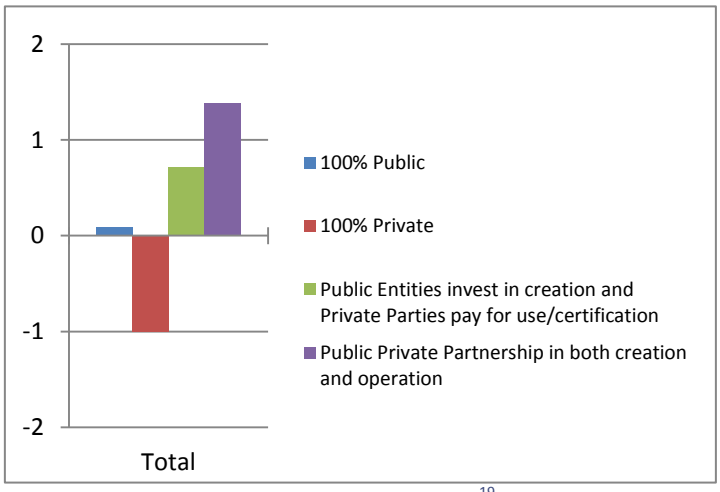


Figure 8: Financial model[19]

3.4.2 Strong initial public Investment was needed in similar initiatives abroad

Some experiences in foreign countries were based on a model of massive public investment during the first years that then shifted, or are intending to shift, to a model with more private financing. Experts consider that this is reasonable, as the stability needed in the first stages can only be provided by public institutions;[20] but that, if test results have real value, they have to be marketable. For some, this has the negative counterpart that it makes the Testing Coordination Capability, undesirably (see 3.2.1), more dependent.

3.4.3 Multiple reasons for success identified in existing initiatives abroad

Several experts with different degrees of contact with the NSTB of the USA INL, the Japanese CSSC or the Brazilian ICS Sandbox were interviewed and confirmed that there are no single reasons for

[19] This figure shows, in average, the degree of agreement with some proposed drivers between -2 points (Strongly Disagree) and +2 points (Strongly Agree). A complete discussion is included in section 5.1 of "Survey and interview analysis" listed in : 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/survey-and-interview-analysis/view .

[20] This is discussed in "Survey and interview analysis" sections 5.1 and 5.2 and listed in: 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/survey-and-interview-analysis/view .

success. The availability of resources, political will, technical expertise and training capabilities, independence, ability to build trust among stakeholders, cooperation models and actionable findings were frequently cited success factors.[21]

3.4.4 Not advisable to publish product comparative charts

Although requested by some European operators, most stakeholders consider that publishing comparative charts regarding the security status of devices or services is not advisable. As some external experiences have proven, trust and cooperation are enhanced if the Testing Coordination Capability limits its activity to identifying and helping to correct any security problems detected in the systems. Doing otherwise might make competing vendors reluctant to cooperate, and if it turned into a marketing argument, the Testing Coordination Capability independency could be compromised in the long term.

3.4.5 Work in multidisciplinary teams needed

Experts highlight that for the correct operation of a test bed, the human factor and knowledge must be taken into consideration. Experts will have to combine various disciplines, mainly IT and OT, to achieve complete understanding of all implications and risks of any ICS security vulnerability. In addition, as security is an ever-changing field of knowledge, some experts state that 'creative' skills are also advisable.

Because all the qualities required are difficult to find in one person, most interviewed experts recommend the creation of multidisciplinary teams that can work and learn together.

3.4.6 Engage expertise from the industry concerned

An interesting approach that several experts proposed is related to hiring professionals for the industry, for mid- to long-term periods, so they can share their experience in real-life environments and learn about testing methodologies that can be applied in their own company. This is already being done in some environments and is mutually beneficial both for the Testing Coordination Capability and independent companies.

3.5 Major constraints, risks, threats and limitations

3.5.1 Achieving trust is the most challenging organisational issue

It is difficult to overestimate the importance that respondents accorded to the need of building trust as a requirement for effective cooperation. But, at the same the time, it is considered to be the most difficult organisational issue, above the ability to work with such a diverse technological environment, establishing communication or providing results fast enough to be effective. Several activities are especially critical in this respect, such as vulnerability disclosures (see 3.6.3) or publications (see 3.4.4).

[21] A longer discussion of this topic can be found "Survey and interview analysis", section 5.2. and listed in : 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/survey-and-interview-analysis/view .

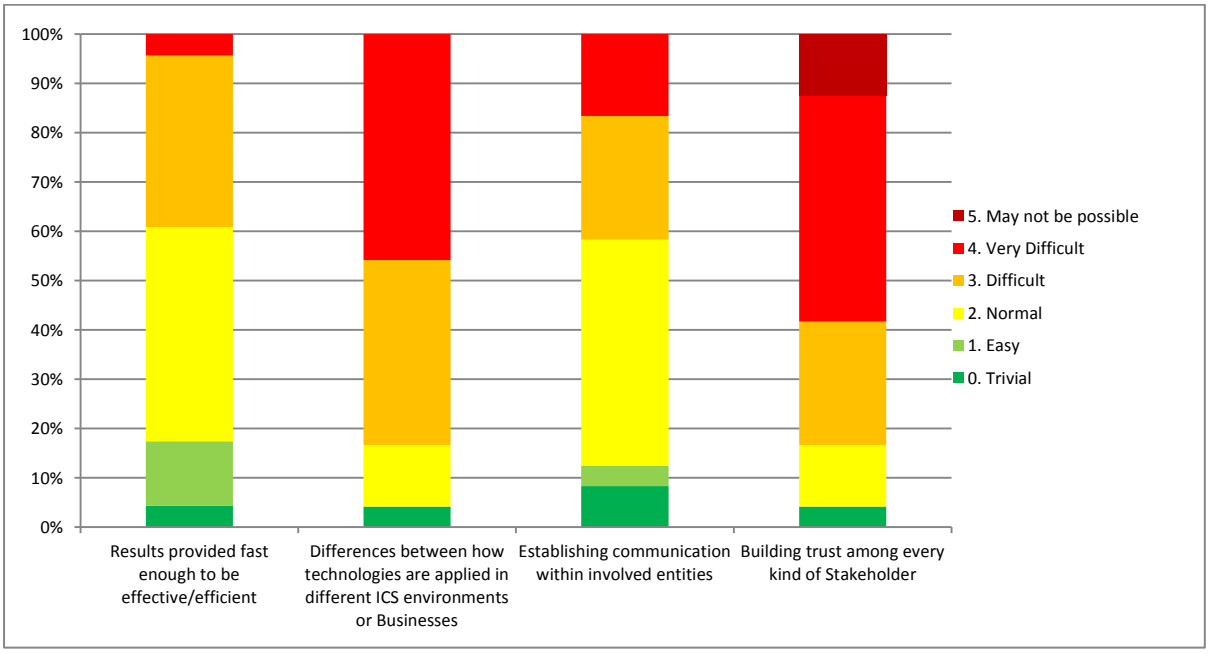


Figure 9: Most challenging limitations from an organisational point of view

3.5.2 Strategies for gaining trust are related to test bed independence

Many fear that some of the biggest companies, whose cooperation is indispensable, could either become too powerful within the organisation or break away from it. As both options are undesirable, most consider that the Testing Coordination Capability should take all parties into account while keeping a high level of independence (see 3.2.1).

Several alternatives have been proposed in order to enhance trust, such as conferring ownership and leadership to public bodies, arranging strong legal agreements (like NDAs), taking special precautions over key aspects concerning responsibility, and defining a set of clear participation rules. During the interviews some experts suggested that a pragmatic approach for this last point would be desirable to prevent independent private companies from participating directly in the Executive Board, while the correct approach would be to do so through representatives of consortiums and/or associations (see 3.6.1).

3.5.3 Diversity is the biggest technical challenge

When asked about technical issues, most experts think that the biggest challenges will come from the number of technologies involved and the different ways they are applied depending on the environment. This is also a factor to take into account, considering the comprehensiveness of tests (3.3.5) and speed of test results as a measure of success. Companies that request security checks will obviously want to have the results as soon as possible but this has to be in balance with their comprehensiveness, in a highly complex technological field.

