Smart Grid Security

Minutes of the Workshop

[Deliverable – 2012-03-31]

Contributors to this report

- Konstantinos Moulinos, ENISA
- Rafał Leszczyna, ENISA
- Elyoenai Egozcue, S21sec
- Daniel Herreras Rodríguez, S21sec
- Jairo Alonso Ortiz, S21sec
- Victor Fidalgo Villar, S21sec
- Luis Tarrafeta, S21sec

Agreements or Acknowledgements

To be completed after the workshop. It will include at least:

- external reviewers,
- participants in the interviews and poll,
- attendants to Workshops,
- contributors to distribution list discussion topics,
- etc.

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@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

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

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

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

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

Reproduction is authorised provided the source is acknowledged.

Contents

1 Introduction 2

2 Summary of the 6th meeting of the Expert Group on Security and Resilience of Communication Networks and Information Systems for the Smart Grid 4

3 Presentation of the results of the ENISA Study 6

4 Morning Session A 12

4.1 Security by design: The role of standards (including architectures) in achieving end to end security...12

4.2 Certification, testing and pilots: How can we learn from each other? 14

5 Morning Session B..17

5.1 Cyber security life cycle: How smart grids providers could implement proper security policies and measures? 17

5.2 Minimum security measures: How to develop them across the EU? 17

6 Test and learning platform for ICS and Smart Grids 21

7 Afternoon Session C...24

7.1 National cyber security strategies for smart grids: The role of Member States in enhancing cyber security of smart grids 24

7.2 Towards and EU wide cyber security strategy for smart grids: How all smart grids cyber security initiatives make sense for Member States and the EU? 25

8 Wrap up and future directions 27

1 Introduction

On the 29th February 2012 ENISA organised a workshop where the results of the Study[1] on smart grid 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, to discuss on several hot topics related to smart grid security, and to gather the different opinions on what could be the next steps of ENISA in the field.

All those experts who participated in the study were invited to the workshop, and around 50 finally attended the event. They were representatives of all the stakeholders types considered for the study: manufacturers, DSOs, TSOs, security tools and security services providers, smart grid services providers, academia/research, public bodies, and standardisation bodies.

The agenda of the Workshop was the following:

09:00 – 09:30	Registration	
09:30 – 09:35	Welcome and agenda of the day	
09:35 – 09:45	*Summary of the 6th meeting of the expert group on security and resilience of communications networks and information systems for the smart grid*	Alejandro Pinto-Gonzalez, DG INFSO
09:45 – 10:15	*Presentation of the results of the ENISA study*	Rafal Leszczyna, ENISA
10:15 – 10:45	Morning session A (discussion) • *Security by Design: the role of standards (including architectures) in achieving end to end security.* • *Certification, Testing and Pilots: How can we learn from each other?*	all participants
10:45 – 11:15	Coffee Break	
11:15 – 12:30	Morning session B (discussion) • *Cyber Security Life Cycle: How Smart Grids providers could implement proper security policies and measures?* • *Minimum Security Measures: How to develop them across the EU?*	all participants
12:30 – 13:30	Lunch	
13:30 – 14:00	*Test and learning platform for ICS and Smart Grids*	Bram Reinders, Alliander
14:00 – 14:30	Afternoon session C (panel) • *National Cyber Security Strategies for Smart Grids:*	

[1] *Smart Grid Security, Recommendations for Europe and Member State, ENISA, 2012, available at http://www.enisa.europa.eu/activities/res/.....*

	The role of Member States in enhancing cyber security of Smart Grids. - *Towards an EU wide Cyber Security Strategy for Smart Grids: How all Smart Grids cyber security initiatives make sense for Member States and EU?*	
14:30 – 15:00	Coffee Break	
15:00 – 15:45	Afternoon session C continued	
15:45 – 16:00	Wrap Up and Future Directions	

The following subsections represent the minutes of the Workshop. The reader will be able to easily get a global outlook on what took place during the discussion sessions as well as on the different topics that were discussed by the presenters.

2 Summary of the 6th meeting of the Expert Group on Security and Resilience of Communication Networks and Information Systems for the Smart Grid

Alejandro Pinto (AP), EC's policy officer of DG INFSO was in charge of formally opening the workshop. He is the point of contact from the EC for the Expert Group on Security and Resilience of Communication Networks and Information Systems for Smart Grids (from now on, DG INFSO's Ad-hoc EG), an initiative in which ENISA is also actively participating. This EG had its 6th joint meeting session on the 28th of February in Brussels, and many of its attendees were also contributing to the study. Nevertheless AP took advantage of this workshop to share with all the audience the objectives and the work that it is being accomplished by this group and to make a call for new participants.

The European Commission created the Ad-hoc EG to:

I. Better understand the views and objectives of the private and public sectors on the ICT security and resilience challenges for the smart grids
II. Identify and discuss about the related policies at EU level

He continued by presenting the policy context which supports the Ad-hoc EG, where COM(2011) 163 on Critical Information Infrastructure Protection as well as COM(2011) 202 on Smart Grids were presented as the two main pillars. Specifically, COM (2011) 202 declares that the Commission should continue bringing together the energy and ICT communities within an expert group to assess the network and information security and resilience of Smart Grids.

After this brief introduction, the two main objectives of the EG were presented:

I. The identification of European priority areas for which action should be undertaken to address the security and resilience of communication networks and information systems for smart grids, as well as the definition of recommendations on how to progress on each of these areas at the European level.
II. The identification of which elements of the smart grid should be addressed by the EG (e.g. smart appliances, smart metering, smart distribution, smart (local) generation, smart transmission) as well as the identification of key strategic and high level security requirements, good practices based on learned lessons and the proposition of mechanisms to raise awareness among decision makers.

