enisa
European Network and Information Security Agency

Protecting Industrial Control Systems

Annex VI. Minutes of the Workshop

[Deliverable – 2011-12-09]

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on CIIP & Resilience, please use the following details:

- E-mail: resilience@enis.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to industrial control systems' security, please use the following details:

- E-mail: Evangelos.Ouzounis@enisa.europa.eu

Contents

1 Minutes of the Workshop

On the 16th September, 2011, ENISA organised a workshop where the results of the Study on ICS security were presented. The aim of this workshop was to share and discuss the most relevant conclusions of the report, including the proposed recommendations, with the experts that participated in the Study. For this reason, an open dialog among the attendees was also planned. This dialog allowed ENISA to pulse the impression of the audience on the recommendations and to gather the different opinions on how to improve them.

All those experts who participated in the study were invited to the workshop, and most of thirty finally attended the event. They were representatives of all the stakeholders types considered for the study: ICS manufacturers, security tools and services providers, ICS operators, Academia & Research, public bodies, and standardisation bodies.

The agenda of the Workshop was the following:

Time	Title	Speaker/Affiliation
09h00-09h30	Registration	N/A
09h30-09h50	Welcome, ENISA's Resilience and CIIP Program	Prof. Manel Medina (ENISA)
09h50-10h20	EU Policy Context	Alejandro Pinto-González (European Commission DG INFSO)
10h20-10h40	Cyber threats to Industrial Control Systems	Zoltan Precsenyi (Symantec)
10h40-11h00	Public Private Partnerships in The Netherlands and Europe	Auke Huistra (CPNI.NL)
11h00-11h30	Coffee break	
11h30-11h50	ENISA-ICS Security Workshop-ABB's view	Bart de Wijs (ABB)
11h50-12h10	ENISA Recommendations on ICS Security	Rafal Leszczyna (ENISA)
12h10-12h30	About the ENISA ICS Security Study	Elyoenai Egozcue (S21sec)
12h30-13h00	Open discussion	All participants, moderated by ENISA
13h00-14h00	Lunch	
14h00-15h30	Topic discussion on the recommendations and the key findings of the study	All participants, moderated by ENISA

15h30-16h00	Coffee break	
16h00-16h45	Panel Discussion	All Speakers, moderated by ENISA
16h45-17h00	Wrap-up	ENISA

The following subsections represent the minutes of the Workshop. The reader will be able to easily get a detailed outlook on what took place during the discussion sessions as well as on the different topics that were introduced by the presenters. In order to facilitate the reading of these subsections the following abbreviations are used:

- Prof. Manel Medina (**MM**)
- Alejandro Pinto-González (**AP**)
- Zoltan Precsenyi (**ZP**)
- Auke Huistra (**AH**)
- Bart de Wijs (**BW**)
- Rafal Leszczyna (**RL**)
- Elyoenai Egozcue (**EE**)

1.1 Registration

All assistants were provided with their own ID badge and a printed copy of the final agenda of the Workshop. Most of them also received an electronic copy of the final report core chapters, and were invited to ask for the annexes if they were interested. Only those attendees that registered in the last minute did not have a copy of the report. They were identified and RL promised to send them the electronic copy after the Workshop.

1.2 Welcome, ENISA's Resilience and CIIP Program

After a warm welcome from RL, MM opened up the session presenting the work done by the Commission in the area of the Resilience and CIIP Program, whose objective is to collectively evaluate and improve the resilience of European communication networks and services. MM mentioned previous ENISA's studies, which culminated in 2010 in a Commission Communication on CIIP and a Telecommunication Package to mitigate existing gaps in the field, and define good practices and guidelines. The Communication provided through a CIIP Action Plan several initiatives such as Pan European Public Private Partnerships for Resilience (EP3R), Pan European Forum for Member States (EFMS), baseline capabilities for Gov CERTs,

etc. As MM also mentioned, in 2011 there were issued the new Communication from the Commission on CIIP and the Commission's mandate that reinforced the ENISA position as the security European agency of reference.

After this, MM made a review on the most important aspects related to cyber security of ICS, highlighting the existing challenges. Afterwards, he explained ENISA's approach to address cyber security issues affecting ICS, which basically consists in the identification of security problems, good practices initiatives and challenges, and the development of insights and recommendations for further action in different aspects.

MM also introduced the audience to the Smart Grid challenges, since this topic is intrinsically related to ICS security, and ended his presentation by showing ENISA's approach towards Smart Grid security.

1.3 EU Policy Context

Alejandro Pinto (AP) explained the EU policy context in relation to Network and Information Security (NIS) and CIIP. AP started providing an overview on the EU reference policy framework, highlighting its evolution since 2004. He described the overall aim of the Digital Agenda as to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast Internet and interoperable secure applications.

After a short briefing on the current situation of NIS in Europe and its Member States he presented, in relation to this topic, the list of challenges and initiatives of the EU Commission to address them. These initiatives include: The Digital Agenda, The establishment of the EU-U.S. Working Group on cyber-security and Cybercrime, the adoption of EU internal security strategy, and the CIIP COM(2011)163 on the "Achievements and next steps: towards global cyber-security.