When asked about the kind of assets or infrastructures that the centre should have, all types of equipment were considered decisive, which is consistent with 3.2.5, and can emphasise the interest of the stakeholders in performing 'holistic' approaches. Considering the fact that this could come at great economic expense, several experts have proposed focusing on smart, smaller and versatile testing premises.

3.5.4 Difficult agreement for testing methodologies is foreseen

Traditionally, standards used in the ICS industry have been more generalist guides than clear directives. To carry out good verification tests it would be necessary to find an agreement in the security criteria that, according to the experts, would be very difficult if not impossible. The diversity of technologies and points of view is expected to be pose considerable challenges, especially when taking into account that many legacy components are still in production and some others are much more evolved. In any case, some say, several of the most accepted references[22] in this field have been created without full agreement, have proven themselves effective and can be used as a starting point.

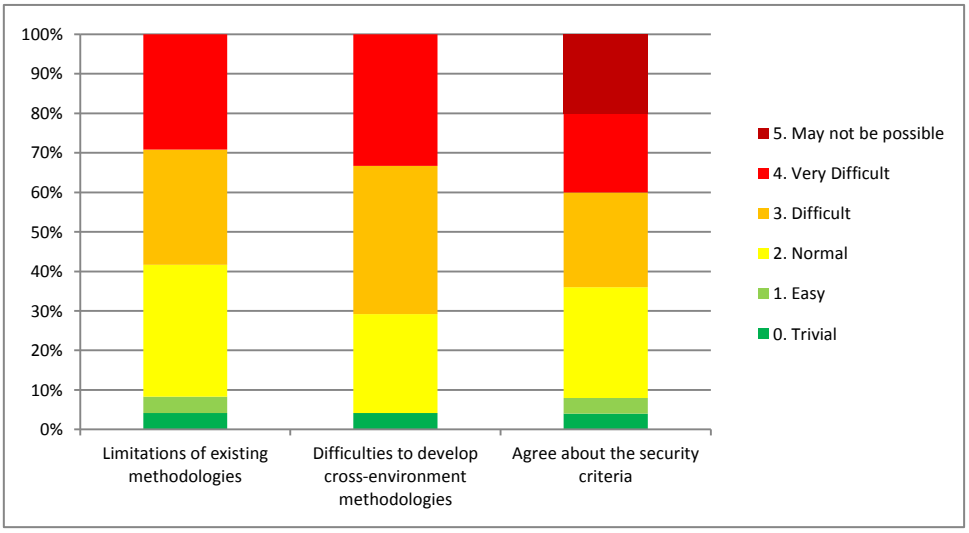


Figure 10: Most challenging limitations from a methodological point of view

3.5.5 Complexity of the legal environment among biggest challenges

During the interviews, some experts suggested that the biggest challenges will come from legal and regulatory considerations. The number of regulations applicable depending on Member State, sector, being considered a Critical Infrastructure or not, among other criteria, makes it very difficult to deliver clear guidance for ICS security testing practices and requirements. Some experts consider that the solution has to be defined at the political level, segmenting the problems when possible or getting requirements included in current regulations (see 3.2.3).

3.5.6 Need for an accurate economic model for public–private partnership

Following the logic of previous Key Findings (see 3.4.1 and 3.4.2), the experts consider that finding the financial resources for the initiative could be a delicate issue. Many public bodies across Europe are in a budgetary crisis and, as described, private funding can affect Testing Coordination Capability independency and, therefore, trust.

[22] Like ISA-99.

3.6 Relationships with other stakeholders

3.6.1 Representative composition of the Executive Board

It is commonly agreed that all stakeholders have to be taken into account in order to gain full value from the initiative (see 3.2.4). Interviewees with experience in leading similar initiatives noted that often single companies with particular interests block debates or try to move them in a certain direction for particular purposes. Those experts strongly advised not including independent companies in the Executive Board directly, but doing so through consortiums or associations that can represent any stakeholder group in a more effective way. Some experts of the same group also pointed out that trust is built through relationships, so they recommend keeping the representative membership as stable as possible over time.

3.6.2 Fluid communication with CERTs recommended

Most experts consider that the Testing Coordination Capability should keep fluid communication with relevant European and International CERTs at all times, but especially in case of emergencies. The CERTs could also provide guidance, act as arbiters, perform several communication tasks and help to increase stakeholders' trust. In addition, some of them are specialised in handling security incidents related to Critical Infrastructures such as UK-CNPI, CNPIC-es/INTECO-CERT (Spain).

3.6.3 Debate regarding the handling of vulnerability disclosures

Most stakeholders have strong opinions regarding vulnerability disclosures and how they should be handled. Several reasons, such as the need for trust and cooperation, preventing access to information by malicious agents, or just organisational reputation, are used to support a cautious use of this information. Some others consider that the information has to flow more easily, even with some restrictions, in order to resolve vulnerabilities or apply countermeasures.

The topic is highly sensitive for most experts and is considered as one of the keys for losing or gaining confidence. Non-disclosure agreements, anonymity in publications, following clear dissemination rules and delegating trusted organisations, such as public CERTs, are often quoted as reasonable options to follow.

3.6.4 Vulnerability resolution enforcement recommended by security test lab experts

Although they agree that it would be controversial, a few security test labs experts consider that it is necessary to provide the testing lab with some ability to enforce vulnerability resolution. This, they warn, could have a negative impact on trust and cooperation but otherwise some systems would continue in production even with exploitable critical vulnerabilities. Financial sanctions or disclosing those vulnerabilities after reasonable and previously agreed timescales are some of the options they propose.

3.6.5 Involve stakeholders in dissemination activities

It is considered interesting that the Testing Coordination Capability would cooperate in dissemination and awareness activities. Using existing initiatives in this field, involving existing stakeholders in eventual publications or guidelines or developing alert and notification systems in cooperation with CERTs are all considered to be worthwhile activities. However, all these activities have to be carried out with caution in order not to damage the stakeholders' trust (see 3.4.4 or 3.6.3).

3.6.6 Testing environment useful for educational purposes

As already stated, there is no real ICS security educational environment in the EU (see 3.1.2) and therefore it is advised that the work be performed by multidisciplinary teams (see 3.4.5). When asked about possible uses of the infrastructures for educational purposes, some suggestions such as 'providing professional certifications' or 'providing facilities' were rated positively. In fact, during the interviews, many experts noted that industry professionals have to be highly involved in knowledge sharing activities (see 3.4.6).

4 Recommendations

This section presents seven recommendations in order to reach independent ICS security testing coordination capabilities in Europe. These recommendations focus on national and pan-European initiatives that should be implemented as soon as possible. They are intended primarily for public bodies and authorities and specifically for the national and European ones. The recommendations are coherent amongst themselves and also with the activities performed by the European Union and ENISA (such as The Digital Agenda for Europe, the CIIP Plan, or the eventual creation of a European ICS CERT capability). However, they also target other stakeholders such as ICS manufacturers, integrators and operators, ICS security test labs experts, security tools and services providers, academia and R&D, and standardisation bodies.

The seven recommendations are related to each other in order to create a complete approach to improve testing capabilities in the European Union. This is the first step towards the creation of a Testing Coordination Capability able to deal with the most urgent requirements identified, with reasonable costs in terms of time and resources and integrated in the ICS Security environment.

An overview of the complete system is shown in Figure 11, including the main actors, tasks and relations between them.