The EG has already met for six times, being the last one on the 28th of February 2012. Based on the aforementioned two main objectives, a Programme of Work was defined with the mission of contributing to a coherent and increased effort to improve the cyber security of the smart grids and which focuses on the security and resilience of communication and information systems that are critical for the performance of the physical electricity infrastructure. This programme of work includes four main areas, divided into twelve work packages. The areas and WPs are the following:

I. Area 1. Risks, threats and vulnerabilities
   a. WP 1.1 Identify and categorize all relevant smart grid assets
   b. WP 1.2 Develop an attach/threat taxonomy for relevant assets
   c. WP 1.3 Develop a countermeasure taxonomy for relevant assets
   d. WP 1.4 Develop a high-level security risk assessment methodology for relevant assets

II. Area 2. Requirements and technology
   a. WP 2.1 Security requirements
   b. WP 2.2 Extend smart grid requirements to include effective security measures
   c. WP 2.3 Research smart grid communication protocols and infrastructures to incorporate data security measures
   d. WP 2.4 (Public) procurement

III. Area 3. Information and knowledge sharing
   a. WP 3.1 Develop a cross-border alliance between Member States (MS) and relevant competent bodies

IV. Area 4. Awareness, Education and Training
   a. WP 4.1 High level conference for strategic leaders
   b. WP 4.2 Propose initiatives to increase stakeholder awareness on data security
   c. WP 4.3 Skilled personnel on cyber security in energy industry

AP further stated that the first conclusions of the group will be made public in the second quarter of 2012. Besides, it is acknowledged that the first outcomes could immediately feed the current policy process. To this regard, two different policy initiatives, the European Strategy for Internet Security and EU-US PPP Working Group on Cyber Security of Industrial Control Systems and Smart Grid were pointed out.

Finally, AP presented a number of European and international level initiatives with which the group is well engaged. These include the Expert Group 2 of the Smart Grid Task Force of the Commission, the CEN/CENELEC/ETSI Smart Grid Information Security working group, EuroSCSIE as well as the aforementioned EU-US Expert Security Group Public-Private Partnership on Cyber Security of Industrial Control Systems and Smart Grids.

3 Presentation of the results of the ENISA Study

The study aimed at providing an outlook of the security panorama of smart grids, including the identification of threats, risks and challenges as well as the take of stock of the pan-European initiatives on smart grid security. Furthermore, the study identifies gaps and provides recommendations to fill these gaps and at the same time involves the different stakeholders into an open dialog to discuss on the measures being proposed. ENISA will follow up carefully these recommendations and will provide specific actions to improve them and to address their implementation.

Just after presenting the aim and scope of the Study, RL explained to the audience the approach that was followed in the study. The main key findings of the study were based in the raw data provided by the experts during the interviews and the questionnaires as well as in the information coming from the desktop research phase. A key finding is a basic element of knowledge which represents the most relevant and influential observation from the desktop research, the survey and the interviews. A key finding might show an emerging issue, a disagreement among stakeholders, tendencies in answers, etc. and are the basic element to ultimately derive the recommendations of the Study. The desktop research was based on more than 230 documents, which include high reputation publications, such as technical reports, specialised books, good practices, standards and scientific papers; other technical documents, such as whitepapers, product/services, sheets, etc.; and latest news coming from forums, mailing lists, twitter, blogs, etc. Regarding the survey and the interviews, over 300 experts were contacted, from which 50 answered the questionnaires and 23 were interviewed. Besides, both the interviews and the poll were well balanced including an even distribution of the different stakeholder types participating in the study (i.e. manufacturers and integrators, smart grid services providers, academia/R&D, security organisations, public bodies, DSOs, TSOs, and standardisation bodies).

Around 90 *key findings* were identified in the Study and were classified into the following categories:

- The biggest challenges of the Smart Grid (SG)
- The SG business case
- Basic components of the SG
- SG pilots and cyber security
- Basic aspects for a secure SG
- SG cyber security challenges
- Current SG initiatives on cyber security
- Risk assessments in SG
- Certifications and the role of NCAs
- Measuring cyber security in the SG
- Managing cyber attacks
- Research topics in SG security

The most relevant *key findings* presented:

- Cyber security, privacy and fraud prevention are considered key for the success of the smart grid
- Cyber security and privacy are being addressed independently
- Security is being addressed more as an overlay than as part of the design phase
- Defence in depth + security by design = guiding principles
- Integration of the end user property + intensive use of ICT + the use of Internet and public networks => much wider attack surface
- Reliability and resiliency of the grid are key factors driving the smart grid business case
- Lack of definition of the smart grid concept: “Are added-value services (e.g. demand-side management) included? Is the smart home/industry/building part of the grid?”
- Lack of a standard reference architecture
- Cyber security is a second-line issue in smart grid pilots and is tested in massive deployments
- It is necessary to train and raise awareness among operators, manufacturers and consumers
- Security efforts should not only focus on smart meters but also on substation automation, micro grids, SCADA, telecommunication networks, etc.
- Infrastructures at consumer’s premises should be fool-proof since they are out of the control of the DSO or the service provider.
- Lack of expertise and budget limits in the root causes for dismissing cyber security
- Some technical challenges: 1) Integration of legacy systems, 2) secure devices, 3) activity monitoring
- Inexistent/incomplete regulations can have security consequences (e.g. too quick start of meter roll-outs; risks of integrating gas, heat and electricity)
- About security initiatives: duplicity of topics, lack of visibility, same experts in all initiatives, etc.
- Need for a coordinating entity on smart grid cyber security and privacy initiatives
- DSOs and TSOs should undertake mandatory risk assessments
- Need for a specific risk assessment methodology
- NCAs should certify the security of SG product/set-up and organisations
- Today, standards-driven security certifications can be a burden because of immaturity of SG technology
- Alternative: quick tests (e.g. white box and code audits)
- Cyber security must be measured in terms of robustness, reliability and resiliency
- In case of incompliance there should be regulatory pressures
- (In)compliance results should be made public while not revealing sensitive information
- TSOs and DSOs are used to dealing with incidents. There are mechanisms in place for this.
- DSOs and TSOs should be in charge of cyber incident detection (IRRIS FP7 project)
- Operators should be obliged to report on cyber incidents