AP then explained each one of these initiatives in detail. Specifically on the Digital Agenda, he mentioned that it includes among its seven priority areas one on "boosting Internet trust and security", which is further divided into three main areas of action: cyber-security preparedness, cybercrime, and safety and privacy of online content and services. He then went through Key Actions (KA) 6 and 7. KA 6 (Action 28) presents measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernised European Network and Information Security Agency (ENISA), and measures allowing faster reactions in the event of cyber attacks, including a CERT for the EU institutions. For achieving these measures it counts with a "tool box" which includes ENISA, EFMS, EP3R, EPCIP, Observer in Cyberstorm, and CIIP conference. On the other hand, KA 7 (Action 29) presents measures, including legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace at European and international levels by 2013.

Regarding the EU-US Working Group (EU-US WG) on Cyber-security and Cybercrime, AP highlighted that this group was established in the context of the EU-US summit of 20 November 2010 held in Lisbon to "tackle new threats to the global networks upon which the

security and prosperity of our free societies increasingly depend". The EU-US WG will address a number of specific priority areas, including securing industrial control systems and smart grids, and will report progress within a year.

After this, AP made a review on the CIP European context, highlighting the most relevant facts, which include:

- The request in June 2004 of the European Council for an overall strategy to protect critical infrastructures.
- The adoption by the Commission in December 2006 of the Communication on a European Programme on Critical Infrastructure Protection EPCIP (COM(2006)786) with the objective of improving the protection of critical infrastructures in the EU.

Regarding COM(2011)163 on the "Achievements and next steps: towards global cyber-security", AP mentioned that this Communication aimed at taking stock of the results achieved since 2009. It is built on existing policy initiatives, and in particular on the Digital Agenda, the Stockholm Action Plan and the ISS, and it describes the next steps at European and International level. AP made a review on the results achieved and which are presented in this Communication, highlighting the European Forum for Member States (EFMS), the European Public-Private Partnerships for Resilience (EP3R), and the Baseline of capabilities and services for pan-European cooperation.

AP ended the presentation introducing the audience the Expert Group (EG) on the Resilience and Security of Communication Networks and Information Systems for the Smart Grid. Firstly, he stated the cyber security problem of the Smart Grid, highlighting that the ICT infrastructures, as underpinning platform have become critical for the Energy sector, without which some services could come to an abrupt halt. The EC and ENISA convened the EG to:

- Better understand of the views and objectives of the private and public sectors on the ICT security and resilience challenges for the smart grids.
- Identification and discussion about the related policy at EU level.

Finally, AP also explained that currently the EG is divided into two Sub-Working Groups, the first one focusing on the high level analysis of risks and security requirements, while the other focusing on challenges and recommendations. Moreover, a small group of Experts is working on the Work Program for the Expert Group which will take into account, among others, the activities of the two Sub-Working Groups.

1.4 Public Private Partnerships in The Netherlands and Europe

AH gave a presentation on the Public-Private Partnerships (PPP) in the Netherlands and Europe. He started by introducing the fact that ICT is of fundamental importance. For this same reason our society becomes more and more vulnerable for the disruption or misuse of

the ICT infrastructure, as have been shown by the recent incidents of Stuxnet, Night Dragon, RSA, and DDoS-attacks. At the same time most CI which heavily depend on ICT are owned by the private sector. Therefore the private sector has its own responsibility in CIP. However, not enough information between the public and private organisations is exchanged. Moreover, this is an international problem since many CIs can affect more than one country. For this reason, AH considers that in order to raise the resilience of CIs against cyber terrorism it is necessary to:

- Build and facilitate a (inter)national Public Private network based on trust and value
- Create the Cybercrime Information Exchange with sectoral Information Sharing and Analysis Centres (ISACs)
- Use clear membership guidelines, including Traffic Light Protocol (TLP) to encourage greater sharing of sensitive information
- Sector is in the lead (chair of the ISAC is from industry)

AH starts presenting the Cybercrime Information Exchange (IE). This Dutch national initiative is based on the basic principle that companies themselves will only take effective measures if they have access to the right information and are able to make accurate risk assessments. By sharing information intensively about incidents, threats, vulnerabilities and good practices, the participants can prevent incidents themselves. This will safeguard the Dutch economy as a whole and the continuity of the individual organisations at the same time. To this regard, AH stresses the idea of information sharing based on value and trust, and remarks that first the "social network" has to be built (meetings face-to-face) and then a technical infrastructure should be provided to support it.

At an International and European level, AH provides a list of Information Sharing initiatives that are promoted by the CPNI.NL, including E-SCSIE and European FI-ISAC at the European level and Meridian (annual CIIP conference) and MPCSIE at the international level.

AH then presented with a high level of detail E-SCSIE, its members and its terms of reference, highlighting that its aim is for European industry, government, and research to benefit from the ability to collaborate on a range of common issues, and to focus effort and share resource where appropriate. He also mentioned that E-SCASIE main focus is Information Sharing and its outcome would be a raised level of protection adopted across Europe's SCADA and Control Systems (SCADA/CS)

The second part of AH's presentation was on the Dutch National Roadmap to Secure Control Systems. The first phase starts in 2010 and ends in 2014. It includes seven work packages targeting: awareness and knowledge dissemination, building the network, training &

education, knowledge development, red teaming framework, international network, and a plan for a second phase.

