"Recommendations for Harmonized ICS Testing Capability in the EU" Workshop
01/10/2013 – 10:00 CET, Tallinn, ESTONIA

1 Registered Experts

Name	Job	Affiliation
Adrian Pauna	NIS Expert	ENISA
Andro Kull	Information Security Lecturer	University of Tallinn
Andreu Bravo	Chief Information Security Officer	Gas Natural
Anna Maria Praks	Research Associate	Institute for Security and Safety
Antonio Requejo	Security Consultant	Freelance
Bart de Wijs	Head of Cyber Security	ABB
Bernhards Blumbergs	Scientist	NATO CCD CoE
Carlos Monreal Ibañez	Project Manager - R&D Department	S21sec
Christian Braccini	researcher	CCDCOE
Christian Gorecki	Senior Researcher	AGT International
Damiano Bolzoni	PostDoc	University of Twente
Danel Apse	IT Manager	Estonian Defence Forces
David Willacy	Digital Risk Security Manager	National Grid
Emin CALISKAN	Scientist	CCDCOE
Engin DALGIC	Cyber Security	Ministry of Energy
Ghislain NGAMBA NYAMFIT	CONSULTANT IT	DOTCOM SARL
Guido Gluschke	Managing Director	Institute for Security and Safety
Heikki Kortti	Senior Security Specialist	Codenomicon
Henri Pirinen	Design Engineer	Fortum Power and Heat oy
Janno Kase	Chapter President	ISACA Estonia Chapter
Jens Wiesner	Referent	BSI
John Owens	Operations Manager	Energy Networks Association
Kaur Kullman		RIA
Konstantinos Moulinos	NIS Expert	ENISA
Konstantinos Rogalas	ICT Consultant	anapur AG
Luis Tarrafeta	Project Manager - R&D Department	S21sec
Lior Frenkel	CEO Co-Funder	Waterfall Solutions
Marco Caselli	PhD candidate	Universiteit Twente
Martin Hutle	Project manager	Fraunhofer Research Institution

		AISEC
Martin Uwdusk	Cyber Security Expert/CIIP	EISA
Meelis Roos	security engineer	Cybernetica
Miguel Herrero	Security Consultant	INTECO
Olev Sepp	unit manager	Est MOD
Ragnar Rattas	Cyber Security Expert	EISA
Raimo Peterson	Branch Chief	NATO CCDCOE
Raymond Hallie		ENCS
Riho Lodi	Head of IT Department	Elering AS
Robert Malmgren	Senior Security Expert	Robert Malmgren AB
SATOSHI TAKEMOTO	Engineer	Hitachi
Satu Simonen	Solution manager	Wartsila
Teet Raidma	Manager of IT Advisory	KPMG Baltics
Thomas Bleier	Program Manager ICT Security	AIT Austrian Institute of Technology GmbH
Tiago Vilas	Cyber Security Advisor	Modulo
Tomas Nystrom	Information Security Manager	Fortum Power and Heat Oy
Toomas Lepik	Infosec expert	EISA
Toomas Molder		Hegariit
Toomas Vaks	Director of Cyber Security	EISA
Toomas Viira	Head of CIIP Department	EISA

2 Topic and agenda of the workshop

Topic: *"Recommendations for Harmonized ICS Testing Capability in the EU" Workshop*

Agenda:

09:30-10:00	**Registration**
10:00 - 10:10	**Welcome, Workshop Objectives (ENISA)**
10:10 – 10:30	Ragnar Rattas –"The Estonian approach on ICS security assesments" *Overview of Estonian Information System's Authority experience in the area of ICS SCADA security assessments.* ***(EISA)***
10:30 – 10:50	Carlos Monreal : "Methodology used for the project" *Overview of the methodology used* ***(S21sec)***
10:50 – 11:10	**Coffee Break**
	Session: "Challenges of ICS SCADA testing"
11:10 – 11:30	Raymond Hallie – "ENCS - Challenges in the ICS SCADA Testing" *Overview of the Testing Experience ENCS has* ***(ENCS)***
11:30 – 11:40	Short introduction on the Challenges of ICS SCADA testing identified in the Report *Overview of the Challenges*
11:40 – 13:00	Discussion & comments on the Challenges presented in the report