- Controversy on the need for a pan-European entity in charge of coordinating large scale cyber security incidents
- A centrally coordinating entity can worsen reaction times. Alternative: decentralized approach by improving procedures
- CSIRTs should not be the central piece but can play a role in incident management: advising the normal crisis management structures in place at the EU and MS

Based on the *key findings,* eight recommendations were developed. The recommendations were listed first and then a detailed review on the main aspects of these recommendations was performed. The main aspects that were highlighted included:

R1. Improve the regulatory and policy framework on SG cyber security

Key aspects:

- Develop specific documents and regulations
- To define the root principles, challenges, goals and needs of a European-wide cyber security strategy for SG

The regulatory framework should look for:

- Considering privacy and cyber security altogether
- Defining security objectives for current SG deployments (e.g. smart meters roll-outs)
- Demanding mandatory risk assessments
- Demanding security certifications: products and organisations
- Establishing regulatory pressures (e.g. fines) for not complying companies
- Making public (in)compliance results
- Asking for reporting in case of cyber security incidents

R2: Create an EU-level coordinating entity for SG cyber security initiatives

Key aspects:

- Establish a unique central coordinating entity at the EU-level
- With a global vision of EU and MS's initiatives on cyber security of SG (e.g. SGIS, DG INFSO's ad-hoc EG, …)

Objectives:

- Avoiding duplicated work
- Enhancing communication among task forces and work groups
- Defining a clear and unified strategy for ongoing and new initiatives
- Identifying synergies among national and European initiatives
- Disseminating the work being done
- Establishing a common dictionary of technical terms
- Managing lobbies

R3: Foster dissemination, knowledge sharing, awareness rising and training

Key aspects:

- Under the umbrella of the EU-coordinating entity
- Promoted by MS and EU
- Targeting grid operators, electricity service providers, manufacturers and end consumers
- Actively involve academia/R&D
- Increase DSO/TSO leadership

Objectives:

- Awareness-rising of C-level staff
- Training for manufacturers on how to build secure devices and applications
- Training for operators on threats and risks affecting security and resiliency of the grid
- Awareness-rising and training on fraud prevention, privacy, etc. of end consumers and service providers
- Encouraging existing initiatives to actively disseminate their work
- Analyse the creation of a knowledge sharing platform for DSOs and TSOs (and possibly other stakeholders) considering involving CISRTs

R4: Develop a minimum set of reference standards and guidelines

Key aspects:

- Led by the EU in collaboration with MS
- Leverage ongoing initiatives (e.g. DG INFSO's ad-hoc EG)
- Should set the basis for mandatory security assessments and for developing certification schemes

Minimum set of standards and guidelines:

- A common reference architecture
- A reference risk assessment methodology
- Technical requirements for SG systems
- Guidelines on security governance
- Guidelines for achieving fool-proof HAN/IAN/BAN

R5: Promote the development of security certification schemes

Key aspects:

- Promoted by EU public authorities
- Target product and organisational security
- Leverage existing initiatives such as CC, ISA99 and ISO 27K

Objective:

- Harmonize security and resilience requirements across MS

- Establish the base for a minimum set of auditable controls
- Accredit NCAs for certificate issuance

R6: Foster the creation of test beds and security assessments

Key aspects:

- Both tasks should be promoted by MS and the EU
- Test beds: should perform quick/agile security tests based in basic security principles (e.g. WIB's requirements for vendors)
- Security assessments: incentivize independent security assessments and pen-tests on DSOs, TSOs and other actors

Objective:

- Fill the gap while certification schemes are developed
- Once they are ready, test beds could become accredited certification evaluators

R7: Discuss the creation of a European entity and the role of CSIRTs in the coordination of cyber incidents

Key aspects:

- To be discussed by EU and MS
- Manage large scale cyber incidents reported by operators
- Coordinate transnational electricity infrastructures and national CIP agencies

Envisioned characteristics of the coordinating entity:

- To have a global overview of the situation of the European grid
- To have direct communication with normal crisis management structures and CSIRTs
- Responsible for escalating alarms
- Act in accordance with political decisions and pre-established incident handling strategies
- Understand and advice on the interdependencies inside the European power grid and affecting other CIs

R8: Foster research in SG cyber security leveraging existing research programmes

Key aspects:

- Leverage FP7 and Horizon 2020

Proposed topics of research:

- Protection of monitoring functionalities and automated decision making systems of the smart grid

- Robust, secure and resilient architectures (e.g. self-healing/graceful degradation, management of cryptographic material)
- Trust and assurance and end-to-end security (e.g. dependencies analysis, use-case modelling)
- Security in dependable systems
- Supply chain protection
- Secure smart grid in the cloud
- Legal and economic aspects of cyber security in the smart grid

4 Morning Session A

Firstly, EO introduced the two topics of Session A, which were security by design and certification, testing and pilots. In the first case, the topic was oriented towards the role of standards in achieving end to end security, while the second topic encouraged the experts to share their knowledge on on-going initiatives in the field of security certification and testing. Both topics are two of the most relevant issues highlighted by the study, and are at the core of recommendations 4, 5 and 6 of ENISA's study.