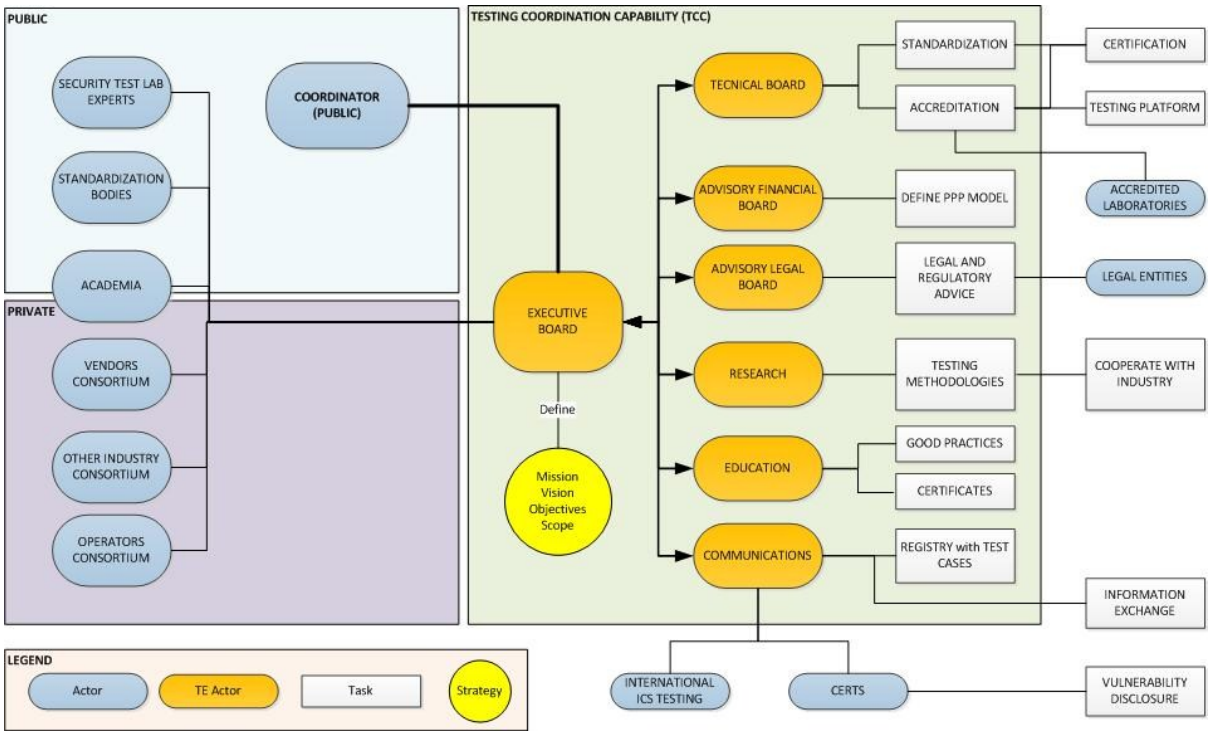


Figure 11: Overview of recommended Testing Coordination Capability

As the figure shows:

- An entity called Coordinator should foster Public Support for the initiative and involve other public and private organisations to cooperate (Recommendation 1: The creation of a Testing Coordination Capability under public European leadership) in the early stages of the initiative.
- These stakeholders and their representatives, under the lead of the Coordinator, would create a Working Group that would become the Executive Board, able to define the strategy

and further steps in the definition of the Testing Coordination Capability (Recommendation 2: The establishment of a trusted and functional Executive Board to enforce leadership).

- The Executive Board would then create (or engage already existing experts in order to create) thematic Working Groups for technical, financial, legal, research, educational or communications issues. (Recommendation 3: On the creation or involvement of working groups for specific activities)
- The working group in charge of the Financial Model, by now called 'Advisory Financial Board' would have to create a realistic business definition able to guarantee both sustainability and independence. (Recommendation 4: Definition of a financial model appropriate to the European situation)
- Within the responsibilities of the Technical Board, supported by the Executive Board, would be the study of feasibility of a distributed model of operation. Test methodologies and standards, and a clear accreditation model designed to engage current test beds and certification institutions would have to be developed. (Recommendation 5: Carrying out a feasibility study for a Distributed Model of Operation)
- Other entities such as CERTs, other international ICS Security Testing initiatives and, in general, any stakeholder have to have clear communication procedures with the Testing Coordination Capability. The communications group would design these protocols and operate them (Recommendation 6: Establish collaboration agreements with other organisations dealing with ICS security)
- Knowledge and expertise in ICS security testing is still scarce and has to be fostered by involving professionals from the industry, research and education. This can be addressed altogether under an umbrella of Knowledge Management programmes. (Recommendation 7: Establish a knowledge management programme)

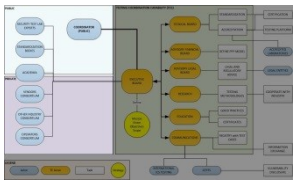
The detailed descriptions of the recommendations below are structured as follows[23]:

- Description: where the core content of the recommendation is presented. This can be considered as the 'what' and the 'how' parts of the recommendation.
- Objective: provides a more detailed description of what would be the benefits of this recommendation.
- Steps: suggests a number of possible phases to successfully implement the recommendation. Some of them are emphasised as they are considered 'quick wins', being activities that can be effectively achieved in the short term and have an impact.
- Measures of success*: suggests a number of metrics to evaluate the achievements of the recommendation.
- Alternative*: this section presents possible alternatives to the core proposal described in the 'Description' section.
- Stakeholders affected: It provides information concerning the stakeholders for whom each the tasks of the recommendations is specially addressed. 'Leading' entities are intended to take initiative and decisions, 'cooperating' ones would have to develop specific tasks including actions or documentation delivery, 'consulting' stakeholders would only be considered for informational aspects.

[23] The ones marked * are optional

4.1 Recommendation 1: The creation of a Testing Coordination Capability under public European leadership

4.1.1 Description



Although it is commonly accepted that the ICS Security Testing Coordination Capability should work under a public–private partnership (PPP) model at a financial level (see Recommendation 4.4), there are several reasons to recommend a prominent role for public administrations. This recommendation proposes that public administrations should act as coordinators, taking the lead for some of the most critical duties of the organisation, such as defining the Executive Board (Recommendation 4.2), that would consolidate the strategy and operations management which are key factors for building trust and independence. In other words, it is recommended that the European Union keeps itself as the main coordinator of the institution.

Their main responsibilities are explained in detail in further Recommendations but include:

- Define all Strategic Goals, Mission, Vision and Objectives of the Testing Coordination Capability as well as managing its lifetime activity. (Recommendation 4.2)
- Set the lines of work to find an adequate Financial Model and Business Plan that can be sustainable over time. (Recommendation 4.4)
- Centralise and manage communication issues with European or foreign organisations and populations. (Recommendation 4.6)

Many of the key findings of this project support this recommendation directly or indirectly. Most of the experts expressed a belief that public institutions have to be highly engaged to enable the creation of such a Testing Coordination Capability and to set the conditions for success. The strong funding needed in the early stages, added to the uncertainty of obtaining a return on investment, makes it very unlikely that private organisations will get involved in the initiative at the required level. Moreover, some private companies are reluctant to share their knowledge and resources for competence reasons and will prefer to wait in the first place and see if it is really of interest. But, as recent history has shown, once the necessity is understood[24] and once it is supported with strong political will, resources are granted.

There are also several practical reasons that help justify the preeminent role of the public sector, of which the main ones are:

- Public bodies are more likely to encourage trust among stakeholders as they do not operate according to market competition rules.
- They can directly or indirectly act as a recognised arbitrator in eventual conflicts.
- In helping to align efforts, public bodies involved would have direct links to regulators and institutions that are also part of the public sector.
- The public bodies involved would be able to apply more pressure to guarantee successful cooperation with other public initiatives, research programmes, as well as standardisation or incident response activities.

[24] Something that, unfortunately, usually happens after dramatic events such as 9/11 or the 2011 Japanese earthquake and tsunami (see 3.2.2)

- They can operate as a clear point of contact for public or private institutions anywhere in the world, something that would be very much appreciated by the industry.
- Stakeholders such as utility operators and companies, as well as some CERTs, are in some cases public entities or receive public funding.

In addition to these arguments, there are other roles the public sector could play in such a Testing Coordination Capability. These are not recommended for the short term, but for the longer term, once the maturity level of the Testing Coordination Capability allows it. These roles include:

- The legal capacity to require testing of some ICS systems and environments on a mandatory basis under certain circumstances. This should be supported by new European mandates and/or by incorporating cyber-security control objectives in current regulations. In any case, a strong commitment of public institutions is envisioned.
- The ability to enforce[25] vulnerability fixing or the establishment of compensating mitigation measures or safeguards.