	Discussion of Challenges, Collection of Feedback and Identification of Next Steps
13:00 – 14:00	**Lunch Break**
	Session: "Recommendations on ICS SCADA testing"
14:00 – 14:20	Jens Wiesner : "BSI recommendations for ICS testing" *Overview German ICS testing framework,* ***(BSI)***
14:20 - 14:40	Miguel Herrero: "The Spanish Recommendations for ICS testing framework" *Overview Spanish ICS testing framework,* ***(INTECO)***
14:40 – 15:00	Coffee Break
15:00 – 15:10	Short introduction on the Recommendations of ICS SCADA testing identified in the Report *Overview of the Recommendations*
15:10 – 16:30	Discussion& comments on the Recommendations presented in the report
16:30 – 16:45	Plenary Discussion, Next Steps, Closing Remarks

Registration

Between 9:30 and 10:00 workshop attendees arrived to the "Cuxhaven and Bremerhaven rooms" in Radisson Blu Hotel in Tallin.

All assistants were provided with their own ID badge. A printed copy of the final report draft was also provided with the aim to let the experts review it during discussion.

Welcome, Workshop Objectives

Adrian Pauna and Konstantinos Moulinos welcomed all the attendees and thanked to the Estonian Information System's Authority for the help given in the organisation of the event.

After that, Adrian Pauna explained the main objectives of the workshop and the agenda to the audience, and gave the floor to Mr Ragnar Rattas.

The Estonian approach on ICS security assessments

Ragnar Rattas started by presenting how Estonian ICS security entity deals with ICS security matters. For this purpose they have 3 departments: CIIP, CERT-EE and Supervision. The CIIP scope integrates 43 vital/critical services. Some of them include ICS/SCADA systems.

The ICS security assessments are performed, on a voluntary basis, sponsored by the state. A comprehensive assessment of IT systems is included. Within their task list, the assessment includes:

- Information gathering from public sources: what kind of tools is each company using
- Networks perimeters: how is possible to protect different types of networks
- Workstation & servers
- Remote access: facing Internet
- Physical security: how much time security company takes to come
- Disaster recovery plans, architecture, security policies, etc.

Ragnar Rattas ended his presentation summarizing key points:

- "Regular" IT is extensively used by ICS
- The "quick wins" can be achieved by improving security in IT systems.

Questions & Answers

An expert asked how many tests have been done by the Estonian ICS security entity. Ragnar Rattas answered that they have executed less than 10 tests. This is because they have been working in several

tasks at the same time. However, they obtained a big coverage because Estonia is a small country with only a few companies with ICS/SCADA systems for Critical Infrastructures.

Another expert asked about the approach this entity follows: separate tests or test of the complete system (in production).
Ragnar Rattas answered that it's very complicated to test a big number of inter connected systems in production. He thinks that it's not possible to have a full testing done.

An expert asked about what is the usual outcome they produce.
The speaker answered that they usually generate two documents:

- Technical report
- Management report, the most important one that includes key findings for the management of the company. This is not a mandatory report but it is considered valuable.

Another expert asked about how difficult has been to work within a trust based model.
Ragnar Rattas explained that they have managed to create trust between operators, vendors and themselves. This was easier for them because of the advantage that Estonia is a small country.

Finally, an expert asked about who bares the liability for implementing the recommendations. Ragnar Rattas said that service providers (utilities) are responsible to provide the adequate services.

Methodology used for the project

Carlos Monreal and Luis Tarrafeta described to the audience the methodology that S21sec and ENISA used for the project in order to obtain the report that is going to be discussed during the workshop.

They exposed that the project has been split into two phases, namely: the stock taking and the analysis.