4.1 Security by design: The role of standards (including architectures) in achieving end to end security

As a general consideration on standards, experts declared that before developing any standard it should be analysed firstly what should be allowed/provided and what not. Otherwise, some stakeholders can consider the standards not relevant or could not be able to implement them for a number of reasons. This is considered especially true for risk assessments. According to the experts, nowadays stakeholders are working based on use cases but don't know what the final architecture of the smart grid is going to be like. Therefore, risk analysis aspects cannot be well addressed. It is not possible to deal with risk assessments if the architecture is not defined first. As a starting point for risk assessments in the smart grids, some experts suggested to leverage existing experiences in Europe on how stakeholders are currently undertaking real risk assessments. Additionally, it is recommended to take advantage of FP7 projects as a shortcut on terminology, threats and risks taxonomies, etc. Likewise, leveraging current experience on how operators are enhancing the cyber security posture in actual SCADAs is encouraged. To this respect, there was a call for having reference standards and for DSOs to team-up in real life – not only in European-level meetings such as this workshop – and share their knowledge, in order to come up to common procurement schemes that allow DSOs to pressure vendors and manufacturers so as to push them to implement security by design processes in products' development cycles.

During the discussion, some of the experts highlighted that Markets are envisioned to play a major role on the cyber security aspects of the smart grid. According to the experts, Markets are essential for the success of the smart grids since they will define the different use cases and in turn the smart grid concept as a whole. Security can be driven by standards but it will be driven for sure by the functions that need to be provided, which are defined by markets in the end.

With regards to the concept of security by design and end-to-end security in the smart grid, there were two different points of view. Some experts considered that security by design should be implemented in specific components considering an end-to-end approach. More precisely, experts stated that there is a need for a reference architecture on the whole smart grid on top of which security is defined globally, in an end-to-end way. On the other hand, there were other experts who suggested that, to secure the smart grid, the Internet should be considered as a model. According to these experts, in the Internet there is not an entity responsible for coordinating security yet it is indeed secure and resilient – at least those parts that need to be secure. For this purpose a decentralised strategy firmly based on the integration of the increasing number of actors would be very important and should be further encouraged. Likewise, according to this body of opinion, it will be necessary to identify and then focus on those aspects of the smart grids that really need to be – and can be – secured and start defining different "zones" with different requirements. The experts supporting this point of view stated that it would be very difficult – if not impossible – to follow a global end-to-end approach when securing smart grids. They declared that it would be more efficient to concentrate just on the important aspects. Besides, according to them, such a decentralised approach would not dismiss standards at all, but will be more efficient, since it is very difficult to define a standard that fits all aspects.

A debate on the sovereignty and responsibility of DSOs with respect to the security of smart grids, as well as the real necessity of reference standards also took place during the discussion. One of the experts considered that DSOs should be able to "do what they want" since safety and security are a cost they normally have to assume. This same expert considered necessary to reflect on who should be paying for safety and security, and on why smart grid agents should respect the standards presented by a European organism. On the other hand, another expert stated that, since DSOs and TSOs are in fact responsible for the safety and security of electricity transportation, they need to have standards that can be relevant for their procurements. In contrast to the argument defending the sovereignty of operators, other experts stated that even though DSOs and TSOs have economic responsibilities they also have national (e.g. a DSO might switch off a whole city if necessary) or cross-national responsibilities – the whole system depends on small inter-linked European companies –. For these reasons, questions such as "where does the responsibility lie?" or "what is the appropriate security level?" need further discussion. Actually, one of the experts explained that in the UK each company can take autonomous decisions on risks and security, but there are times when these decisions can also affect other organisations. This is the case of systemic risks for instance. According to another expert, nowadays it is possible that TSOs ask a DSO to switch a city off in order to prevent a black-out. However, in the future smart grid, where the Markets will play a major role, if electricity generation is only market driven and TSOs and DSOs could not influence anymore we can come to a situation where decisions are not optimal from a national security point of view.

Finally, experts agreed on the importance of having pilots to test cyber security issues, something which is not being done right now. According to an expert, pilots are necessary to bring down to earth all aspects around cyber security in smart grids. This expert stated that "as long as you don't come to something concrete you never know what you are really facing, if it makes sense or not, etc". A debate on what is understood for a pilot took place just afterwards. It was agreed that a pilot should have a test range, like a small town. Moreover, it was suggested that pilots could play an important role in demonstrating whether end-to-end security is feasible or not. According to the experts, nobody is moving because they don't want to be the first one and fear to make mistakes. To break this vicious circle, pilots on cyber security aspects were considered important so as to foster cyber security in the smart grids.

4.2 Certification, testing and pilots: How can we learn from each other?

The discussion addressed the certification of products and the organisation of security in the future smart grid. To this respect, there was a body of opinion highlighting that current use cases show that there is not yet a common view on the smart grid. Therefore, smart grids are considered too immature for security certifications. Nevertheless, certifications are considered an important topic to cope with future regulations. Moreover, it was pointed out that security certifications for products and organisations should be seen as a quality process that allows organisations and products to achieve a "label" that makes users confident about the product or the services.

It was interesting to see how many experts considered that certifications are important but not enough to guarantee that a system or organisation is secure. Establishing an Information Security Management System (ISMS) or a product certification scheme could result in the perception of a false level of security yet they are considered necessary aspects. A good number of experts also backed the idea of performing complementary testing activities. An expert suggested that certifications are not agile enough and cyber security evolves very quickly. Therefore, a more agile approach should be also fostered. For instance, these experts suggested that a third party testing body could perform quick tests for equipment checking for vulnerabilities and attacks that are revealed each day (i.e. something that certifications cannot deal with). According to an expert, such testing should not only be done in laboratories but also in real set-ups. These same experts agreed that both, certifications and agile tests are necessary.