In any case, all stakeholders should be engaged to cooperate at all stages, from the definition, creation and establishment of the body to its daily operation of the ICS Security Testing Coordination Capability. Their knowledge, vision, requirements and feedback have to be taken into account at all times. As a matter of fact, they are intended to be direct beneficiaries of the Testing Coordination Capability activities, so that they are able to provide, or help to provide, reliable and secure services to citizens and companies.

4.1.2 Objectives

There are several high-level goals that can be easily achieved through public leadership:

- Define clear objectives, tasks and responsibilities of the Testing Coordination Capability.
- Help in unifying and harmonising efforts across the European Union.
- Win trust among stakeholders.
- Grant independence from private interests.
- Cooperate with other initiatives to foster ICS security in the EU.

4.1.3 Steps

Quick Win 1: The Coordinator for the Testing Coordination Capability would contact relevant Stakeholders and become a clear Point of Contact for any interested entity.

- At European Union level, recommend the creation of an ICS Security Testing Coordination Capability aligned with current National Security Strategies to obtain political support.
- Invite most relevant stakeholders for a leading working group of experts (see Recommendation 4.2) envisioned as an Executive Board to define the main strategic, economic and cooperative lines.
- Coordinate activities within internal groups and with external entities.

[25] Through sanctions, vulnerability disclosures, etc. The topic is mentioned in KF 3.2.6 and discussed in "Survey and interview analysis" and listed in : 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/survey-and-interview-analysis/view .

4.1.4 Measures of success

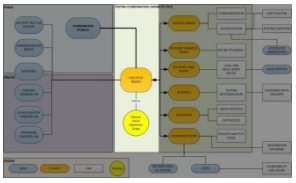
- Measure of satisfaction: The results of the different activities must be useful for all involved members. In order to achieve this, impartial and competent results including actionable findings have to be provided.
- Degree of involvement and trust: All types of stakeholders, both public and private, should demonstrate their commitment by contributing to the initiative with different resources, including cooperation and knowledge.
- Level of agreement: Regarding the activities and statements specified in the strategies.
- Tracking the validity of their long-term strategies: Accepting that they need to be flexible and adaptable, they must be coherent, with clearly defined, long-term objectives.

4.1.5 Stakeholders affected

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

4.2 Recommendation 2: The establishment of a trusted and functional Executive Board to enforce leadership

4.2.1 Description



As described in Recommendation 4.1, once political support is granted, the next step is to create a working group, intended to eventually become the Executive Board of the Testing Coordination Capability. This board should have representatives from all relevant stakeholders involved in the ICS industry and should be led by a European Public Organisation.[26] Members of the working group – and eventually of the Executive Board – should include recognised experts in any field of the ICS world, for example business issues, political or legal matters, standardisation initiatives, technical and research aspects, etc. This will grant the WG/Board a clear understanding of the complexity of the situation, of stakeholder needs, and of the challenges to overcome as well as of the necessary resources to be put in place. At the same time, it will streamline the alignment of the Testing Coordination Capability activities and strategies with current and future regulations and standards.

It is strongly recommended not to accept private companies as members of the board/WG on an individual basis. Representatives from existing consortiums or associations would be very much preferred, regardless their size or presence in the market. This is intended to ease decision-making and to foster cooperation as single interests lose weight against common benefits. Regarding the

[26] See Recommendation 1 in section 4.1.

procedure, existing Good Practice for Information Sharing Exchanges[27] can be followed. It is also strongly recommended to take advantage of operator capabilities as driver agents in the market (see 3.1.5). Their needs and suggestions have to be taken into account so cooperation can be achieved, but granting a balance of power within the community.

The main duties for this Executive Board would be:

- To define the strategy of the Testing Coordination Capability, defining its Mission, Vision and Objectives.
- The Executive Board should provide governance and oversight of the operations for the EU ICS Testing Capabilities to include vision, financial oversight, operations oversight, and periodic review of the performance of the different capabilities.
- To define the Entity strategy to implement the Mission and Vision, and to achieve the objectives in a highly competitive environment. Such a European Testing Coordination Capability needs to find its place by providing its own added value, filling the gap left by existing test bed initiatives in order to attract private interest. In this sense, it is considered that, once the objectives are established, some room has to be left so the stakeholders can develop their own creativity and innovation.
- To lead, or at least arbitrate in, any activity that requires agreement from all stakeholders, for instance the definition of the operational model, the financial model, the lifecycle and improvements of test bed activities, research and educational initiatives, etc.
- To assign specific activities to future working groups. These new panels of experts could be created on an ad-hoc basis or engaged from existing initiatives across Europe. It is reasonable to consider that some of these working groups could eventually be integrated within the structure of the Testing Coordination Capability. (More details in Recommendation 4.3.)
- To ensure that all activities will add value to the entities involved.
- To determine whether to constitute a certification framework along with testing facilities. As demonstrated, many stakeholders, particularly operators, have shown interest in this subject, but it remains unclear what and how to certificate. Although, on some levels, this has to be answered by technical and legal experts (see Recommendation 4.3) there must be a general strategy to follow in this regard.
- To assume, at least during the early stages, communication tasks with related entities. Later, this obligation may be delegated to a department within the Testing Coordination Capability.
- To contribute to raise awareness and share knowledge within the European or international ICS community.

In order to gain trust and respect from the ICS Community, the Testing Coordination Capability's Executive Board should:

- Demonstrate their independence from particular benefits and equity and common interest in their decisions, even if acting as an arbitrator when necessary. Public leadership should help in this regard.

[27] See Reference [51]

- Grant that all stakeholders are represented and their visions taken into account by allowing them to be part of the Executive Board or by getting them involved in any of the future/delegated working groups.
- Define clear participation rules and legal agreements for any cooperation tasks.
- Favour a sustained panel of experts, so that common understanding and cooperation can be achieved easily also through human factors.
- Operate by clear and agreed rules as well as with extreme caution when sharing critical information, for instance on vulnerability disclosures or security testing results.[28]

4.2.2 Objectives

- Achieve a clear definition of the organisation objectives.
- Ensure representation from all stakeholder types.
- Harmonise activities and maintain them aligned with the needs.
- Enhance trust.

4.2.3 Steps

Quick Win 2: The Coordinator would state clear participation rules for the Testing Coordination Capability.

Quick Win 3: Stakeholder representatives would be engaged for the Executive Board working group.

Quick Win 4: The Executive Board will define a common strategy for the Testing Coordination Capability.

- A working group for the definition of the ICS Security Testing Coordination Capability should be created.
- The working group agrees on general strategy matters and available resources.
- It also defines the subgroups to be created or engaged to develop a functional model for the Testing Coordination Capability.
- Once the Testing Coordination Capability gets constituted and the working group is turned into the Executive Board, which will devote itself to top management activities.

4.2.4 Measures of success

- Degree of involvement and trust: All types of stakeholders, both public and private should demonstrate their commitment by contributing to the initiative with different resources, including cooperation and knowledge.
- Level of agreement: Regarding the activities and statements specified in the strategies.
- Tracking the validity of their long-term strategies: Accepting that they need to be flexible and adaptable, they must be coherent, with clearly defined, long-term objectives.

[28] This has been described in KF 3.4.4, 3.6.3 and 3.6.4.

4.2.5 Alternative

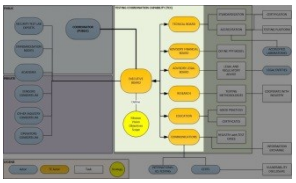
Another option instead of contacting consortiums is to request information directly from companies and enterprises, but it is expected that the measure of success will be lower.

4.2.6 Stakeholders affected

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

4.3 Recommendation 3: On the creation or involvement of working groups for specific activities

4.3.1 Description



The European Organisation or Agency with the leading role in the creation of the Testing Coordination Capability, assisted by the Working Group – which would eventually be transformed into the Executive Board – would have to set up a series of activities to implement the mission and vision of the body and to achieve its main goals.