The third and last part of AH's presentation was on Cyber-TEC, a non-for-profit European Public Private Partnership on cyber security for critical infrastructures. This initiative currently focuses on smart grids and process control, but will be extended to include other critical infrastructures. Cyber-TEC wants to take a leading role in Europe on cyber security of Critical (Information) Infrastructures by bundling knowledge and know how through one organization. AH declares that currently they are preparing the business plan for this initiative, which final version will be available in December 2011. A draft version of the plan is presented during the Workshop (for more info, please refer to AH presentation). It will consider a time-span of 5 years, starting in 2012 and looking for a private/public division in revenues of 60%-40% in 2012 and 80%-20% in 2016.

AH ends his presentation by listing the next steps on Cyber-TEC. He mentions that Cyber-TEC will be shared with the USA under the umbrella of the EU-US WG on Cybercrime and Cyber-security.

1.5 ENISA-ICS Security Workshop-ABB's view

BB starts by presenting a "cyber security in ICS demand map" which excluded the global players such as BP, ExxonMobil, Shell or Daimler. North America and Central and Northern Europe are the countries where operators more demanded cyber security, and where requirements where clearer. The most active sectors are electricity transportation and distribution, oil and gas, and power generation.

BB considers that there are different types of customers: those that know exactly what they want, those that know where they want to go, those that seek help, and those that don't care about cyber security.

BB then continued exposing ABB's point of view on compliance and certification. BB considers that compliance or certification should never be the main goal of any security activity. They should be a natural step or a side effect of any sound security program (assuming the regulation / standard / certification program is reasonable). Furthermore, BB states that one of the challenges with certification is the definition of a true benchmark, declaring that if there is no true benchmark, certification becomes useless for both vendors and end users.

After this, BB listed the different PPP where ABB is currently participating. He highlighted the US-CERT, the CPNI.NL and the CPNI.UK. Then, BB also listed those cyber security standardisation initiatives supported and driven by ABB.

BB continued his presentation by introducing the Robustness testing process at ABB. As a supporting centralised and independent testing facility, ABB has formally established the ABB's device security assurance centre. It is a formalized part of all device development, which assures well-defined and consistent approach towards cyber security. It utilizes

commercial, open-source and proprietary tools and employs 5 full time testers. Moreover, during 2010 more than 120 tests were performed.

BB states that ABB was the first vendor to have systems tested at Idaho National Laboratories SCADA test bed, starting the tests in 2004. Currently, ABB has tested 3 different systems at INL. ABB considers these tests at INL very valuable for both ABB and customers (in 2008, tests were carried out with the support of a customer consortium) and required thorough preparation, clear recipients of results, strict follow-up, and time and money.

ABB is following a defence in depth strategy on cyber security. As a result ABB established a commercial partnership with Industrial Defender, a ICS cyber security leading company. Therefore, ABB offers its customers robust, security enabled ABB products combined with Industrial Defenders' cyber security solutions.

BB ended his presentation by explaining how the customer support in ABB is dealing with cyber security issues. He presented to the audience their security patch validation procedures, their malware protection through regular AV, malware protection through Application White Listing (AWL), and finally, ABB's application patches management procedures.

1.6 ENISA Recommendations on ICS Security

RL started his presentation on the recommendation of the ENISA ICS Security Study, by presenting the aim and scope of the study. He stated that these included:

- A description of the ICS security panorama, including threats, risks, and challenges, as well as tacking stock of national and pan-European initiatives.
- The identification of gaps
- Propose recommendations to address these gaps
- To engage stakeholders into dialogue

RL continued explaining briefly the approach to the study, declaring that Recommendations are based on Key Findings, which in turn are based in the survey and interviews and in Desktop Research. For more information on this see EE's presentation and refer to the Study report.

After this introduction, RL started presenting the recommendations of the study. The approach to the presentation is to list the basic key findings and other key data that are behind each of the recommendations so that the experts could discuss on this and provide their impression.

1.7 Description of the ENISA ICS Security Study

EE started his presentation explaining that the study was divided into two main phases, the Stock taking phase and the Analysis phase. The stock taking phase consisted in taking stock of threats, risks and challenges; emerging issues; initiatives; solutions; and known good practices, standards and policies in the domain of ICS security. EE further explained that the result of this phase can be consulted in Annex I. Desktop Research Results (Current ICS panorama), Annex III. ICS Security Related Standards, Guidelines and Policy documents, and Annex IV. ICS Security-related Initiatives. On the other hand, the Analysis phase was about the qualitative analysis of the data. These data comes from different information sources and therefore they are quite heterogeneous and have to be consolidated and normalized as natural steps for analysis. EE mentions that detailed information on the analysis phase can be found in Annex II. Survey and Interviews Analysis and Annex V. Key Findings.