Additionally, EO asked the audience about on-going national initiatives addressing and developing product and organisational certifications in the field of smart grids. There were two different answers here that signalled a FIPS-based approach in the UK for smart meters and a Common Criteria oriented Protection Profile definition for AMI in Germany. Surprisingly it was also mentioned that both initiatives are contradictory to some extent in the measures being defined. Therefore it was pointed out that there is a need for an EU-level certification process that harmonises everything.

EO also asked the audience about the current smart grid pilots and what can be learned from the cyber security perspective from these initiatives. Moreover, he was interested in knowing how we could make the knowledge coming from pilots available to everybody. However, the experts answering the call explained that unfortunately there were not security findings in pilots since current pilots do not cover security issues. In any case, a good number of experts supported the idea that pilots could show us how to mitigate part of the systemic risks of the smart grid and that dialog would be essential in sharing these findings. To this respect an expert also pointed out that it would be important to have a risk assessment methodology before initiating any activity related to testing security functionality in pilots. Such a tool would be really helpful in pilot testing of smart grid cyber security aspects. Besides, this expert stated that the output from the pilots will be very handy to define a minimum set of requirements for standards and a legal framework, including security certifications.

Deeping into the knowledge sharing aspects, several experts declared that there is already very valuable information that could be shared among DSOs and TSOs. For instance, an expert suggested that currently in Germany, DSOs and TSOs are also undertaking security assessments focused on current electricity networks. These results however could also be relevant from a smart grid perspective. In the same way, another expert explained that there are DSOs in Europe (e.g. Swissgrid, Alliander, ENEL, E.ON, etc.) which have performed pen-tests so far with a lot of interesting findings – in some cases even shocking ones. However, this expert also mentioned that these companies think that this is highly sensitive information and are not willing to disclose it to anybody. He suggested that a trusted environment to share the conclusions of these pen-tests and to speed-up learning should be established. As a piece of advice to convince DSOs and TSOs to share the results of such pen-tests, an expert suggested to only share a top ten vulnerabilities list, not disclosing the details (i.e. business impact, related incidents, etc.), and then find a common way on how to deal with them. Such a list could be updated each year. In addition to sharing vulnerabilities and common errors an expert suggested that a top-ten list of things that should be done (i.e. good practices) should also be discussed.

Backing up the idea of the importance of knowledge-sharing, some experts stressed out the fact that cyber security is a very dynamic topic and it is important to constantly monitor what is going on. For this reason, knowledge sharing initiatives looking for synergies with ENISA and other stakeholders should be defined. In relation to these synergies, EO explained that building EU-level information sharing initiatives is very difficult. These initiatives should happen at a MS level first and then this knowledge could be leveraged at an EU level. However, some of the experts agreed that national initiatives are important but argued that the European level is even more important. To this regard, experts stated that DSOs in small countries such as The Netherlands already know what is going on inside their own country. This expert explains that such companies consider they could learn more from other companies in Europe. Besides, another expert mentioned EuroSCSIE as a good example for such kind of initiatives at the EU level. According to these experts there is no need to have more than 4 - 5 DSOs for the sake of simplicity. They mentioned that there is no need to involve all 27 MS with all DSOs and all the legal aspects around. A different and more agile approach should be followed.

One of the experts of the audience suggested that knowledge sharing initiatives should also focus on leveraging the infrastructure provided by FP7 projects consortia, mentioning the Address project as an example where several DSOs (Iberdrola, ENEL, Vattenfall, etc.) are already working together. Besides, this same expert declared that it would be necessary to further foster the dissemination of the results of such kind of projects among the smart grid stakeholders, since value-added initiatives could be derived by utilities based on the best research done in Europe. Nevertheless, other experts highlighted that it could be difficult to achieve that the members of these projects share the results of their research. To this respect, a “vehicle” to share such sensitive information should be defined, that could be based on this idea of the top-ten list previously mentioned.

As a conclusion EO states that ENISA will organise a specialised workshop on certifications in the Smart Grid, to further discuss this interesting topic. Moreover, it will analyse off-line how to define a trusted information sharing scheme addressing the topics discussed during this session.

5 Morning Session B

Firstly, EO introduced the two topics of Session B, which were on the cyber security lifecycle and on minimum security measures. In the first case, the topic was oriented towards how smart grid providers could implement proper security policies and measures, while the second topic encouraged the experts to share their points of view on how to develop minimum security measures across Europe. During the discussion many relevant issues were highlighted that enrich recommendations 3, 4, 6, and 7 of the study.

5.1 Cyber security life cycle: How smart grids providers could implement proper security policies and measures?

EO introduced the topic and asked the audience on which security measures are being implemented already and what suggestions for improvement could be provided on this issue. Moreover, he also asked if the current security policies in place for smart grids appealed the audience.

However, the discussion was short and the only one expert sharing his point of view mentioned again that a distributed security approach should be further investigated. Additionally he pointed out that the same security measures will not fit in the same way for TSOs or for DERs. Therefore, he suggested that it is needed to take this into account when implementing security policies and measures.

5.2 Minimum security measures: How to develop them across the EU?

EO started the discussion by saying that in Europe there is a good number of security policies for telecommunications, and other sectors, but there is no single entity covering the security measures affecting smart grids. For this reason, he pointed out that being quick and agreeing on a number of minimum measures to be proposed by the EC, so as to push MS to consider them, might help addressing the harmonisation problem of security on smart grids. EO asked the audience about what should be the level of abstraction of these minimum measures.