As explained,[29] the need for an ICS Security Testing Coordination Capability is so pressing that several initiatives (public, private or in the form of PPP) have emerged within the different Member States. In order to build an efficient and effective ICS security testing coordination capability with a European vocation, such initiatives should continue – with efforts coordinated for efficiency and harmonisation reasons – while new ones will have to be created as well.

Although the final list of necessary activities – and related working groups and initiatives – to implement the Mission, Vision and main objectives of the Testing Coordination Capability will have to be determined by the competent authority, some of them could be inferred during the study and include:

- Technical Board: One of the most important initiatives would be the creation of a working group (to be named Technical Board) in charge of dealing with the many technical challenges of the Testing Coordination Capability, as for instance:
    - How to design cost-efficient and versatile infrastructures that could generate widely accepted and actionable results.
    - Agree on the testing methodologies and security criteria to be considered.
    - Face the diversity of technologies and particularly consider legacy and *state of the art* interactions.
    - Be able to follow 'holistic' approaches when analysing the security of ICS systems and components.

[29] See Key Finding 3.1.1.

- Merge the OT and IT vision simultaneously.
- Generate consistent as well as creative results that will need to be updated over time.[30]

Some groups in the European Union, such as the ERNCIP, ENCS, EuroSCSIE or SCADALab, among others, are already working on these topics and should be taken into account.

- Communications department: Once the Testing Coordination Capability has been established, a group of professionals should be in charge of promoting the work of the centre (for example through the publication of reports) and of managing communications with third parties, such as partners, collaborating entities, CERTs, press, etc. (More details in Recommendation 4.6.) A very important task for this group would be to establish procedures to deal with newly discovered vulnerabilities or potential security breaches, as well as deciding an adequate time window for their disclosure (if appropriate and agreed).
- Advisory board on financial issues: If the leading Public Institution and/or the Executive Board requires assistance, an ad-hoc working group should be created to support them during the development of a realistic financial model (as described in Recommendation 4.4).
- Advisory board on legal and regulatory issues: It is commonly agreed that the legal and regulatory framework affecting ICS is a matter of great complexity. They depend on Member States' specificities, types of businesses, technologies involved, services provided, European Community law and its transposition to national law (e.g. European Programme for Critical Infrastructure Protection and national CIP laws), etc. An advisory board dealing with legal and regulatory issues and harmonisation will certainly be useful. Activities, such as defining non-disclosure agreements (NDA), or studying whether and how a vulnerability fix can be enforced could be part of their daily responsibilities. Furthermore, if testing activities are eventually considered mandatory due to a new regulation, or if it becomes common practice in the industry because of tacit industrial mandates, this board could play an important 'controlling' role.
- Research teams: It should be considered that the Testing Coordination Capability conducts periodic research activities to improve techniques, tools, methodologies and procedures for testing the security level of ICS. Researchers from academia could be considered important members of the research teams to be created.
- Educational activities: The Testing Coordination Capability should be a reference centre for educational activities on ICS Security. Even though it might not be a priority in early stages, the Testing Coordination Capability could provide a unique environment in this regard, for both current security professionals and future ones. A number of internal or external experts could be engaged for this purpose.

The aforementioned teams of professionals could be part of the structure of the Testing Coordination Capability or engaged from the industry[31] for specific projects or periods of time. This means that the procedures for hiring or dismissing personnel have to be clearly defined. In any case, the European Organisation to lead the Testing Coordination Capability should retain the power to revoke cooperation with other entities at any given time.

[30] Some of these challenges can be approached by proposed techniques mentioned in Recommendation 4.7.
[31] See Recommendation 4.7.

4.3.2 Objective

- Achieve efficiency and harmonisation.
- Employ expertise in all fields necessary for Testing Coordination Capability activity to ensure, within possible, that the challenges can be overcome.
- Involve the industry and Member States.

4.3.3 Steps

Quick Win 5: Current initiatives in ICS Security Testing will be officially contacted in order to establish more specific cooperation tasks.

Quick Win 6: Working groups would define the testing methodologies and criteria that are more closely aligned with the strategy.

- The Executive Board should define the members of specific working groups.
- Tasks and duties will be cascaded and valuable information should flow within groups.
- Review of activities to endorse working groups or already existent initiatives

4.3.4 Measures of success

- Number of problems solved and average time to solve the tasks.
- Degree of satisfaction with the resolution of the different tasks.

4.3.5 Alternative

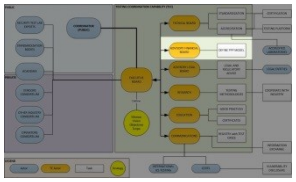
Legal and Regulatory group could be subcontracted within a network of local consultants or public institutions.

4.3.6 Stakeholders affected

- Security Test Lab Experts: **Leading** Technical board, cooperating in research and education tasks
- Manufacturers and integrators: **Leading** in financial issues, cooperating in the rest
- ICS Security tools and services providers: cooperating
- Operators: **Leading** in financial issues; cooperating in the rest.
- Academia and R&D: **Leading** in educational and research tasks
- Public bodies: **Leading** in Communication tasks, Financial and Regulatory issues; cooperating in harmonisation tasks
- Standardisation bodies: cooperating

4.4 Recommendation 4: Definition of a financial model appropriate to the European situation

4.4.1 Description



Creating a Testing Coordination Capability on ICS cyber-security in the European Union would require a large investment, even if we take advantage of existing resources. The initial investment required for its implementation alone will be substantial. To this must be added the investments and costs of daily operations. In this regard the diversity of the technologies covered will have a decisive influence. Furthermore, it is also important to take into account the current economic environment, particularly sensitive at budgetary level for many Member States. Therefore, it is not unreasonable to speculate that achieving the necessary funds for the creation and operation of the centre is one of the critical points for the success of the initiative.

Although it is recommended that the body should be created and operated under public ownership and leadership (see Recommendation 4.1), most experts contacted during the study agree that the Testing Coordination Capability should follow a public–private partnership model.[32]

It is recognised that large private companies could provide substantial funding, especially vendors and operators, and it would make no sense to give up this funding when they are beneficial for both the general interest and the private sector. In this regard, there are many reasons why private companies would participate in such an initiative. For example, security testing can help them improve security specs and functionalities in their products, reduce risks in their organisations, decrease their own testing expenses, check for interoperability[33] with other vendors, achieve security seals and certificates, and simplify the requirements to sell or operate in the European Union, among others.

Although the Testing Coordination Capability may offer many attractive and marketable features to the private sector, it is unlikely that private companies would spontaneously take over the bulk of the investment in the early stages of the process. Most similar experiences worldwide initially received the largest investment from public institutions, often from Homeland Security (or the equivalent ministry) or Industry departments (or the equivalent ministry). Moreover, in the few similar experiences of success, a strong political will[34] has ensured stability in early stages and has also been shown to be fundamental in sustaining them over time (see Recommendation 4.1). This is due to various reasons, but probably the most important one is the ability to build trust and ensure the independence, which would be lost if large private companies had much influence within the proposed initiative.

For this reason, it is recommended to establish a well thought out and well designed financial model, as it is not only necessary to obtain funding, but also to ensure the centre's independence. This model should be compatible with the fundamental goals of the centre, including adding value to stakeholders and increasing the level of security in the ICS arena. It would have to take into account all expenses such as equipment, staff, laboratory, representation, operational and administrative costs, and balance them with potential incomes. The financial model should consider that, in some cases, private companies could help reduce investments and expenses by sharing their own devices, sending their own technical staff to collaborate, help in developing publications, etc. Moreover, a

[32] In fact, some consider that it should be completely public, and most disagree about the idea of making it 100% private.
[33] At least, when it affects security.
[34] See note 24.

thorough analysis is required to identify possible sources of funding, which may include budget from the EU and/or Member States, charges for certification and/or audit, income from the sale of reports, sponsorships and membership payments, income from ad-hoc projects, etc. In the long term, if security tests are declared mandatory, funding policies would probably have to be reviewed since the private sector would probably expect that most costs should be charged to citizens.