After this brief introduction, EE started to explain in detail the main aspects of the Stock-taking phase. He mentioned that this phase was based on three different information gathering methods: desktop research, survey and interviews. The desktop research process consisted in secondary research, involving the access to information from published resources. These published resources were of high reputation and included technical reports, specialised books, good practices and standards; in total more than 140 documents were analysed. EE also stresses the fact that these documents are published by relevant organisms, companies, consortiums or research centres. EE also highlights that apart from these documents, ICS security tools and services providers' whitepapers, product/services, sheets, etc. were included. Moreover the news coming from specialised forums and blogs, mailing lists, twitter, etc. were considered in order to keep up with the latest information. EE finished the desktop research by providing examples on the organisms, companies and consortiums that were used as a source of information: ISO/IEC, CPNI.UK, NERC, ESCoRTS, Gartner, DigitalBond, IEEE, and MSB. Moreover, he also described the tool that was used to automate the processing of the news coming from more than 20 specialised blogs and mailing lists and over 30 different Twitter Hashtags on the topic of ICS security. EE continued explaining the survey part of the study, which was based in a set of questionnaires containing between 25 and 27 open and closed questions. These questions were based on the Desktop Research and S21sec's own experience in ICS security real projects. The questions were divided into different categories: political, organizational, economic/financial, dissemination/awareness, standards and guidelines, technical. EE further explains that questions were formulated differently according to the targeted stakeholder when they ask about a common issue. Moreover, there are also several questions that are specific to that stakeholder type. EE states that the questionnaires were circulated in PDF format, which allowed S21sec to easily process the answers by means of an automated tool and at the same time, provide the participants with an easy-to-use, standard document format. Finally EE provided some figures on the survey. He highlighted that 164 questionnaires were sent out of which 48 were fulfilled and received back. Finally, EE provided detailed information on the Interviews process. He stated

that more than 20 interviews were conducted in a personal basis by means of audio conferences, using either Skype calls or regular telephone calls.

Furthermore, customised topics were also included in some cases. Some examples of these topics are: Legislation on attacks against ICS, convenience of an ICS-CERT, cloud computing for ICS.

Finally, EE ended this part of the presentation with an overview on the figures of the Desktop Research phase.

Then EE continued presenting the second phase of the Study, the Analysis phase. He started by introducing the necessity of consolidating and normalising the raw and heterogeneous data coming from the Stock taking phase before any analysis can be done. In order to do this, EE declared that they defined 57 knowledge concepts classified into different categories. Each concept represents a specific topic of ICS security.

Questions in the interviews and the questionnaires are defined to match one of these 57 concepts which help for further process.

Additionally, the information has to be normalised. Open questions and interviews represent the most complex and unstructured data (i.e. as many different answers as respondents). Therefore it is of key importance to process the answers and extract common points/aspects. EE explained that this was done manually based on the raw data.

EE highlighted that the data is analysed and consolidated by means of dedicated, proprietary tools developed ad-hoc for this process.

Once this process is done, the data was analysed qualitatively to obtain structured set of information: graphs, tables, statistics, etc. Out of these structured sets of information basic pieces of knowledge are extracted. EE called these pieces of knowledge “Key Findings” and he defined them as “the most relevant and influential observation from the desktop research, the survey and the interviews”. EE also stated that a “Key Finding” might show an emerging issue, a disagreement among stakeholders, tendencies in answers, etc. Moreover, EE declares that Key Findings are linked to the information sources to assure traceability and good reasoning. To illustrate this, EE presented an example of a Key Finding of the study.

Finally, EE mentioned that Key Findings are the basic element to ultimately derive the 7 recommendations of the ICS Security report.

EE ended his presentation listing some of most interesting figures on Key Findings.

1.8 Open discussion

Before the lunch-time an open discussion took place on several aspects related to ICS security.

One of the attendees asked the audience about the existence of simulation tools on ICS cyber security which are able to represent the connections among the different SCADA components. The following individual answers on the subject were provided by different participants:

- Existing simulators in the electricity sector could be used to represent ICS.
- It is impossible to address all application areas only with simulation tools. Simulators should rather respond to specific scenarios.
- It would be interesting to have a more centralising tool instead of having several "domestic" ones.
- Interdependencies are a critical aspect to be tackled by such tools.
- A reference to some universities working on availability aspects was provided. For example to Dresden University of Technology (Germany).

There was also a short debate on ICS security certification. One expert suggested that it would be necessary to define both a certification framework and a test bed. Moreover, another expert expressed that a general platform should be defined from which more specific ones should derive.

1.9 Topic discussion on the recommendations and the key findings of the study

The discussion was focused on the recommendations for ICS protection proposed by ENISA. What follows is a summary of the comments done by the experts for each recommendation.

1.9.1 R1. Creation of national and pan-European ICS security strategies

One of the experts participating in the workshop highlighted that the proposed security strategies should not only focus on ICS security but they should have a broader scope (e.g. Smart Grid). Moreover, he thinks that they should be included in existing cyber security strategies. Another expert supported this idea by saying that an integrated strategy is needed since ICS might also depend of other infrastructures such as telecommunications.

As it was explained by RL, the ICS-relevant country situation differs in various regions of Europe (in some of them ICS operators are mostly private while in others publicly-governed, in some of the countries, the governance is centralised while in others there are multiple dispersed independently managed infrastructures, etc.) there is a need for the country-centric approach in which each country develops its own ICS security strategy. Eventually a pan-European strategy could be developed by unifying the national documents.

However, four participants opted for the alternative top-down approach, where the reference European strategy should precede the national ones which can derive from it. These experts believe that otherwise the development of the strategies in some Member States may be lagging.