There was a body of opinion supporting that before defining a minimum number of measures it is first needed to define the risk elements. Likewise, to define the list of risks it is important to perform a data collection effort, which in turns leads back again to the previous discussion on the willingness of the smart grid stakeholders to share their knowledge among each other. According to some of the experts, a small group of TSOs or DSOs should be defined in order to share that knowledge and identify the risks. One of the experts pointed out that, in such an initiative there would be two levels/circles that should be considered: the group of actors working together collecting/preparing the information/knowledge, and a second level above in charge of coordination. According to this expert, in order to maximize the chances of success both circles should be kept small. Moreover, this expert stated that if a very formal process is established the probability of success would be quite low.

Other experts suggested that DSOs and TSOs are more open to share knowledge than other stakeholder types. For instance, it was said that vendors, and particular meter vendors, will not be willing to share that information because of the high competence. However, it was suggested that they have to be involved in all those initiatives where DSOs and TSOs join to discuss cyber security issues of the smart grid.

During the meeting it was highlighted that a minimum set of security requirements could be defined for different stakeholders, since for instance DSOs and TSOs present commonalities. However, for this particular case it was also mentioned that there might be as many different ways of implementing a power grid as different utility companies are out there. Therefore, having reference architectures would also help very much.

On the other hand it was also highlighted that a minimum set of requirements sounds less than acceptable, and therefore efforts should focus not in defining a minimum set of requirements but those that provides an acceptable level of security. To this respect, EO considers relevant to also take into consideration the different maturity levels of the organisations. Moreover, he suggested that small operators cannot be dismissed when defining these requirements and it should be understood that such companies might not be able to cope with the same requirements that could be asked to large operators. Complementing this idea, another expert agreed that what is an acceptable minimum set of requirements for one company might not be enough for others. Therefore, different companies should have different requirements.

RL decided to bring up the topics of mandatory risk assessments and related methodologies, since these are much related to the initial discussion on the importance of identifying the risk elements before being able to define security measures.

One of the experts expressed his concerns on the mandatory risk assessments topic. According to this expert, in order to make risk assessments mandatory, a specific and defined approach should be established and typical company profiles should be defined. Furthermore, it was suggested that ENISA could play an important role here.

With regards to risk assessment methodologies for smart grids, an expert suggested that to identify risks assets threatened by these risks need to be identified first. Only then risks can be identified and a plan to manage these risks can be defined. Therefore in order to perform a risk assessment you also need to have the aforementioned reference architecture. As a reply, EO wondered what can be done if risks cannot be identified till the architecture is ready and security measures cannot be defined till the risks and architecture are defined, and suggested to explore the possibility to base on the smart grid pilots as a starting point. RL also stated that once there is a reference European architecture formal risk assessments could be started. However, he suggested that, in the meantime, following the distributed approach suggested in the previous discussion sessions could also be fruitful. To this respect, it is interesting to highlight the suggestion of another expert which considers that business impact analyses should be undertaken instead of risk assessments. In this way, he declared that a minimum set of requirements could be defined independently of the implementation details which are necessary for formal risk assessments.

The discussion also addressed the necessity of building a new risk assessment methodology for smart grids. The experts acknowledged that there are multiple risk analysis methodologies that could be leveraged. Moreover, EO backed up this idea by stating that there are many general risk assessments methodologies. According to him, building a new risk assessment methodology from scratch is not the best approach. He considers that it would be much more valuable to leverage the results of those power grid companies that have probably perform risk assessments already on smart grid issues. EO suggested that ENISA could gather this knowledge, compile it and share it with other members.

During this session it was also discussed how the work being carried out several expert groups (i.e. SGIS, DG INFSO's Ad-hoc EG) could be leveraged. A representative from the SGIS explained that this group is already addressing the topics discussed before. He further explained that they are taking stock of the use cases, and based on them they are defining the security architecture model. Besides, he explained that based on this model zones and layers are defined. These zones and layers would allow establishing a minimum number of security measures. Likewise, a representative from the DG INFSO's Ad-ho EG explained that the group is focusing on analysing threats, risks, security measures and other relevant topics. Another representative declared that this group has defined a risk classification criteria based on voltage levels and other factors. However, this expert and another one also considered that a further discussion on who should establish the classification criteria is needed, since it is not easy to decide that grids or plants delivering or generating over a certain voltage capacity need to be well protected since or the other way around.

Before ending the discussion on the security requirements, some experts highlighted the importance of considering cyber war and cyber crime as another dimension when addressing the security issue of the smart grids. It should be clarified if TSOs are supposed to protect themselves against cyber war or cyber crime incidents since national boundaries do not exist anymore: an attack to one TSO can impact other TSOs in other countries in Europe.

RL and EO decided to further discuss recommendation 6 of the study which suggested fostering the creation of test beds and security assessments. However, some of the attendees brought attention on the importance of CSIRTs. One of the experts stated that ENISA could study what could be role of CSIRTs in smart grid security. EO answered that ENISA could foster the creation of an ICS-CSIRT or other types of CSIRTS. Likewise, ENISA could also promote the extension of current national contingency plans and associated exercises, which now target the telecommunications sector, to the smart grid arena. To this respect, one of the experts said that the smart grid would not be a national level issue and that an EU-wide level of action is very necessary. Finally the discussion was brought back to the test beds issue proposed by recommendation 6 of the study. Some experts agreed that an important aspect of such test beds would be to decide who should pay for them and if they should be established at a MS basis or at the European level. EO declared that the EU is funding to some extent to those companies that are sending out people to the INL[2] in the US to learn about these topics. On the other hand, another expert stated that DSOs and TSOs have a responsibility on making the grid secure, and explained that in the Netherlands they are organising test beds which are costing tens of millions of Euros. Besides he mentioned the European Network for Cyber Security (ENCS) as a reference on how to organise these aspects. According to this expert there should be different test beds around Europe each one addressing different but complementary aspects.