It is important to consider that a European Testing Coordination Capability would have to operate in an international competitive environment, where other similar initiatives are already working (see Recommendation 4.6). There must be valid reasons for international entities to choose the European test bed instead of other more mature alternatives in the market. Likewise if a distributed model is chosen (see Recommendation 4.5), some of the potential customers would be more keen on making use of the testing facilities than others. The return on investment could be speeded up if such facilities are set up in the early stages of the centre.

4.4.2 Objectives

- Ensure economic sustainability for the test bed
- Grant stability during the creation and first years of the maturity process
- Find a balance between public and private funding
- Foster the creation of marketable value and competitive advantages
- Involve all stakeholders

4.4.3 Steps

Quick Win 7: Working groups involved will identify potential sources of funding and develop a business plan.

- Test entity leaders to start identifying the bodies to be responsible for the creation of the Financial Model, which may or may not be among its members.
- The committee would propose a financial model aligned with the objectives of the test bed and realistic in terms of the economic situation. This study should take in consideration different alternatives and their feasibility.
- The Executive Board would approve and establish the Financial Model and will agree further steps.

4.4.4 Measures of success

- Economic stability during the first years of existence
- Progressive and controlled income from private companies
- Customer satisfaction with the results, in line with their market value
- Sustainability of the test entity over time
- Maintain the level of independency

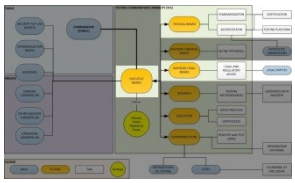
4.4.5 Stakeholders affected

- Security Test Lab Experts: *consulting*
- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating or *consulting*
- Operators: cooperating

- Academia and R&D: *consulting*
- Public bodies: **leading**
- Standardisation bodies: *consulting*

4.5 Recommendation 5: Carrying out a feasibility study for a Distributed Model of Operation

4.5.1 Description



The European Union, its Member States, policies, companies, regulations, standards and even individual security testing initiatives make up a very complex landscape. Harmonising existing initiatives and implementing the mission and vision of the Testing Coordination Capability as well as achieving its main objectives could be daunting tasks. However, Europe can take advantage of its own size and heterogeneity to follow a distributed approach/ model and achieve success. Such a distributed approach would mean having a number of distributed centres coordinated by a single public organisation (see Recommendation 1, section 4.1), with the ability to accredit existing and national ICS/CIP testing facilities and/or certification authorities as 'centres of excellence' for very specific areas of ICS security testing knowledge.

The Executive Board (see Recommendation 2, section 4.2) would have to identify and define different accreditation types, based on the different activities that those centres should cover and making the most of their heterogeneity, avoiding forcing them to work as pure clones. Stated another way, a set of duties would have to be defined and centres would have to be accredited accordingly. During the study it was not clear what different duties should be considered and how they should be grouped. This is why this is suggested to be a task for the Executive Board and supporting working groups (see Recommendation 3, section 4.3).

The benefits of such a model include:

- Some of the existing initiatives can be engaged, taking advantage of their experience but also helping them improve and grow.
- The Testing Coordination Capability would be closer to the industry as it relies on well-known and trusted initiatives. Many potential customers would probably feel more comfortable and keen to collaborate with the Testing Coordination Capability if they are already familiar with it.
- The costs of the advice on legal and regulatory issues, promotion efforts, or any other matter of common interest could be shared by the centres. Obviously, the alternative is that local offices themselves outsource these tasks to third parties (e.g. consulting companies).
- If centres were accredited by periods of time, the quality of the assessments would be higher and favouritism would be avoided.
- Member States would be more favourably disposed to promote and invest in centres located within their borders.
- If segmented by type of business, centres could specialise in different fields of expertise. This would allow for a deeper understanding of the businesses and their specific needs, and would help to face the challenge of technological diversity and multiple use cases.

- Regarding the debate about the adequacy or subject of certification,[35] it could be interesting, as an option, to accredit certain centres to be specialised in controls such as security postures or quality assurance.

In order to minimise the impact of the intrinsic weaknesses of a distributed model,[36] some control mechanisms should be put in place to assure that the quality of the results is consistent among centres, that the testing methodology and results are homogeneous, etc.

4.5.2 Objectives

- Find a suitable model for the EU complexity.
- Have a faster model to get into production.
- Adapt testing procedures for specific needs.
- Expertise can focus on both technical and legal issues.
- Maintain the quality of testing over time.
- Involve Member States.

4.5.3 Steps

Quick Win 8: ICS Security Testing accreditation criteria will be defined.

- Set an accreditation model aligned with the objectives that the Testing Coordination Capability has agreed.
- Have defined which other testing labs, test beds, testing facilities and test tasks can temporarily be attached and included for specific test cases.
- Define the segmentation model criteria.
- Define the criteria for inclusion of new test facilities and how to handle when test centers lose their accreditation.
- Call for existent initiatives and testing bodies that are likely to participate and create open procedures for potential applicants.
- Put into place the model and keep the lifecycle.

4.5.4 Measures of success

- Contrast the efficiency for each facility in its field of expertise. Take into account the acceptance of the results, the value provided and cost.
- Measure the quality and homogeneity of the results.

4.5.5 Stakeholders affected

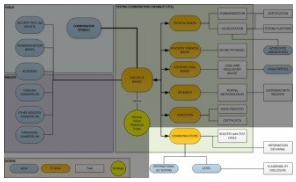
- Security Test Lab Experts: **Leading**
- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: *consulting*

[35] See KF 3.3.2 .
[36] A short discussion on this can be found in "Survey and interview analysis", sections 4.6 and 4.7 and listed in: 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/survey-and-interview-analysis/view .

- Operators: cooperating
- Academia and R&D: *consulting*
- Public bodies: **Leading** or cooperating
- Standardisation bodies: cooperating

4.6 Recommendation 6: Establish collaboration agreements with other organisations dealing with ICS security

4.6.1 Description



There are several interesting initiatives on ICS security testing across the European Union. These initiatives are somewhat immature and follow different approaches and techniques. The lack of coordination often results in inefficiencies, lack of coherence and the loss of potential and beneficial synergies. On the other hand, outside Europe, equivalent initiatives have achieved significant status and have abundant resources. Nevertheless, this is still exceptional. For these reasons, existing European initiatives[37] should be coordinated at different levels while preserving individual interests.

The European Testing Coordination Capability should be able to establish and support communications with and among the aforementioned initiatives across the EU,[38] as well as to act as the main point of contact for foreign organisations. In the medium term, cooperation agreements could be negotiated, in order to achieve a more efficient, highly specialised, and less costly operation, through technical development and knowledge sharing. It is important to determine then the kind of services that could still be improved, so as to gain a differential advantage, and become a reference for worldwide organisations.[39] It would be important to acquire and keep enough capabilities and resources in order to prevent excessive dependencies from such parties, since they can have different objectives. Moreover, any activity outsourced (e.g. specific security tests) should count on alternatives – either local or foreign – to minimise the impact in case it becomes unavailable or does not perform as expected for whatever reason.

Collaboration agreements should not be restricted only to ICS testing initiatives but should also be extended to other organisations dealing with ICS security. Standardisation organisations and regulatory bodies should be taken into account to align the Testing Coordination Capability's activities with current cyber-security guidelines, good practices and regulations and avoiding reinventing the wheel by developing new ones. Likewise, research centres and academia should also be considered. They could help improve current ICS cyber-security testing methodologies and develop advanced tools. Moreover, by opening new fields of research the Testing Coordination Capability could achieve the aforementioned differential advantage as well as be involved in world-class educational activities.

[37] e.g. ENCS, ERNCIP, EuroSCSIE, SCADA Lab, etc.

[38] Of course, if the Executive Board includes representatives of existing consortiums, this collaboration would be already in place.

[39] For some discussion regarding the space for improvement of foreign entities, see "Survey and interview analysis", section 5.2 and listed in: 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/survey-and-interview-analysis/view .