Furthermore, two experts from the audience proposed that in addition to considering the common aspects of ICS security, the strategies should take into consideration sector specific aspects (i.e. identify the critical business processes, behavioural characteristics, etc.).

Finally, an expert concluded that under his point of view the ICS security activities should be fostered in the existing CIIP and CIP European strategies.

1.9.2 R2. Creation of a good practices guide for ICS security

Most of the audience agreed that the existing best practices should be taken as a reference in order to not duplicate the work ('not to reinvent the wheel'). They also agreed that there should be some kind of European reference material. To achieve this, one expert suggested that a reference document should be built upon the existing material, which is sometimes country specific or might not be ICS specific. To this regard, RL explains that the common practice when defining a pan-European initiative is to leverage what has been done in Member States and make a single reference for all the Member States. Furthermore, an ICS vendor representative also claimed that for vendors it would be much easier to only deal with one reference document than with multiple ones.

However, another expert expressed his concerns on having a reference European guideline by asking to the audience if such a reference guideline would replace all the others.

During the discussion four participants agreed that there is space for guidelines with a more practical approach (i.e. focusing not so much in "what-should-be-done" but in "how-to-do-things"). This idea was reinforced by an expert who clearly stated that some current good practices need to be read "more than ten times" to understand their content. These experts agreed that reference guidelines should help on how to implement existing good practices. Additionally, a representative from a public body considered that more important question is if industry implements good practices than which good practice they implement (as long as they make use of relevant ones as reference). Moreover, this same expert considered that this would be more efficient to use an existing guideline than making a reference guideline which combines existent good practices into a set of new documents since this approach would also leverage current efforts.

RL highlighted the fact that the majority of the experts asked before during the survey and the interviews had a different opinion on this issue. There was a preference for a high-level reference guideline instead of too low-level/technical ones. Moreover, he also explained that according to the Study there is a lack of confidence and common agreement on which existing good practices to follow, so some experts are "lost". RL also pointed out that several experts, during the interviews and in the survey, suggested that too technical/low-level guidelines could provide too much information for a potential attacker.

EE also explained why the ENISA recommendation suggested having European reference security guidelines. This is because some ICS operators have been involved in mergers of companies operating in different countries with different reference best practices, which reinforces the need for a common reference at the European level.

One of the attendees considered important to define a working group to further discuss the requirements of these reference guidelines, since the issue is complex to be fully addressed only during workshop.

An expert suggested that a starting point could be to have an organisation or body in charge of updating the set of existing good practices, technical reports and other reference material (including information on their purpose, scope, sector, etc.) as done in the ESCoRTS project.

Additionally, another expert further suggested that activity areas (i.e. what should be done) on ICS security should be identified, and based on them management awareness should be fostered. This expert considers than once this is achieved, it is possible to go deep into each one of these activity areas and develop guidelines, best practices and eventually even future regulations.

Finally, RL asked the audience on their preference regarding who could be in charge of developing such reference guidelines and how should this be done. ENISA was indicated as the best candidate for this task as, according to an expert – ENISA has demonstrated good skills in performing research studies and bringing different stakeholders together. The same expert considers that defining guidelines can be a real challenge for individual organisations or governments and therefore an organisation like ENISA is much better positioned for this work. Another expert also stated that it might also be interesting to have a joint initiative between ENISA and all the stakeholders in the different sectors where ICS are important (e.g. Industry associations, energy companies, water supply, etc.)

1.9.3 R3. Creation of ICS security plan templates

RL started the discussion by explaining to the audience the definition of the term “security plan” according to the Study report.

An expert started a noteworthy discussion on the importance of the term security in ICS. He expressed his concern about the fact that the term security does not include aspects such as redundant components, continuity and dependability, aspects that are collectively named with the word resilience. He expressed that resilience should be considered in combination with security to guarantee that an ICS can recover from a successful attack. Three other experts responded to this idea. For instance, another attendee considered that security is more related to the CIA triad (Confidentiality, Integrity, and Availability). Based on his own experience with power plants, he explained that Integrity and Availability are the most important security aspects. Moreover, he mentioned that when dealing with industrial equipment at the end of their life-cycles, it might happen that spare parts are not available anymore to replace the components that start to malfunction. He considers that it is needed to have different alternatives (i.e. a broader approach) to deal with this kind of situations. Then, another expert stated that according to him, availability does not mean resilience or just having a reconfiguration strategy when a systems’ failure occur. Finally, an operator representative further developed this by arguing that there are deep differences between cyber security and ICS security. Under his point of view, cyber security does not take into

account the dynamics of the system, while the broadest conception of ICS security would do so. He considers too strict to reduce the security problem of ICS to a cyber security problem. He thinks that the term resilience takes into account the behaviour of the system before and after an occurrence (e.g. attack).