[2] *INL stands for the Idaho National Laboratory, which is a national laboratory supporting the US Department of Energy and which, among other things, has been performing cutting-edge research, conducting vulnerability assessments and developing innovative technology with regards to the increasing the resiliency of the electric grid, improving control systems cyber security posture, etc.*

6 Test and learning platform for ICS and Smart Grids

Bram Reinders (BR) was invited to introduce to the audience the European Network for Cyber Security (ENCS). The ENCS is a non-profit European Public Private Partnership on cyber security for critical infrastructures with an initial focus on smart grids and process control, and which will be extended to other critical infrastructures in the future.

BR explained that in January 2012 the Dutch National Security Centre was set. It was quickly acknowledged that cyber security in Critical Infrastructures is not limited to the border of each MS. Therefore it was considered necessary to work together with other countries in Europe. These tasks were out of the scope of the National Security Centre and it was decided to create a new initiative, the ENCS (formerly called CyberTECH).

The mission of ENCS is being the partner for securing critical European infrastructures. ENCS's main purpose is to decrease the risk levels for smart grids and process automation infrastructures in the public-private domain. ENCS proposes four lines of business:

- R&D: including facilities for innovation, simulation and demonstration.
- Test bed: oriented to product testing and evaluation.
- World class education and training (including DHS/INL in the US): red and blue team training; education of top management (C-level), process engineers, (risk) managers, (information) security professionals.
- Information and knowledge sharing: by means of public-private partnerships, national and international coordination and cross sector open innovation.

As it was mentioned earlier, this initiative also intends to include other sector apart from Energy. These are:

- Water supply
- Chemicals and oils
- Food
- Telecom/ICT
- Financials
- Transport
- Defence
- Governments
- Others

The ENCS, which is organised as PPP initiative, is more private than public since most of the funding is from private organisations and over a 60% of the organisations come from the private sector. The collaboration in such kind of PPPs is similar to the way in which companies collaborate in European FP7 projects. Moreover, the ENCS does not aim to compete with other organisations. It strives for a coordinating and organizing role on the European level. Moreover, different national and European initiatives should be complementary and be executed accordingly, establishing collaboration agreements. To this respect, BR mentions Italy's laboratory for testing SCADA equipment. Furthermore, the ENCS looks for alliances within the EU and outside the EU (e.g. US, Israel, etc.) and for pushing/pulling scientific, governmental and industrial expertise and experience. The ENCS bridges the gap between cyber-security related closed communities (e.g. government intelligence agencies and the CSIRT-community) and the society (industry, academia, consumers). For instance, in the research area, the ENCS has been able to organise in one month time a network of excellence under the FP7, which includes the universities of Bristol and Darmstadt, EDP from Portugal, Alliander, Elster, etc. To this respect, the ENCS has a business plan that includes 15 different research topics, many of them related to technology. They look for very practical aspects and for paradigm shifts. On the other hand, in the area of product testing, Alliander can take advantage of the ENCS to analyse, in a real deployment, new equipment provided by suppliers. The ENCS could also leverage existing initiatives, such as EuroSCSIE, Meridian and even well-established CSIRTs for information and knowledge sharing activities. Moreover, he also declared that education and training lines of action could be enriched with the findings from the test bed. In fact, all four areas are tightly related one to another.

BR explained to the audience that a quantitative analysis was undertaken which provided detailed information about the potential market for the ENCS in the area of cyber security in the smart grid and process control domain. What follows is the list of figures presented during the meeting:

- ENCS EU Total Addressable Market (TAM) is some €95.5M in 2011.
- Most of investments are currently directed to R&D, which represents some 74% of current spending in ENCS TAM.
- By 2016, IDC EI expects the ENCS TAM to reach €389.7M in the EU, following strong growth rates in all areas.
- By then, R&D will still represent the largest share of the ENCS TAM, but its share will have decreased from 74% to 65%.
- Following very strong growth, testing services will move from €6.5M to more than €80M in 2016. By then, they will represent nearly 10% of the ENCS addressable market.
- Training & education will show less impressive, but still strong growth rates, to reach a size of €56.3M in 2016 (€18.1M in 2011).

The types of membership were also explained. These include:

- Owners and operators of CIs, starting with electricity and telecommunication infrastructures owners. Banking will also be included in the future.
- Manufacturers/Suppliers: service providers like vendors, advisory, etc.
- Associate Members: most likely small & medium enterprises
- Academic members: most likely research institutes
- Governments: agencies, NGO’s, etc.

Finally, a number of other activities and topics that could be leveraged or promoted by the ENCS as well as a number of positive consequences for the industry were listed. These are:

- Desirably, operators will not installed equipment which has not been tested in some years’ time

- Managed security monitoring would be very an interesting topic of research
- Research on signature-based and anomaly-based detection schemes
- Privacy discussion could be enriched with the results of ENCS
- The risk model being developed by DG INFSO's Ad-hoc group could be further leveraged by ENCS by putting it into practice and giving feedback to improve it

After the presentation, a member from the audience asked if there are already on-going real projects under the umbrella of the ENCS. BR answered that they are currently addressing an end-to-end security assessment for smart meters. Additionally, another expert suggested that in an initiative such as ENCS, manufacturers pay for the testing, DSOs provide the infrastructure and third companies can be in charge of the testing activities and other related issues.

7 Afternoon Session C

Session C was organised as a panel session where seven different panellist discussed on two different topics. The topics were:

- National cyber security strategies for smart grids: the role of member states in enhancing cyber security of smart grids
- Towards an EU wide cyber security strategy for smart grids: how all smart grids cyber security initiatives make sense for member states and EU

These panellists included representatives from public bodies in the EU and in the US, smart grid and process automation manufacturers, and TSOs. The names and organisations of the panellists are:

- Vizenzo Giordano (VG), Institute for Energy and Transportation in the JRC EC
- Jay Holcomb (JH), US NIST
- Andrea Servida (AS), DG INFSO
- Michael Munzert (MM), Siemens Energy Automation
- Himanshu Kurana (HK), Honeywell
- Bart de Weijs (BW), ABB
- Eric Luijf (EL), TNO

What follows is an overview of the basic matters exposed during the individual dissertations of the panellists as well as of the main discussions that took place afterwards with the audience.