Another valuable collaboration space would be with CERTs and National Law Enforcement bodies.[40] There are highly interesting mutual benefits for both the Testing Coordination Capability and the emergency response teams. Such collaborations would help to visibly improve the security level of ICSs in the EU as well as the response times in managing cyber-security incidents that affect them. This is also coherent with existing efforts such as ENISA's initiatives to coordinate and enhance CERTs.[41] Furthermore, a hypothetical EU-wide ICS-CERT[42] would be an obvious candidate to perform critical activities such as disclosing vulnerabilities discovered by the Testing Coordination Capability, or helping identify which systems need to be reviewed from a security perspective.

4.6.2 Objectives

- Gather know-how.
- Avoid losing independence
- Get aligned with standardisation organisations and regulatory bodies to streamline the adoption of existing security requirements and avoid reinventing the wheel.
- Improve effectiveness of response to detected attacks, potential exploits, newly discovered vulnerabilities or general failures.

4.6.3 Steps

Quick Win 9: Non-Disclosure Agreements and other legal requirements to be elaborated.

Quick Win 10: Current CERTs would be contacted for specific cooperation, including Vulnerability Disclosures and incident response.

- Establish communication with identified entities.
- Study their approximations, determine gaps and overlays.
- Determine how to reach mutual agreements.
- Include a department for communication duties.
- Participate in ICS Security initiatives and events.

4.6.4 Measures of success

- Determine the time to get into production.
- Measure the level of satisfaction about cooperation both internally and externally.
- Determine the value of research and educational activities.
- Define metrics for cooperation in incident responses.

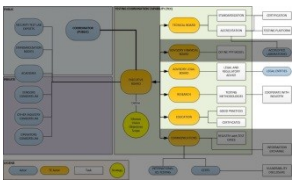
[40] Europol, Interpol, EC3, and the National Law Enforcement bodies have the responsibility for cybercrime/ cyberterrorism investigation and prosecution of attacks against critical infrastructure.
[41] 'Harmonisation of ENISA national/governmental CERT (n/g CERT) capabilities scheme and good practice for ICS CERT capabilities', 'Secure communication solutions for n/g CERTs: Stocktaking & Requirements', 'EISAS – Deployment study', 'ENISA CERT exercise material extended with cybercrime scenarios', 'Good Practice Guide on the practical implementation of the "Directive on attacks against information systems"' or 'Best practice guide on alerts, warnings & announcements + collection of incident response methodologies'.
[42] Some steps are being taken in this direction, such as the ENISA 'Harmonisation of n/g CERT capabilities scheme and good practice for ICS CERT capabilities'.

4.6.5 Stakeholders affected

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

4.7 Recommendation 7: Establish a knowledge management programme for ICS testing

4.7.1 Description



One of the biggest challenges of the Testing Coordination Capability will be to generate sufficient value for stakeholders. Important measures of the success of the Testing Coordination Capability, such as 'acceptance of the results' or 'comprehensiveness of tests', can only be achieved if its personnel have a high degree of expertise. As technologies change at an increasingly faster rate, the Testing Coordination Capability needs to keep the pace by constantly learning and self-adapting.

On the other hand, existing private initiatives on ICS security training are in the early stages, there is no specific training programme on this subject in Europe as yet,[43] and at the same time most current professionals working in this field come from two very different areas of competence: either they have a pure SCADA/ICS background, or a biased IT cyber-security one. This often leads to misunderstandings, as their points of view and even the language they use frequently differ. However, both profile types will be needed in the Testing Coordination Capability. In fact, even specific competences such as knowledge by business type (e.g. nuclear, power distribution, water treatment, railway transportation, etc.) or on 'wrong data models' [44] will probably be necessary as well. In this respect, the creation of a 'base of knowledge' of testing cases could be of interest.

Based on all this, we recommend that the Testing Coordination Capability defines and establishes a knowledge management programme which should consider the creation of heterogeneous teams of experts as well as put into practice knowledge management techniques focused on developing, keeping and exchanging know-how within the Coordination Capability Working Groups and

[43] Although some efforts are being made in this area by the ENCS in the Netherlands or INTECO cyber exercises in Spain, among others. These types of initiatives have to be taken into account by the ICS Testing Coordination Capability.

[44] This refers to tests that check the system behaviour under abnormal conditions in a very wide sense, so they are more difficult to standardise. There is a short description and discussion in "Survey and interview analysis", section 2.1 and listed in: 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/survey-and-interview-analysis/view .

collaborating organisations. Furthermore, this programme should also identify and evaluate educational activities and courses of interest in order to adequately train staff members.[45]

In regard to the aforementioned heterogeneous teams, the programme should consider engaging professionals from the industry. Thus, there would be two major classes of personnel:

- On one hand, public employees, officers or subcontractors, as permanent members of the structure, so they can retain the experience and knowledge and fully understand the mission, strategy and procedures of the Testing Coordination Capability. It would be of particular interest to promote their skills through courses, seminars and/or exchanges with other existing initiatives.
- On the other hand, experts from private companies, whether hired or transferred in order to participate in testing activities. This temporary staff should be working in the Testing Coordination Capability for reasonable periods, which may vary from a few months to several years, or even be engaged for specific projects as needed. The advantage of the longer periods of time is that, once the stage is finished, those professionals become more knowledgeable in ICS security testing and its environment, which could provide high value to companies that are willing to cooperate with the Testing Coordination Capability.

This convergence should lead in the medium to long term to a homogeneous environment where IT and OT are merged, with highly specialised technicians and managers for ICS and ICT environments, leading to procedures where information flows more easily and securely among them.
Finally, as part of the knowledge management programme, consideration should be given to possibility of issuing certificates for professionals that are involved in the ICS security activities of the Testing Coordination Capability. This could vary from simply certifying their participation in educational sessions, to even temporary memberships, although it is not considered necessary to overstretch the co-location of training and education facilities.

4.7.2 Objectives

- Gather current knowledge from existing testing bodies and industries in order to create a multidisciplinary (for technicians and managers alike) knowledge base.
- Develop and ensure that know-how is kept within the Testing Coordination Capability
- Return knowledge back to the industry, increasing security expertise in the ICS environment.

4.7.3 Steps

Quick Win 11: Experts from the industry would be engaged.

Quick Win 12: A base of knowledge with testing cases, types and procedures would be created.

[45] See Recommendation 4.6.

- Establish responsible and permanent staff through the Technical Board (from Recommendation 4.3).
- If necessary, provide resources for permanent staff members to follow existing trainings.
- Acquire temporary staff members from industry.
- Store the gathered know-how (manuals, white papers, etc.) in a structured, access-controlled knowledge base.
- Put into practice knowledge management techniques to share, maintain and increase know-how.
- Research in testing methodologies, in collaboration with stakeholders from academia (see Recommendation 4.6).
- Publish methodologies and lessons learnt as a way to share them with the community.

4.7.4 Measures of success

- Quality from testing increases in comprehensiveness, acceptance of results, amount and criticality of vulnerabilities, etc.
- Evolution in the maturity of testing methodologies.
- Number and quality of documentation regarding the published methodologies of testing.
- Number of experts involved.
- Satisfaction for companies that transfer their experts.

4.7.5 Stakeholders affected

- Security Test Lab Experts: **Leading** for internal training
- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: **Leading** for research and education
- Public bodies: cooperating
- Standardisation bodies: cooperating

5 Conclusions

During the study many interesting topics, debates and different points of view arose. But there are some conclusions that can be summarised.

Although many organisational issues are still a matter of discussion and there are still many challenges to overcome, it is clear that the fifth recommendation from ENISA's 2011 document *Protecting Industrial Control Systems – Recommendations for Europe and Member States* about the 'Creation of a common test bed, or alternatively, an ICS security certification framework' has been strongly endorsed by the wide majority of the experts. In fact, many countries are already working on it. According to the experts, the question now is not whether it is necessary or convenient to unify efforts in ICS Security Testing across the EU, but what are the best means to achieve it.

This can be considered to be included within the actions that the European Programme for Critical Infrastructure Protection (EPCIP) created by European Commission and the Council of Justice and Home Affairs.