On the other hand, RL supported the idea of considering "security" in its broadest sense and he explained that this is the way in which it is used in the report. An expert also mentioned that when someone talks about cyber security almost everyone understands that it is in the widest sense. Moreover, another expert explained that in The Netherlands when someone talks about ICS cyber security it implies activities such as system monitoring, analysis, resilience, response, education and training, etc. This includes all the topics mentioned by the previous speakers. He suggested to clearly writing down what it is meant with security as a way to reconcile the parties involved. Another expert reinforced this idea by saying that the same words might have different meanings depending on your professional background (e.g. IT vs. Industrial people). He provided the example of the term "disaster recovery". For people with an industrial background this would only mean how to recover from a plane crash, or a gas explosion while if you have an IT background it might mean something more related to the cyber world. This expert suggests keeping this in mind but internally, since that is more about a general security concept which is not the scope of the study.

Then returning to the main subject (R3), an expert then expressed that he is in favour of the proposed templates. He explained that they will tackle the "real problems" and will be one of the most practical aspects of implementing ICS security. He mentioned that he represented a company that uses a broad range of systems (industrial protection, ICT systems connected to those systems, etc.). Because of this broad range of systems, they (as a company) would appreciate to have a raw framework that allows them approach security, at least from an overall point of view.

RL expressed that he assumes that these templates are very welcome. Then he recalled the topics that should be covered by these templates and asked if they are any others to be added or some to be removed.

This initiative was very well received by the audience since it is one of the more practical ones. An expert highlighted that there are many different systems in place and that these plans would really help improving their security posture. An expert answered that business recovery/business continuity should be included as well. To this regard, another expert explains that there are several names to refer to almost the same thing: contingency plan, business continuity, and disaster recovery, and suggested to use the term business continuity since this is a "less scary" term. An expert proposed the BS 2599 as a reference for business continuity management and RL said thank you for this reference and mentioned that existing guidelines as this one should be taken into account for the development of the templates.

Finally, another expert mentioned that in the UK they have questionnaires for the operators which focus on all the key areas of security. This tool allows companies to compare themselves against what it is expected and to know what is their current status (assess their

current security posture). The expert mentioned that risk management is the key topic to address by the templates, since this is a basic aspect of day to day security and it takes into account all security aspects, including business continuity.

1.9.4 R4. Foster awareness and training

Firstly, one of the experts agreed on the fact that this recommendation is of paramount importance, especially in what refers to raising awareness of CEOs. He pointed out that the European Commission could play an important role in putting into practices these recommendations through the organization of events, meetings, conferences and similar events all around Europe. To this regard, Alejandro Pinto states that the European Commission has already planned high-level conferences for CEOs to foster the awareness on ICS.

The attendee who took part in the discussion as the first stated that it is necessary to have some kind of mobile training facility to show the CEOs the possible effects of hacking into an ICS as well as how easy this task could be. This would get the attention of companies' Management.

Another participant suggested that, to capture the attention of the CEOs, it is necessary to get a picture of real incidents and show them to the Management. He declared that many real incidents are unknown to the Top Management. The expert stated that using examples from other companies will probably not have the desired effect in the Top Management. He considers that it would be more effective to demonstrate that it is possible to hack their company's ICS. For this purpose, a test bed could be very handy. This opinion was seconded by another expert.

Additionally, one of these experts suggested that it would be a good idea that the European Commission leaded such training initiatives. Two levels of training were identified by this same expert:

- National with mobile training facilities
- High level training facilities at the European level

Regarding this topic, RL asked the audience about who they consider that should be responsible for delivering the training, proposing either academia, or universities, private sector, etc. Answering the previous question, one of the experts stated that this would depend on the target audience. He identified two groups based on the Management level: users/operators and CEOs. In the case of users/operators and future CEOs, he considered that these trainings could be carried out by universities or training professionals through master, MBAs, specialised courses, etc. For the CEO level, the underlying principle should be "bring the topic to the forums and associations of which the current CEOs are part". So depending on the targeted audience trainers would be different. However, he also considered that there are some tasks for which all training stakeholders could be involved.

Finally, RL asked the audience if ICS systems should be isolated for security reasons, as well as what was the opinion of the experts in relation to the paradigm of security by obscurity. Regarding to this question, three participants indicated that the isolation of the systems is an important challenge of the security on ICS. Moreover, they agreed that nowadays isolation is not possible because interconnections with corporate systems and services are necessary. At this point these same experts suggested that it is necessary to focus in isolation (e.g. by zoning and defining security levels for each type of zone) and not in "disconnection by implementing the appropriate security controls. They also stressed that this is very different to security by obscurity. To this regard, an expert highlighted that hiding information on ICS from the outside world is not the appropriate approach. He mentioned that in the Black Hat conference since the last three years hackers are already interested in this topic. Moreover, he mentioned that Stuxnet has demonstrated that security by obscurity is an obsolete paradigm.

1.9.5 R5. Creation of a common test bed, or alternatively, an ICS security certification framework

One of the participants opened the debate by suggesting that it is necessary to create a mobile laboratory or mobile test bed for training. When asked by RL on the feasibility of such a mobile facility, the expert answered that he has experience with such kind of mobile test beds. Another participant highlighted the effectiveness and necessity of something similar to the Idaho National Laboratory as a fixed laboratory with the appropriate resources for testing ICS equipment. The first participant stressed the importance of mobile laboratories since small companies might find challenging to access a fixed laboratory for testing their products. Based on his impression RL then concludes that most of the audience is in favour of having such common test bed and asked the audience about who should be in charge of it and how things should be done.