Regarding the stock taking, project team has been collecting information from three sources

- Desktop research, obtaining information related with test bed capabilities from published/high reputation resources. They have analyzed more than 100 documents for this project.
- Questionnaire, containing 26 open and closed questions that are divided into 6 categories and finally deployed as an on-line Web form
- Interviews, performed directly to 27 experts with the double purpose of going deeper into some of the answers of the questionnaire and to ease the exchange of points of view in several hot topics in the field of ICS SCADA Testing Capabilities

Regarding the analysis and good practices, five main tasks has been executed so as to:

- normalize the unstructured data coming from the previous phase
- analyze the information in order to perform a qualitative analysis that obtains a structured set of information including graphs, tables and statistics
- obtain a set of 36 key findings (basic element of knowledge)
- extract 7 recommendations derived from the key findings, including also a set of 12 quick wins
- improve the report with the suggestions coming from the experts in current workshop

Adrian Pauna highlighted that during the workshop we will have the opportunity to discuss about all this information.

ENCS - Challenges in the ICS SCADA Testing

Raymond Hallie presented relevant information regarding the ENCS test facility, which is one of their main service lines. He explained where they are today and which are next steps and the main challenges to be faced.

ENCS testing facility's objectives are twofold:

- Research and Development (R&D). Today ENCS offers its R&D facility so that internal and external researchers are currently working in the R&D lab. and,
- Security validation test-bed for ICS, Smart grids systems and components. This is still under development. Regarding the methodologies, processes, toolset, equipment, trainings, they are still working on it.

In relation with ENCS testing facility, key points are:

- Semi open environment. Resources shared with stakeholders like universities, R&D centres, etc.
- The environment provides remote access, that means that Universities can connect with their environment in order to run their tests
- They also organise the R&D agenda where physical tests are required
- Finally they run their own projects in this test facility

Regarding the security validation test-bed for ICS, Smart grids systems and components activities:

- Providing security test services
- They are focused on critical infrastructures
- Offering integral approach, combining systems and components in order to work together for a complete testing environment
- Developing methodologies that really obtain results

Regarding the next steps, ENCS is going to finalize their validation test-bed. They also want to perform further development processes and working procedures. Finally it is planned to develop an ENCS toolbox.

ENCS exposed the main challenges they have found:

- Complexity of the methodologies for test-bed deployment.
- Required high flexibility for different technical setups. There are totally different configurations depending on the concrete case, so it is important to be versatile.
- Minimising the gap between test-bed environment and real production systems.
- Validation of cyber tools and tests processes.
- Strong market need for accreditation.
- It is still to be improved how to fit the required creativity and innovation into a testing methodology. By now, they always provide a percentage of hours to be used "freely" by the experts that conduct testing. Learned lessons are, if possible, included into the testing methodology.

Questions & Answers

An expert asked if the configuration of the setup for the testing environment can be done automatically. Raymond Hallie answered that they are working on this topic and they are able to automate with virtualization, emulation and simulation approaches. He also states that there is a point in which they are investigating.

Other expert asked about how many people can be trained. The answer was 30 – 50 people.

Another expert asked about how do ENCS chooses their replica environments.

The speaker answered that they are doing assessments will the help of DSOs and they adapt the real situation to what they have. But this is one of the scenarios. There is one case that is more mature, Alliander, where they try to check it from running situation to future situation. Other option should be to increase the automation of their environment.

In the end an expert asked if there are any vendors that use ENCS's facilities for testing.
Raymond Hallie said that for the moment they are not working with vendors, the drivers are the users, the asset owners. He believes that they are the ones that can push the rest to get involved.

Short introduction on the Challenges of ICS SCADA testing identified in the Report

A short introduction on the Status, Gaps and Challenges of ICS SCADA testing identified in the Report was exposed by Adrian Pauna with the support of Konstantinos Moulinos and Luis Tarrafeta.

Adrian explained that Key findings were structured in the report in 6 groups. All key findings included in each group were described and an open debate raised during the exposition.
Due to the high and interesting debate, this session had to be split into two, talking about last three groups after lunch, just before recommendations' session. For a better understanding, the full content of both sessions has been merged in one.

Categories of key findings, including debate:

Category: Current status of ICS Testing

- Not harmonized situation for ICS Testing
- No real "ICS Security educational environment" in the EU
- Low Maturity Level of ICS Security Testing methodologies and initiatives in Europe
- Interest in a Certification Framework

Debate:
Konstantinos Moulinos asked if a harmonized approach in Europe in testing is needed.
An expert responded that probably we don't need testing because performing a test gives as result only a score and this is not good in order to improve security. He asserts that it could be less provocative as entities tend to have good numbers (scores) in tests, because of marketing reasons. He also thinks that it's better to define the environment instead of the product. Finally, he said that it's more important to use the components correctly in each infrastructure.
This is because a product secure by design can be affected by misconfigurations and this way become vulnerable.
Other experts agreed and said that, for example, people are still using simple passwords by default. This not the result of the lack of awareness regarding the risk they expose but due to the way they accept this risk.
Another expert asserted that safety is often part of the design but security is usually not, except nuclear and a few more areas. The conclusion was that probably we will not able to harmonize.
Konstantinos Moulinos said that ENISA conclusion is that, in order to mitigate the immature status of testing capabilities, the best way to run a market is to plan objectives and leave room for the stakeholders to use creativity and innovation.

An expert asked about whom should be involved in the certifications schemes: operators or vendors. This question started a big debate regarding what to certificate: components, processes, full systems, organizations. In the end there was not a final agreement of where to focus tests. This was, in fact, one of the Key Findings of the study.

Most of the experts agreed in that doing something regarding this matter is always better than doing nothing.

Category: Objectives for a European ICS Testing Capability

- Several drivers show the need of a European Testing Capability, being independent is the main one
- Political Will has been necessary in similar experiences abroad
- Get aligned with already existent standards is preferred to develop new ones
- Offer value to all stakeholders considered key for success
- A systemic or holistic approach is recommended but is more difficult to standardize
- Means to enforce vulnerability resolutions to be considered

Debate:

Some experts discussed regarding the adequacy of making testing mandatory.

One expert said that mandatory testing should depend on the criticality of the system. Other expert said that it's difficult to put the line between what's critical and what's not.

Another one said that this is a complex equation because which include changing the entire ICS infrastructure. This at the moment it is seen to be too expensive and not achievable by one entity.

Regarding the information exchange and vulnerability disclosure, there was also an intense debate:

- One expert exposed that publishing the vulnerabilities will not contribute to the resolution and it can expose many infrastructures to be attacked.
- Other experts answered that NDA is to manage disclosure, not to keep it closed. The question that arose was: Which is the objective of testing to prove or to improve the systems? Those are conflicting goals.
- Other opinion was that the publication should be not transparent but only to the vendor and affected operators. A vendor exposed that they work with thousands of vulnerabilities but they did not disclose them.
- Another expert said that for an attacker it is very easy to discover a vulnerability of a SCADA system. So it is not very important if that vulnerability is publicly disclosed or not.

Category: Consideration about the model and methodologies

- Need for both Testing facilities and a Certification Framework
- Debate concerning if Certification and Compliance are adequate for improving security
- Unclear which should be the subject of certification
- Stakeholder roles for definition and operation will require common agreement and public leadership
- "Acceptance of the results" and "Comprehensiveness of tests" are the best measure of success
- EU complexity makes desirable a "Distributed Model" with an Accreditation Organism on top
- Segmentation by business is the most recommended

Debate:

Some of the experts agreed completely with the last key finding in this category: segmentation by business

There was a discussion regarding the certification and compliance key finding.

Some experts expressed their disagreement about having certification. Luis Tarrafeta clarified that an accreditation entity for the whole Europe could help all vendors, no matter the size, to improve their testing capabilities.

Other experts proposed that it could be helpful to publish information and let vendors improve internally so they can help themselves.

Konstantinos Moulinos said that in house testing could not be similar to certification.

Category: Overview of Available Resources

- Public Private Partnership as the most accepted Financing Model
- Strong Initial Public Investment has been needed in similar initiatives abroad
- Multiple Reasons for Success identified in existing initiatives abroad
- Not advisable to publish product comparative charts
- Work in multidisciplinary teams needed
- Engage expertise from the industry recommended

Category: Major Constraints, Risks, Threats and Limitations

- Achieve trust is the most challenging Organization Issue
- Strategies identified to grant trust are related with Test bed Independency
- Diversity is the biggest technical challenge
- Difficult agreement for testing methodologies is foreseen
- Complexity of the Legal environment among biggest challenges
- Need for an accurate Economic Model for Public Private Partnership

Category: Relationships with other Stakeholders

- Representative Composition of the Executive Board
- Fluent communications with CERTs recommended
- Debate regarding Vulnerability Disclosures Handling
- Vulnerability Resolution Enforcement recommended by Security Test Lab Experts
- Involve stakeholders in dissemination activities
- Testing Environment useful for Educational purposes

Debate

Konstantinos Moulinos confirms that not many asset owners are present at the workshop.
An operator that is present in the workshop asserted that he had the same concern. He thinks that the main problem is to share information between operators. Only energy and telecommunications sectors have started working in these activities.
Konstantinos Moulinos said that the dissemination of the report has been done to 150 people and the recommendations incorporate information coming from this group. So revision comments are also expected from them.

BSI recommendations for ICS testing

Jens Wiesner explained an overview of the German ICS testing framework and presented a set of recommendations of BSI for the ICS testing capability.

He started exposing the needs and necessities. Their first objective was to “end the uncertainty”, so they thought that the best way to start was covering a high demand for certification or, in a wider perspective, security validation.
BSI efforts are focused on awareness, publications, and spot tests of devices and to foster a public-private partnership.

He also exposed some tasks BSI has performed and recommendations they can give the community regarding the requirements to a test-bed:

- Awareness

    - Campaigns
    - Media
    - Fairs
    - Life-demos
    - Different approaches in each country
    - **Recommendation: "European test-bed is not suitable"**
- Education
    - National efforts: commercial providers, ICS-Skill training (hacking, red/blue-team training...)
    - Necessary approved skill-certificate
    - **Recommendation: "Centralized facility not needed"**
- Research/knowledge coordination
    - Many local uncoordinated efforts
    - Necessary to coordinate throughout Europe
    - Distribution of classified knowledge. They have knowledge but distribute and share it across Europe is not easy. There is a lack here.
    - **Recommendation: "Establish a platform for coordination purposes"**. It does not need to be a physical institution. It should be a set of workshops, meetings, etc.
- ICS testing
    - Complex scenario
    - Unique scenarios
    - **Recommendation: "Not feasible for large scale systems in a test-bed"**
- Device testing
    - Penetration testing and so on
    - Firmware analysis
    - More sophisticated attacks such as hardware based
    - **Recommendation: "Recommend a public guide for test beds and vendors to test and certify single devices to a given standard at a single time"** to certificate it's not to be completely secure but at least is an incentive.
- Arguments against an EU-wide test-bed
    - Security is not only achieved by secure component
    - "Compliance is not security!"
    - Acceptance of a EU certification on international market
    - Unique features in comparison to NERC CIP and others

As a summary of the exposition, Jens Wiesner said that, from BSI's point of view, the need is to make ICS more secure and to help users, asset owners and vendors. So the necessity is to build common basis for distribution of knowledge, certifications and procedures.

The Spanish Recommendations for ICS testing framework

Miguel Herrero explained how INTECO, the Spanish cybesecurity centre at the national level. INTECO provides services and they are the CERT of ICS.

He specifically talked about the SCADALAB project in which they are working in two different areas: laboratory and test beds. The procedure and workflow related with the test-bed area was explained. More information about the project will be published in their Web site at http://scadalab.eu

Finally Miguel Herrero kindly invited the audience to a SCADALAB's workshop that will be held in Madrid on next week.

Short introduction on the Recommendations of ICS SCADA testing identified in the Report

Adrian Pauna explained one by one all the recommendations identified in the report. Konstantinos Moulinos and Luis Tarrafeta helped clarifying some aspects related with recommendations. All experts were involved into a rich and constructive debate regarding the exposed recommendations.

Adrian Pauna started by presenting an overview of the complete system, including the main actors, tasks and relations between them. He focused on the supervisor entity and on how the rest of entities will be linked with it and the main stakeholders that should be created in order to execute different tasks.
An expert said that it seems that ENISA is proposing to start everything in parallel. Adrian Pauna and Konstantinos Moulinos clarified that it would be better to be sequential, going step by step creating different boards and achieving different tasks. There was an agreement on that.

Recommendation 1: "The creation of a Testing Capability under Public European ownership and leadership"

Adrian Pauna exposed that an entity called Supervisor, should foster Public Support for the initiative and should involve other public and private organizations to cooperate in the early stages of the initiative.
Adrian clarified that this proposal is not related with the creation of a big entity that does everything. This recommendation is talking about coordination between different activities.
A quick win for this recommendation is: the Supervisor for the Testing Capability would become a contact point for relevant Stakeholders and for any interested entity.

An expert said that the real problem is not which type of entity the Testing capability should be. Konstantinos Moulinos answered that, for the moment, it is still not clear, so it will be necessary to go more in depth with the discussions, in the future.
There was an agreement in replacing "Testing capabilities" by "Testing **coordination** capabilities" in this recommendation.
An expert asserts that it's more important to have coordination in order to decide what to be tested. So it is less relevant the decision regarding where to test, which consultants to use, which vendors, etc.
All experts agreed on that this entity should be public at least at the beginning.

Recommendation 2: "The establishment of a trusted and functional Executive Board"

Adrian Pauna exposed that stakeholders, by their representatives and always under the lead of the Supervisor, would create a Working Group that would become the Executive Board. This will be able to define the strategy and the steps in the definition of the Testing Capability.
Some quick wins for this recommendation are: the Supervisor would state clear participation rules for the Testing Capability, Stakeholder representatives would be engaged for the Executive Board working group and the Executive Board will define a common strategy for the Testing Capability

Konstantinos Moulinos said that there is a real need for a working group and that this initiative should be guided by some people from both public and private stakeholders. He also said that this recommendation should be rephrased as "create and executive board".

One expert said that it is good to have different stakeholders represented in this kind of initiative. From his perspective, the key point is the semi-lack of people with competence. So the big question is what the target is and how to reach it.
Konstantinos Moulinos answered that there are good practices regarding this issue, so the best approach should be first to create an ecosystem and then to go for the consortium.

Some experts said that it's difficult to join a balanced consortium because, some sectors have different needs and are avoiding initiatives like the exposed in this recommendations, so it could became a Babel tower. Maybe not all the people there should have the same weight or segmentation in the coordination. Another proposed way, would be to define some rules of participation or terms of references.

Finally, an expert said that, as we are changing the focus from testing to coordination, maybe the audiences should be different, but the necessities are the same.

Recommendation 3: "On the creation or involvement of working group for specific activities"
Adrian Pauna exposed that in this recommendation the Executive Board would engage already existing experts in order to create thematic Working Groups for technical, financial, legal, research, educational or communications issues.
Some quick wins for this recommendation are: Current initiatives in ICS Security Testing will be officially contacted in order to establish more specific cooperation; Working Groups would define the testing methodologies and criteria that will be aligned with the strategy.

Konstantinos Moulinos said that, for the moment we have at least two initiatives (the one from BSI and ERNCIP project) that could be used for the creation of these working groups.

An expert asked if there is some kind of exclusion between different groups. Konstantinos answered that there is not.

Other expert said that if we are talking about a coordination body, and in the case that the Executive Board would need more knowledge, the best approach should be to create advisory boards.

Recommendation 4: "The definition of a Financial Model realistic with the European situation"
Adrian Pauna exposed that 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.
A quick win for this recommendation is: Involved working groups will identify potential sources of funding and develop a business plan.

Konstantinos clarified that there are three options. The first one is to have a model totally covered by a public entity, such as BSI, other option is to have a private model and the third one is to create something mixed between public and private.
One expert said that public entities are pretty much known, but the private ones are segmented. The problem is that today is very difficult to engage all private sectors to participate. Luis Tarrafeta clarified that the main idea is to create something in which vendors also win. This way it will be more attractive for them to finance the idea.

Recommendation 5: "Making a study of feasibility for a Distributed Model"
Adrian Pauna exposed that within the responsibilities of the Technical Board, supported by the Executive Board; it would be the study of feasibility of a distributed model of operation. Testing methodologies, standards, and a clear accreditation model designed to engage current test beds and certification institutions would have to be developed.
A quick win for this recommendation is: ICS Security Testing accreditation criteria should be defined.

One expert asserts that as we are talking about a coordination body, it should be assumed that the model will be distributed.
Luis Tarrafeta added that there are several things to be studied related with the distributed model (centres of excellence, expertise in security postures or legal requirements, etc.) so it should be studied how to articulate them.

Konstantinos Moulinos said that different applicable laws in each country can bring problems, so it should be also studied.

Recommendation 6: "Establish collaboration agreements with other organisations dealing with ICS security"
Adrian Pauna exposed that entities such as CERTs, international ICS Security Testing initiatives and, in general, any relevant stakeholder must have the possibility of clear communication with the Testing Capability. He also said that the communications group would have to design these protocols and operate them.
Some quick wins for this recommendation are: Non-Disclosure Agreements and other legal requirements will be elaborated; Current CERTs would be contacted for specific cooperation, including Vulnerability Disclosures and incident response.

One expert asked whom in Europe will have the responsibility for CERT. Konstantinos Moulinos answered that, for the moment, as far as there is no a Euro-ICS-CERT, existing CERTs would have to deal with it.
The expert said that he thinks that there should be some local entities to cooperate in incidents, and Vulnerability Disclosure dissemination. He also said that the amount of information to be disclosed is the responsibility of the owner so they need help for publication. This will mean also that they will follow their processes. Konstantinos Moulinos answered that ENISA is currently working on this so next year there will be some results.
Another expert said that the presented diagram in the report should be improved by drawing the vulnerability disclosure task after CERTs, if they are going to be the ones to perform it. It was agreed to do so.

Recommendation 7: "Establish a knowledge management programme"
Adrian Pauna exposed that knowledge and expertise in ICS security testing is still scarce and has to be fostered by involving professionals from the industry, research and education.
He also said that this can be addressed altogether under an umbrella of Knowledge Management programs.
Some quick wins for this recommendation are: Experts from the industry would be engaged; A base of knowledge with testing cases should be created.

Konstantinos Moulinos clarified that last quick win is in order to avoid reinventing the wheel. Some expert asked if this recommendation is talking also about doing it coordinately. Konstantinos Moulinos answered yes.
Finally some experts asserted that going step by step would be quite better than trying to achieve all at the same time.

Plenary Discussion, Next Steps, Closing Remarks

Experts said that having firstly a knowledge management programme it would be useful in the idea of creating a testing body.

Other expert requested to include vendors in the working groups, as they are excluded of EuroSCSIE. There was a debate about how to motivate them. Some ideas were to promote meetings, workshops, etc. in a more pro-active manner.

One expert suggested to be more precise and to include other things complementary to the Testing area. He also mentioned that the awareness level regarding the necessity of improved security should be increased. We should avoid having people that consider that SCADA systems cannot be affected. Other expert said that all these things are very interesting and it is needed more cooperation. Another action should be to disseminate this to the industry. Konstantinos Moulinos said that it would be necessary to make them alert, to engage the Asset Owners as they can really motivate the other stakeholders.

Konstantinos Moulinos suggested, as an idea, the creation of a "Top ten" list of threats. One expert said that BSI published a TOP 10 ICS SCADA Threats [1] report in English last. Adrian Pauna asserts that ENISA can try to do this.

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_010E.html