In parallel, the information security issues for vital infrastructures in Europe have been addressed by The Digital Agenda for Europe (DAE) and the Critical Information Infrastructure Protection (CIIP) action plan. Specifically, the last Communication on CIIP, CIIP COM(2011)163, targets ICS security.

Many topics are, and are likely to remain, a matter of debate. But the need for cooperation, information sharing and engagement from all stakeholder types is not in question. In an environment with ever-increasing risks, where highly knowledgeable attackers and natural disasters have shown the weaknesses of the systems, the need to increase security in CI and ICS systems is evident. The search for resources might be challenging, but not assuring the systems is simply not affordable.

The main need is for a clear strategy to define the objectives, the mission and the vision of the eventual Testing Coordination Capability in the European Union. These objectives have to be clear and sustainable over time, but with enough flexibility to adapt to future requirements. If this task is clear, not only will the ICS environment increase their security level, but efficiencies will be generated and the results will be beneficial for the whole ICS community and Europe as a whole.

Probably, the most important asset of the ICS Security Testing Coordination Capability would be the trust of all involved stakeholders. To be kept independent from particular interests, reliable, with high quality action enabling results while remaining cautious in information sharing activities, is the single most important key factor for success.

All public and private entities involved are strongly advised to participate in the eventual initiatives that could arise from this study. But ENISA, in accordance with the new set of duties that it has received, is directly called up to take the initiative, assume responsibilities and contribute in the following steps in order to enable an harmonised, efficient and tailored for the European Union needs ICS Security Testing Coordination Capability.

6 References

[1] National Institute of Standards and Technology (NIST), "NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security," 2011.

[2] Commission of the European Communities, "COM(2004) 702: Critical Infrastructure Protection in the fight against terrorism," 2004.

[3] PANLAB Consortium, "PII - Deliverable 3.2: Test bed Service Description Specification," 2009.

[4] European Network and Information Security Agency (ENISA), "Protecting Industrial Control Systems. Recommendations for Europe and Member States," 2011.

[5] European Network of Secure Test Centres for Reliable ICT-controlled Critical Energy Infrastructures (ESTEC) , "Final Report," 2009.

[6] T. Yardley, R. Berthier, D. Nicol and W. H. Sanders, "Smart Grid Protocol Testing Through Cyber-Physical Test beds".

[7] United States General Accounting Office (GAO), "GAO-04-628T: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," 2004.

[8] Energetics Incorporated, "Roadmap to Secure Control Systems in the Energy Sector," 2006.

[9] Commission of the European Communities, "COM(2004) 698: Prevention, preparedness and response to terrorist attacks," 2004.

[10] Commission of the European Communities, "COM(2006) 786: on a European Programme for Critical Infrastructure Protection," 2006.

[11] Commission of the European Communities, "COM(2006) 787: on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection," 2006.

[12] Commission of the European Communities, "COM(2006) 251: A strategy for a Secure Information Society – Dialogue, partnership and empowerment," 2006.

[13] Commission of the European Communities, "COM(2005) 576: Green Paper on the EPCIP," 2005.

[14] Commission of the European Communities, "COM(2008) 676: on a Critical Infrastructure Warning Information Network (CIWIN)," 2008.

[15] Council of the European Union, "Council Directive 2008/114: on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," 2008.

[16] European Commision, "COM(2011) 202: Smart Grids: from innovation to deployment," 2011.

[17] European Parliament; Council, "DIRECTIVE 95/46/EC: On the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995.

[18] European Commission, "M/501: Mandate to the European standardisation organisations for standardisation in the field of equipment used in the offshore oil and gas industry," 2012.

[19] European Commission, “M/487: Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards,” 2011.

[20] European Commission, “JOIN(2013) 1: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” 2013.

[21] President of the United States of America, “EO 13228: Establishing the Office of Homeland Security and the Homeland Security Council,” 2001.

[22] President of the United States of America, “EO13231: Critical Infrastructure Protection in the Information Age,” 2001.

[23] United States General Accounting Office (GAO), “GAO-04-354: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,” 2004.

[24] United States General Accounting Office (GAO), “GAO-07-1036: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,” 2007.

[25] President of the United States of America, “EO13636: Improving Critical Infrastructure Cybersecurity,” 2013.

[26] Swedish Civil Contingencies Agency (MSB), “Guide to Increased Security in Industrial Control Systems”.

[27] Viking Project, “Viking Project,” 2011. [Online]. Available: http://www.vikingproject.eu. [Accessed 2013].

[28] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 1: IT-security for industrial automation - General model,” 2011.

[29] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 2.1:IT-security for industrial automation - Example of use of the general model for device manufacturer in factory automation - Programmable logic controller (PLC),” 2013.

[30] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 2.2: IT-security for industrial automation - Example of use of the general model in factory automation for plant and machinery installers - Forming press,” 2013.

[31] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 3.1: IT-security for industrial automation - Example of use of the general model for manufacturers in factory automation - Process control system of a LDPE plant,” 2011.

[32] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 3.2: IT-security for industrial automation - Example of use of the general model for integrators in process industry - LDPE reactor,” 2013.

[33] Technical Division Industrial Information Technology, “VDI/VDE 2182 Part 3.3: IT-security for industrial automation - Example of use of the general model for plant managers in process industry - LDPE plant,” 2013.

[34] National SCADA Test Bed (NSTB), “Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program,” 2008.

[35] Industrial Control Systems Joint Working Group (ICSJWG), “Common Industrial Control System

Vulnerability Disclosure Framework," 2012.

[36] National Security Agencia (NSA), "A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)," 2010.

[37] Joint Research Centre (JRC), "ERNCIP - European Reference Network for Critical Infrastructure Protection," [Online]. Available: http://ipsc.jrc.ec.europa.eu/index.php/ERNCIP/688/0/. [Accessed 2013].

[38] SfP 983805 SCADA Test bed Simulator Consortium, "Emergent Phenomena Test bed Simulator for Improving SCADA Performance in Power System Security Management," 2013.

[39] European Network for Cyber Security (ENCS), "The European Network for Cyber Security," [Online]. Available: https://www.encs.eu/. [Accessed 2013].

[40] Idaho National Laboratory (INL), "Idaho National Laboratory," [Online]. Available: https://inlportal.inl.gov/portal/server.pt/community/home. [Accessed 2013].

[41] Sandia National Laboratories (SNL), "Sandia National Laboratories," [Online]. Available: http://www.sandia.gov/. [Accessed 2013].

[42] Energy.gov, "National SCADA Test Bed," [Online]. Available: http://energy.gov/oe/national-scada-test-bed. [Accessed 2013].

[43] Idaho National Laboratory (INL), "National Supervisory Control and Data Acquisition Test Bed," [Online]. Available: http://www.inl.gov/research/national-supervisory-control-and-data-acquisition-test-bed/. [Accessed 2013].

[44] Public Safety Canada, "Canadian Cyber Incident Response Centre SCADA Test bed," 2013. [Online]. Available: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx.

[45] Control System Security Center (CSSC), "Control System Security Center," [Online]. Available: http://www.css-center.or.jp/en/index.html. [Accessed 2013].

[46] Energy.gov, "Office of Electricity Delivery and Energy Reliability," [Online]. Available: http://energy.gov/oe/office-electricity-delivery-and-energy-reliability. [Accessed 2013].

[47] Sandia National Laboratories (SNL), "National Supervisory Control and Data Acquisition (SCADA)," 2012. [Online]. Available: http://energy.sandia.gov/?page_id=859. [Accessed 2013].

[48] ISA99, "ISA99 Committee," [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/Home.aspx. [Accessed 2013].

[49] European Commission, "European Programme for Critical Infrastructure Protection," 2010. [Online]. Available: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm. [Accessed 2013].

[50] The university of Arizona, "Autonomic Critical Infrastructure Protection (ACIP)," 2011. [Online]. Available: http://acl.ece.arizona.edu/projects/current/HSSS/. [Accessed 2013].

[51] ENISA, "Good Practice Guide: Network Security Information Exchanges", 2009. [Online] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

TP-02-13-769-EN-N

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
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