One of the experts answered RL by referring to the CyberTEC platform and proposing it as a reference model for this recommendation. The expert also mentioned that more than one laboratory could exist in Europe, but cooperation among them would be essential.

He pointed out that this test bed should be driven by governments, but the private sector could also play a leading role (e.g. Alliander in CyberTEC). Actually, in the case of CyberTEC it was highlighted that the private sector was investing a lot of money and effort into the initiative and the public sector is providing support. Moreover, there was a consensus on the fact that such an initiative should be publicly and privately funded. Additionally, all the different stakeholders (manufactures, integrators, end-users/operators, public bodies, etc.) should be involved in the process. Finally, RL mentioned his concerns regarding how to be sure that such platforms are not used to promote some security solutions of specific companies. Answering to that, the previous expert stressed that such a platform should have a neutral character avoiding that just a few companies can take benefit of it and being open to anybody who would like to make use of it.

1.9.6 R6. Creation of national ICS-CERTs

RL started this part of discussion highlighting the interest of some state members on national or European ICS-CERTs as platforms for knowledge sharing and mentioned EuroSCSIE as an example of this kind of platform.

The first participant to take part was in favour of having national ICS-CERTs since he considered that it would be easier for national-level CERTs to identify and track ICS that are critical in the region they operate. He was also in favour of promoting the collaboration among these CERTs at the European level in order to exchange experiences between different sectors (water, energy, etc.) and countries. He then asked RL about what would be the best way to carry out this procedure. Answering the previous question, RL remarked that, under his point of view, at the moment the best knowledge exchange platform at European level is EuroSCSIE.

On the other hand, another participant stated that he is not in favour of segregating ICS CERTs from existing national CERTS. He considered that current national CERTs could assume these tasks perfectly (e.g. sharing of ICS knowledge).

RL asked the audience whether the best way to successfully create such initiatives is to build them as public-private partnerships. In relation to this question, one of the experts showed his agreement with public-private partnership initiatives since he considered this approach the best way to get involved the private sector. By doing so it would be possible to achieve a more detailed knowledge on the particularities of ICS systems and to facilitate information exchange on the national level.

Finally, most of the audience was not in favour of having independent sector-oriented ICS-CERTs.

1.9.7 R7. Foster research in ICS security leveraging existing research programmes

One of the experts considered that research is a priority so it should be highlighted as a very important recommendation. He further detailed that the current knowledge level at this moment is not enough to appropriately tackle the ICS security and resilience problems. He considered that research should focus on how to make a quantitative evaluation of the current state of the security level and resilience capabilities of ICS systems. He declared that this is nowadays very difficult to implement and verify.

Another attendee stated that the workshop is a great opportunity to change the way in which things are being done. For example, thinking on the Smart Grid, he remarked that there is a need to research on how to deal with simultaneous attacks against multiple substations in electricity distribution environments. Moreover, he also proposed to further investigate on CI interdependencies spanning several countries. Finally, he also pointed out that it is appropriate to discuss about if the current control model is the more secure way of doing things, and used the example of the Internet model, which works in a distributed/decentralised and autonomous way. In his opinion, there is a need to investigate

alternatives to the classical control/supervisory model and change the paradigm by leveraging on the research being done in the Smart Grids.

1.10 General Discussion

After the discussion on the different recommendations, RL requested opinions and suggestions from the attendees regarding the report.

One of the experts suggested making clear in the report that “awareness should be considered the most urgent recommendation”. He stated that the ICS security national and European strategies should start with an awareness programme. Another expert stressed the fact that Top Management awareness is very important, and because of this, several areas should be addressed. RF pointed out that the involvement of the Top Management has been considered as a key finding in the report. Following the discussion thread, another participant stated that key messages for Management should be consensus-based on the opinions of different stakeholders (e.g. ENISA). He considered this very important to have a real impact. For instance, it would be necessary to make Management understand that 0-risk does not exist. Additionally, another attendee supported this idea and stated that it is also important to change Top Management mentality about security as an expense rather than as an investment.

On the other hand, one of the experts suggested including in the report the stakeholder groups who have taken part in the ICS study. RF explains that this information is already included, specifically saying that six different groups of stakeholders were addressed for which five different questionnaires defined in order to maximize the information gathering. He further recommended the participant to read Annex II on the "survey and interview analysis".

Moreover, two experts stressed the importance of giving the report the appropriate attention in order to make more people aware of the proposed recommendations. They suggested making a close follow-up of the report and proposed the EP3R, the EU PPP, as the umbrella to discuss further the recommendations provided.

Additionally, it was suggested that the report should highlight that the EU should enforce a higher openness in information sharing.

On the other hand the opinion of the most of the experts is that the report on ICS security is a very good document.

1.11 Wrap-up

Before the end of the Workshop, some comments were provided to ENISA.

The audience appreciated the way in which ENISA operates. Participants believe that ENISA should continue its activities in the field of ICS Security and in particular in engaging all the relevant stakeholders into the common effort to protect ICS. In general it is the common sense that this is the role of governmental agencies – to lead such initiatives.

Experts believe that there is still space for increasing the awareness of the ENISA's role in the private sector, and the ICS operators such as ENEL.