7.1 National cyber security strategies for smart grids: The role of Member States in enhancing cyber security of smart grids

With respect to the national cyber security strategies for smart grids and in particular with the specific lines of action to be followed, one of the recommendations was to define a knowledge sharing trust model that allows information and knowledge sharing among all stakeholders. According to the panellists cyber security will not probably be used as a "business weapon" and sharing information is key to be ready for addressing new vulnerabilities, threats and to improve resilience of the smart grids.

Another important issue to consider is that industry needs to step forward and provide input to improve cyber security in the smart grid environment. Long product life-cycles are a challenge that the industry will have to deal with. To accomplish this, regulators should build the framework conditions to enable industry to be more competitive and public bodies need to provide incentives and to define the applicable legislation. Besides it is also necessary to foster the cooperation between Europe and USA.

During the discussion, one of the experts highlighted that the European Commission can assume the role of compiling the initiatives and projects on the field. Additionally, he noted that cyber security was not considered important or, at least, details were not revealed in the pilots analysed and compiled by the JRC. Some of experts highlighted that cyber security is seen as burden in pilots for testing other functionalities that are considered more important. Nevertheless, one of the panellists pointed out that the VIKING project has provided very interesting results on cyber security, such as the fact that the way in which communications are routed can really improve the resilience. Once again, it is mentioned that it is necessary to share results of this kind.

Concerning to the role of manufacturers, several experts noted that operators should ask them to include cyber security measures. One of the panellists explained that nowadays this is not common practice but it is envisioned that it will occur more frequently in the mid-term, either as requesting compliance with the ISA99 as a whole or more detailed ones. To this regard, the US panellist highlighted that in USA there is a clear regulation, the NERC-CIP, which reinforces this kind of behaviours. Additionally, other experts highlighted that there are MS where the largest customers clearly define security requirements and they discuss these requirements (E.g. Swissgrid) with the vendors. Related to this, another expert considered that NER-CIP is a very good starting point, but at the same time it does not meet all the necessary aspects of an end-to-end security model. Furthermore, one of experts pointed out that there is a lack of a security culture in operators. As a result, they might ask for products that allow complying with ISO 27000 as a whole instead of defining more specific requirements based on more appropriate standards.

Regarding patch management, one of the experts declared that it is very important that vendors are addressing the patch management already moving towards an IT-based model. Another expert highlighted that patch management is not an easy task since there is not a culture of patching in vendors and operators. It is necessary to carry out a process of awareness in this sense.

Finally, in terms of structured attacks it was mentioned that the DHS is already providing best practices documents to improve the security posture of the organizations (for example trough risk assessment models). Besides, NIST SP 800-53 rev. 4 already includes an updated version on how to deal with ICS security.

7.2 Towards and EU wide cyber security strategy for smart grids: How all smart grids cyber security initiatives make sense for Member States and the EU?

Most of the experts agreed that a unified approach on cyber security for smart grids is necessary in Europe, where a clear and common set of requirements and policies valid for all MS need to be defined. Besides, according to the experts, there are many different organisations involved in smart grid aspects, both at each MS and at the European level that need a more integrated and coordinated approach of the cyber security domain. Moreover, it is also emphasised that it is necessary to extend the security needs to the consumers side (EV, HAN, IAN, BAN, etc.), because they are also part of the common set of problems, requirements and frameworks of the smart grid.

Regarding security requirements, most of experts agreed that there will probably be different security requirements depending on the domain they are being intended to. However, there should also be a common approach, and this common part should be as large as possible and will probably be defined with a high level of abstraction, while low level security requirements will probably have to be different depending on the specific domain. One of the experts suggested inviting the manufacturers to come up with the minimum common standards on security requirements, and all of them accepted the challenge.

Another expert mentioned that the JRC is building a smart grid laboratory which is intended to be open to everybody around Europe and will help reduce the gap between IT and industrial fields. He considered that this lab could be an answer to the test bed aspects, whereby to analyse vulnerabilities and threat scenarios. To this respect, JH noted that it would be important to address patch management with vendors. He mentioned the US ICS-CERT as an example and stated that they work with vendors on vulnerabilities on different levels: applications, OS, etc.

Finally, it was suggested that the collaboration between the US and EU should be continued by leveraging the EU-US partnership. Besides, experts recommended that ENISA could support the process for standardising security requirements as well as analyze how to bring together all testing laboratories in Europe.

8 Wrap up and future directions

Before closing the workshop, EO and AP summarised the future actions that will be undertaken based on the suggestions and conclusions of the meeting. These include:

- The report of the ENISA study on smart grid security will be available by the end of March or the beginning of April.
- A new study from ENISA on smart grid security is on their way.
- ENISA in cooperation with the Commission will involve the UK and Germany and prepare a monographic workshop on smart grid cyber security certification.
- ENISA acknowledges that information sharing is very relevant. Therefore ENISA will start off-line actions leveraging existing initiatives such as ENCS or EuroSCSIE and involving some experts to analyse the available opportunities and strategies.
- ENISA will support the initiative by which a number of leading vendors will "sit on the table" with operators to discuss on how to define the baseline/minimum cyber security requirements for smart grids.
- The EC will take the information coming from this workshop together with DG INFSO's Ad-hoc expert group results and guarantee that it cross-fertilizes other ongoing initiatives so as to hack up political actions.

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