Finally, the audience considers that ENISA should foster knowledge distribution and awareness rising, especially for SMEs.

2 Abbreviations

ACC	American Chemistry Council
AD	Active Directory
AGA	American Gas Association
AMETIC	Multi-Sector Partnership Of Companies In The Electronics, Information And Communications Technology, Telecommunications And Digital Content
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programming Interface
API	American Petroleum Institute
ARECI	Availability And Robustness Of Electronic Communication Infrastructures
ARP	Address Resolution Protocol
AV	Anti-Virus
BDEW	Bundesverband Der Energie Und Wasserwirtschaft
BGW	Bundesverband Der Deutschen Gas Und Wasserwirtschaft
BW	Band Width
CA	Certified Authority
CC	Common Criteria
CCTV	Closed-Circuit Television
CEN	European Committee For Standardization
CENELEC	European Committee For Electrotechnical Standardization
CERT	Computer Emergency Response Team
CFR	Code Of Federal Regulations
CI	Critical Infrastructure
CI2RCO	Critical Information Infrastructure Research Coordination
CIFS	Common Internet File System
CIGRE	Conseil International Des Grands Réseaux Électriques
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructures Protection
CIKR	Critical Infrastructure And Key Resources
CIP	Critical Infrastructures Protection
CIWIN	Critical Infrastructure Warning Information Network
CNPIC	Centro Nacional Para La Protección De Infraestructuras Críticas
COTS	Commercial Off-The-Shelf
CPNI	Centre For The Protection Of National Infrastructures
CRP	Coordinated Research Project
CRUTIAL	Critical Utility Infrastructural Resilience
CSSP	Control Systems Security Program
DCS	Distributed Control Systems
DD	Data Diode
DDOS	Distributed Denial-Of-Service Attack
DHS	Department Of Homeland Security

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

IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation Of Automatic Control.
IFIP	International Federation For Information Processing
IMG-S	Integrated Management Group For Security
INL	Idaho National Laboratory
INSPIRE	Increasing Security And Protection Through Infrastructure Resilience
INTER-SECTION	Infrastructure For Heterogeneous, Resilient, Secure, Complex, Tightly Inter-Operating Networks
IO	Input/Output
IPS	Intrusion Protection System
IPSEC	Internet Protocol Security
IRBC	Ict Readiness For Business Continuity Program
IRIIS	Integrated Risk Reduction Of Information-Based Infrastructure Systems
ISA	Instrumentation, Systems And Automation Society
ISACA	Information Systems Audit And Control Association
ISBR	Information Security Baseline Requirements
ISMS	Information Security Management System
ISO	International Organization For Standardization
IST	Information Society Technologies
IT	Information Technologies
JHA	Justice And Home Affairs
KF	Key Finding
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPDE	Low Density Polyethyl
MAC	Media Access Control
MCM	Maintenance Cryptographic Modules
MIT	Middleware Improved Technology
MSB	Swedish Civil Contingencies Agency
MTU	Master Terminal Unit
NAC	Network Access Control
NBA	Network Behaviour Analysis
NBA	Network Behaviour Analysis
NCI	National Critical Infrastructure
NCS	Norwegian Continental Shelf
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NHO	Norwegian Business And Industry
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan

NIS	Network And Information Security
NISCC	National Infrastructure Security Co-Ordination Centre
NIST	National Institute For Standard And Technologies
NISTIR	National Institute Of Standards And Technology Interagency Report
NRC	Nuclear Regulatory Commission
NRG	Nuclear Regulatory Guide
NSAC	National Security Advice Centre
OLF	Norwegian Oil Industry Association
OPC	Ole For Process Control
OS	Operating System
OSG	Open Smart Grid
OSI	Open System Interconnection
OTP	One Time Password
PCCIP	Presidential Commission On Critical Infrastructure Protection
PCD	Process Control Domains
PCN	Process Control Networks
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PDCA	Plan, Do, Check, Act
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PP	Protection Profiles
PPP	Public Private Partnerships
QOS	Quality Of Service
R&D	Research And Development
RAT	Remote Administration Tools
RF	Radio Frequency
RSS	Really Simple Syndication
RTU	Remote Terminal Units
SANS	System Administration, Networking, And Security Institute
SCADA	Supervisory Control And Data Acquisition
SEM	Security Event Manager
SEMA	Swedish Emergency Management Agency
SIEM	Security Information And Event Management
SIM	Security Information Management
SIMCIP	Simulation For Critical Infrastructure Protection
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier

SSL	Secure Sockets Lay
SSP	Sector-Specific Plan
ST	Security Targets
SW	Software
TCG	Trusted Computing Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TISP	The Infrastructure Security Partnership
TKIP	Temporal Key Integrity Protocol
TOE	Target Of Evaluation
TR	Technical Report
TSWG	Technical Support Working Group
UDP	User Datagram Protocol
UK	United Kingdom
USA	United States Of America
VDI	The Association Of German Engineers
VDN	Verband Der Netzbetreiber
VIKING	Vital Infrastructure, Networks, Information And Control Systems Management
VPN	Virtual Private Network
VRE	Verband Der Verbundunternehmen Und Regionalen Energieversorger In Deutschland
WAF	Web Application Firewall
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIB	International Instruments Users' Association
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu