Smart Grid Security

Recommendations for Europe and Member States

[Deliverable – 2012-07-01]

Contributors to this report

ENISA would like to recognise the contribution of the S21sec[1] team members that prepared this report in collaboration with and on behalf of ENISA:

- Elyoenai Egozcue,
- Daniel Herreras Rodríguez,
- Jairo Alonso Ortiz,
- Victor Fidalgo Villar,
- Luis Tarrafeta.

Agreements or Acknowledgements

ENISA would like to acknowledge the contribution of Mr. Wouter Vlegels and Mr. Rafał Leszczyna to this study.

[1] *S21sec, the contractor of ENISA for this study is an international security services company with offices in several countries.*

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 Security: Recommendations for Europe and Member States'', please use the following details:

- E-mail: Konstantinos.Moulinos@enisa.europa.eu

Annexes

1 Executive Summary

The smart grid can be defined as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added (1). Smart grids will be able to efficiently integrate the behaviour and actions of all users connected to them — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety (2).

Information and Communication Technologies (ICT) are envisioned to be the underpinning platform of smart grids, which exemplifies the increasing dependency of the European economy and society on communication networks and computer applications. Smart grids give clear advantages and benefits to the whole society, but their dependency on computer networks and applications, as well as on the Internet, makes our society more vulnerable to malicious cyber attacks with potentially devastating results.

Recognising the importance of the problem, ENISA launched a series of activities, which include the present study, aiming at bringing together the relevant stakeholders and engaging them in an open discussion on smart grid cyber security. The principal goal of the open dialogue is to identify the main concerns regarding the security of smart grids as well as to recognize and support national, pan-European and international initiatives on smart grid security.

This study makes 10 recommendations to the public and private sector involved in the definition and implementation of smart grids. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, raising awareness, developing new measures and good practices, and reducing barriers to information sharing. This guidance is based on the results of a thorough analysis of the opinions of the experts who participated in the study. Furthermore, important information coming from in-depth desktop research is also taken into consideration. All this data has been analysed and has provided almost 100 Key Findings.

The top ones are:

Recommendation 1. The European Commission (EC) and the Member States' (MS) competent authorities should undertake initiatives to improve the regulatory and policy framework on smart grid cyber security at national and EU level.

Recommendation 2. The EC in cooperation with ENISA and the MS should promote the creation of a Public-Private Partnership (PPP) to coordinate smart grid cyber security initiatives.

Recommendation 3. ENISA and the EC should foster awareness raising and training initiatives.

Recommendation 4. The EC and the MS in cooperation with ENISA should foster dissemination and knowledge sharing initiatives.

Recommendation 5: The EC, in collaboration with ENISA and the MS and the private sector, should develop a minimum set of security measures based on existing standards and guidelines.

Recommendation 6. Both the EC and the MS competent authorities should promote the development of security certification schemes for components, products and organisational security.

Recommendation 7. The EC and MS competent authorities should foster the creation of test beds and security assessments.

Recommendation 8: The EC and the MS, in cooperation with ENISA, should further study and refine strategies to coordinate measures countering large scale pan-European cyber incidents affecting power grids.

Recommendation 9: The MS competent authorities in cooperation with CERTs should initiate activities in order to involve CERTs to play an advisory role in dealing with cyber security issues affecting power grids.

Recommendation 10. EC and the MS competent authorities in cooperation with the Academia and the R&D sector should foster research in smart grid cyber security, leveraging existing research programmes.

A full list of recommendations can be found on page 27.

2 Introduction

The adoption of smart grids will dramatically change the grid as we know it today, and traditional energy services and markets will undergo a significant transformation. In addition to bulk generation facilities the smart grid will intelligently integrate distributed or dispersed generation, where many energy sources of small size (i.e. the so called Distributed Energy Resources, DER) will be dispersed along the transmission, distribution and customer domains. Some examples of distributed energy resources include solar panels, small wind turbines, fuel cells, and distributed cogeneration sources, and even the Electric Vehicle (EV) itself.

The smart grid will also result in smarter networks, both in the transmission and distribution domains. It will bring a whole range of new specific applications and technologies to improve the transmission system, and will complement existing technologies such SCADA/EMS and current substation automation. Besides, the smart grid places new requirements on the automation, monitoring control and protection of distribution substations and transformer stations/centres. Advanced Distribution Automation (ADA) technologies and applications as well as Advanced Metering Infrastructures (AMI) will provide the necessary intelligence to this section of the power grid to cope with the new requirements.

It is clear that smart grids will substantially improve control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators. Nevertheless, improved operations and services will come at the cost of exposing the entire electricity network to new challenges, in particular in the field of security of communication networks and information systems.

Thanks to ICT, the grid of the future will become smarter so as to improve the reliability, security, and efficiency of the electric system through information exchange, distributed generation, storage sources, and the active participation of the end consumer. However, vulnerabilities of communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants. This was demonstrated for instance in 2009, when officials from the US public administration recognised that cyber spies from China and Russia had hacked into the US electricity grid and hidden software that could be used to disrupt power supplies (3).

2.1 Cyber security aspects of smart grids

A smart grid is an upgraded electricity network depending on two-way digital communications between supplier and consumer that in turn give support to intelligent metering and monitoring systems. Information and communication technologies have become the underpinning platform for the grid of the future but at the same time they are also its Achilles heel.

The communication infrastructures are not the only source of vulnerabilities. Software and hardware used for building the smart grid infrastructure are at risk of being tampered with even before they are linked together. Rogue code, including the so-called logic bombs which

cause sudden malfunctions, can be inserted into software while it is being developed. As for hardware, remotely operated “kill switches” and hidden “backdoors” can be written into the computer chips used by the smart grid and allowing outside actors to manipulate the systems. The risk of compromise in the manufacturing process is very real and is perhaps the least understood threat. Tampering is almost impossible to detect and even harder to eradicate.

Achieving a secure smart grid will not be an easy task. As it is exemplified in the previous paragraph, there is a series of unknown or not well understood potential vulnerabilities and weaknesses that must be further analysed. Besides, there are also well understood problems that need complex solutions. This is the case of security issues concerning the data protection of end-consumers information. To this regard, the development of legal and regulatory regimes that respect consumer privacy, promote consumer access to and choice regarding third-party use of their energy data is a sine qua non for broad acceptance of smart grids.

Assessing risks, securing processes as well as identifying technological gaps and organizational problems are some of the main challenges that the smart grid will face in the years to come. Raising awareness and fostering training and knowledge sharing among all the actors are urgent measures needed to set the breeding ground for bringing security to the first line of action.

2.2 The policy context

Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) related directives and communications have already established a general regulatory framework for the protection of the critical infrastructures of the power (smart) grid.

In December 2006 the COM(2006) 786 (4) “on a European Programme for Critical Infrastructure Protection” fixed the main aspects of a European Programme for Critical Infrastructures Protection (EPCIP). This communication recognized the threat from terrorism as a priority even though the protection of critical infrastructure would be based on an all-hazards approach. This Communication also defined the main guiding principles of the EPCIP and identified the necessity for creating an EU framework concerning the protection of critical infrastructures. Likewise, of particular interest is the Council Directive 2008/114 on CIP (5), which considers electricity generation and transmission (in respect of supply electricity) infrastructures and facilities as candidates for being identified as European Critical Infrastructures.

In 2009, the Commission adopted COM(2009) 149 (6) on Critical Information Infrastructure Protection. This Communication recognizes that ICT infrastructures are the underpinning platform of other CIs and defines a plan of immediate actions to strengthen the security and resilience of Critical Information Infrastructures (CIIs) based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for EC infrastructures in the field of ICT. In 2011, another Communication from the Commission, COM(2011) 163 (7), summarised the achievements of this plan and defined next steps to be taken. It also recognized that new threats have emerged, mentioning Stuxnet as

an example. Besides, this, the Communication specifically mentions that smart grids can be affected by sophisticated and targeted cyber threats, with the purpose of disruption.

Data protection and data privact issues are also engaged, with the most vigorous declaration on their importance , together with that of cyber security and infrastructures resiliency, coming from specific energy-related policy documents. This is the case in COM(2011) 202 (1), "Smart Grids: from innovation to deployment", where the Commission identifies challenges on smart grid deployment and proposes to focus on, among other things, developing technical standards, ensuring data protection, and providing continued support to innovation for technology and systems. Moreover it communicates the creation of a group of high-level stakeholders to assess the network and information security and resilience of smart grids as well as to support related international cooperation.

2.3 The aim of the study

This study aims at identifying risks and challenges related to cyber security aspects of smart grids. Besides, this study also takes stock of national and European initiatives on standardisation, knowledge sharing, certification, training, pilots, and other activities addressing cyber security in the smart grids. Pilot projects in Europe were studied in order to identify the cyber security controls being deployed. Additionally, the study investigates the importance of Information and Communication Technologies (ICTs) as the underpinning platform of the future grid, and investigates related threats and risks. Based on a thorough analysis, the study proposes good practices and recommendations for all relevant stakeholders that will help them improve the security, reliability and resilience of future smart grid deployments. Moreover, the study aims at helping the involved stakeholders in recognising the importance of security issues, engaging in international cooperation, raising awareness inside their organisations, and supporting standards. Finally, the recommendations resulting from the study will also allow ENISA to pave the way for future actions and studies on smart grids.

2.4 Scope of the study

The two pillars of this study are:

- Identifying the current state of smart grid security based on the concrete, comprehensive, and up to date 'inventory' of factual knowledge coming from the field.
- Obtaining opinions on the subject from all the relevant stakeholders.

Based on these pillars the recommendations for the stakeholders are derived. Work on the factual description of the current situation has focused on the following aspects:

- Review on the definitions of the smart grid
- High level objectives of the smart grid
- Drivers for the adoption of the smart grids in Europe, the US, and other regions

- Quick overview on standardisation efforts on the smart grid architecture
- Physical infrastructure of the smart grid and high-level application and services
- The importance of ICT technology in the smart grid
- Review on real incidents and relevant discoveries on flaws affecting the smart grid
- Cyber security risks, threats and challenges
- Summary of the current European security policy context
- European initiatives addressing cyber security in the smart grid
- Review of the most significant standards, guidelines, regulatory documents as well as active groups and initiatives on smart grid cyber security

Most of the content is based on highly reputable sources of information, such as official good practices, technical reports and standards of organizations such as CEN/CENELEC/ETSI SGCG, NIST, Smart Grid Task Force, ANSI/ISA, IEC, ISO, and others. However, it is also enriched by the contribution of several experts in the topic. These experts have contributed to this part of the study, by providing their knowledge in existing initiatives, known good practices, standards and policies, as well as other topics already addressed.

The second basic pillar of the study, obtaining the opinion on the subject of all relevant stakeholders (grid operators, manufacturers, policy makers, academia, etc.), is actually the crucial part of the study. The relevant representatives of the public and the private sector have been engaged (by means of a survey and personal interviews) to provide their opinion on critical aspects of smart grid security, as for instance current public-private partnerships, information sharing platforms, test beds, and other initiatives; the challenges, barriers and obstacles for smart grid protection; ways to improve the adoption of security good practices and standards; the current policy context; economic strategies and incentives, etc.

This study identifies common points and differences among stakeholders' replies and contributions to propose recommendations for these same stakeholders. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing.

2.5 Approach

The study comprised two main phases. The first phase,“stocktaking”, was intended to gather all the data that will make up the work base for the study. The second phase was based on the analysis of the data in order to develop recommendations for the different types of stakeholders involved with cyber security aspects of the smart grid.

The activities carried out during the first phase of the study included the so called ‘desktop research’, which means the analysis of all available documents relevant to the topic of the study. In this part we made use of recognised existing documents (guidelines,

recommendations, reports, etc.) coming from organisations, companies, consortiums or research centres, as well as the most influential books in the field, and the latest news (for this we have for example subscribed to forums, discussion groups, news feeds, etc.).

The second crucial part of the stocktaking was the survey and interviews with the smart grid experts aimed at obtaining their opinion on the most important smart grid security subjects. Besides, in this part some of the authors of this report actively participated in initiatives such as DG CONNECT's ad-hoc EG, or even contacted the visible head of the most relevant smart grid pilots, so as to ask for further information about the impact of cyber security.

Questionnaires included the 11 topics listed above which in turn were further divided into a total number of 27 different questions or concepts. At the same time, those experts who answered the questionnaire and accepted being interviewed were not only asked on these new concepts but also were proposed to personally discuss on the 'key messages' they shared with us in the answers to the questionnaires. The information provided by the experts was classified according to the main background of the expert. For instance, if one expert worked for a DSO but majorly in R&D aspects it was classified as an expert belonging to the Academia/R&D category. The categories defined are the following:

- Manufacturers and integrators
- Security tools and services providers
- Distribution System Operation (DSO)
- Transmission System Operation (TSO)
- Power generation
- Smart Grid services provider (e.g. marketer)
- Academia and R&D
- Public bodies
- Standardisation bodies

It is worth mentioning that over 304 experts were contacted for the study of which 50 participated in the poll. Additionally we were able to carry 23 personal interviews.

The second phase of the study was based on the qualitative analysis of the findings and the development of recommendations for different categories of stakeholders. As a result of the first stage of the study we had built up a large data source which comprised diverse information. We consolidated and normalized this data into a structured set of information that can be easily and thoroughly processed. The basic element of it is a "key finding", which is a relevant and influential observation from the desktop research, the survey and/or the

interviews. Key findings may show an emerging issue, an initiative taken or believed to be taken, an agreement/disagreement level between stakeholders, values or tendencies in the answers, a relevant line of opinion or any other piece of elaborated information that might have any impact in the field of smart grid security. Key findings are finally combined in order to ultimately derive the recommendations presented in this study.

On 29th February 2012, ENISA organised a workshop where the results of the study 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 dialogue among the attendees was also planned. This dialogue allowed ENISA to gauge the particiapnts' impressions of the recommendations and gather different opinions on how to improve them.

2.6 Target Audience

This report constitutes a source of the most recent information on the topic of smart grid security in Europe. It might be useful to anyone involved in the definition of the grid of the future or interested in obtaining a detailed and broad overview on what are the main issues in relation to the security of the current and future power grids.

One part of this report is devoted to introducing the basic concepts of the smart grid, from its very basic definition, objectives and similarities and differences among countries, to a more technically advanced description on the new infrastructures and applications supporting it. Another important chapter of this report is devoted to providing an up-to-date factual description of the current security panorama of today's power grids and the smart grid in general, including existing initiatives, standards, guidelines, and regulatory documentation, current security challenges and emerging issues. These two parts of the report are presented mostly in a high-level language but sometimes a more technical vocabulary is used. For this reason, it is assumed that the readers have some security and electrical background knowledge. This section is intended for:

- Engineers
- Researchers
- Information security specialists
- Security consultants
- Managers
- Business leaders

In addition, the core sections of this document contain a number of key findings and recommendations regarding smart grid security, resulting from the analysis of the opinions of multiple experts in the field and a desktop research. These key findings and recommendations

are written in a non-technical language suitable especially for decision-makers. The key findings describe possible future strategies, devise new initiatives, and propose new research activities with the aim of building a secure smart grid at different action levels: political, organizational, technical, awareness raising, economical, etc. For this reason, this part of the report is more appropriate for:

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

2.7 About the report

This report is divided into nine main chapters: Executive Summary, Introduction, Purpose and Scope of the Study, Target Audience, Approach, Key Findings, Recommendations, and Conclusions. Additionally, there are 5 annexes which contain the detailed information on the results of the study. They include the detailed output of the desktop research and the analysis of the raw data coming from the experts. Additionally, another annex is devoted to the study validation workshop.

- Annex I and Annex II present the main results of the desktop research phase. Annex I provides a detailed introduction to smart grid concepts, and Annex II gives an overview of the security issues related to the smart grid.
- Annex III provides a detailed analysis of the data gathered from the interviews and the survey in which experts participated.
- Annex IV is a compilation of current security guidelines, standards and regulatory documents on power grid and smart grid cyber security.
- Annex V includes a complete list of initiatives related with smart grid security as well as a detailed analysis of those pilots that are addressing smart grid cyber security.

3 Key Findings

In this chapter we present the key findings discovered during the desktop research and the analysis of the results of the survey and interviews. The key findings have been grouped into various thematic categories, starting with what we consider the biggest challenges in smart grid security, and continuing with a multiplicity of topics on smart grid security, including:

- The biggest challenges of the smart grid
- Basic components of the smart grid
- Smart grid pilots and cyber security
- Risk assessments in smart grid
- Certifications and the role of NCAs
- Basic aspects for a secure smart grid
- Smart grid cyber security challenges
- Current smart grid initiatives on cyber security
- Measuring cyber security in the smart grid
- Managing cyber attacks
- Research topics in smart grid security
- The smart grid business case
- Recommendations for Protecting Industrial Control Systems (ENISA report)

3.1 The biggest challenges in smart grid security

3.1.1 Factors of success

There are several factors which are considered of key importance to guarantee the success of the smart grid: a) A common definition of the smart grid concept; b) Cost reduction and fraud prevention; c) Cyber-security of the grid; d) Guaranteeing privacy of consumers; e) Consumer acceptance via awareness rising and education; f) Smart meter acceptance/roll-out.

3.1.2 Lack of a standard reference architecture for the Smart Grid

Standardization bodies recognise that there is not a clear standard describing the architecture of the future smart grid in Europe. The lack of a standard architecture spans all the different

domains (e.g. generation, distribution, etc.). Additionally some experts expressed their concern because some working groups can not further develop their activities due to this lack of definition. It is agreed that consensus-based reference architecture is necessary.

3.1.3 End-to-end security approach based on a standard architecture

Smart grid companies along the value chain are getting more and more interconnected and interdependent. Therefore, experts referred to the necessity of an end-to-end security approach at all levels of communication, from the lowest levels (meters, physical, etc.) to the upper ones (application systems, integration with corporate systems, value-added services, etc.) and all along the smart grid value chain. They consider that having a standard architecture of the smart grid is on the basis of such a strategy.

3.1.4 Cyber security, not at the front-line of action

A slight majority of experts think that not enough attention is being paid in Europe to cyber security and data privacy, as it is exemplified by current smart grid pilots. According to some experts there is a generalized perception that cyber security is not at the front-line of the smart grid priorities. Several experts stated that prior to security and privacy, primary concepts of the smart grid (i.e. business models, objectives, functionalities, services, etc.) need to be well addressed.

3.1.5 Cyber security and privacy as two different matters

Customer acceptance is considered a key success factor for the smart grid. To that aim, privacy is considered more important than cyber security, mainly in smart meter related applications. This is the reason why privacy and cyber security are being addressed separately, while many experts consider they are intimately related.

3.1.6 Security by design

Experts consider that cyber security and privacy are not being addressed appropriately since in many cases it has been considered as an overlay more than a very integral part of the design phase. These experts consider that cyber security and privacy should be addressed at the design phase so as to minimize costs and maximize security. This will become more important in the near-term with the ever increasing sophistication of industrial equipment.

3.1.7 New cyber risks

The integration of the end user property (e.g. demand-response and home-based energy sources), as part of the smart grid, widely extends the attack surface area, bringing new risks for electricity delivery. Since it is not possible to control what is going on inside the end-customer houses it should be considered as a high-risk area. Additionally, a more intensive use of the Internet and other public networks in the smart grid (e.g. DER connection, and value-added services for end customers) will also bring new risks to power infrastructures.

3.2 Basic components of the smart grid

3.2.1 Horizontal view of the smart grid

For the majority of experts, the smart grid should span the complete value chain of electricity delivery, from electricity production in the power plants to its consumption by final clients, including trading, transmission, distribution, marketing (industrial and residential), etc.

3.2.2 Vertical view of the smart grid

There are some experts who consider that the smart grid is everything that is related with the grid operations and the supporting communication infrastructure, and therefore it should be separated from added-value services built upon them. On the other hand, some experts consider that the smart grid concept includes all aspects, from devices, technologies and infrastructures to operations (e.g. grid management or market operation) and services (e.g. demand-side management).

3.2.3 Bi-directionality feature of the smart grid

Bi-directionality should be considered in two different ways. On one hand it means that the grid should be able to make use of any distributed generation resources. On the other hand, the Smart Grid should be based on a supporting ICT infrastructure based on bidirectional communications.

3.2.4 Smart-home and smart-industry as part of the smart grid

There is no clear agreement among experts when it comes to clarify whether Advanced Metering Infrastructure (AMI), smart homes and smart industry are part or not of the smart grid concept. DSOs for instance consider that what is inside the house (e.g. household automation, smart appliances, home energy management, etc.) is outside the scope of the DSO – with the frontier between the grid and the household at the smart meter or the home gateway. However, other experts consider that the smart grid should include also the smart home and the smart industry.

3.2.5 New applications and services

Smart grid services and applications can be classified into three domains: 1) AMI-based applications/services (e.g. demand-side management, home-energy management); 2) distributed generation management (i.e. DER management); 3) and advanced distribution/transmission automation (e.g. substation automation, storage management, advanced distribution applications, islanding, etc.). Additionally, it is considered that macro-generation (i.e. bulk generation) will also be affected by the smart grid.

3.3 Smart grid pilots and cyber security

3.3.1 Lack of a global perspective on European smart grid pilots

Even though a majority of experts confirmed the knowledge of various pilots related to different domains of the smart grids, there is a lack of global perspective. The result is that each expert only knows in detail those projects related to the topics of their interest. However, the publication from the JRC "Smart Grid Projects In Europe: lessons learned and current developments" (8) has contributed to increase awareness on pilots among the community.

3.3.2 Cyber security, a second-line issue in smart grid pilots

In general terms, pilots are not considering cyber security at all (with very few exceptions). According to the experts many of the projects are at an early stage. For this the reason pilots are focusing on testing smart grid applications and functionalities, which are considered essential, leaving out cyber security measures.According to the experts, cyber security and privacy are only taken into account seriously once they start massive deployments, as it is happening already in the smart meters roll-out.

3.4 Risk assessments in smart grids

3.4.1 Challenges, goals and needs for protecting national energy infrastructures

Experts consider that, in order to determine the cyber security challenges, goals and needs for the protection of national energy infrastructures, public bodies should follow a risk-driven approach. Additionally, it should be considered that priorities on risks and threat levels might be different across Member States.

3.4.2 Mandatory risk assessments to be conducted by TSOs and DSOs

Several experts consider that DSOs, and maybe also TSOs, should conduct mandatory risk assessments, involving technical people to indicate the critical assets and processes, the most critical threats (e.g. intentional threats) and to help define a plan to address them. Mandatory risk assessments should be based on a selected methodology.

3.4.3 The need for a specific risk assessment methodology

Experts consider that there is not a good methodology for understanding/assessing cyber risks of the Smart Grid. They asked for a Programme to address this need. At the same time, some experts referred to the actual work being carried out on this topic by the SGIS European Working Group, the DG CONNECT's ad-hoc expert group, and other US working groups so as to not reinvent the wheel.

3.4.4 Characteristics of the risk assessment methodology

A risk assessment methodology for smart grids should include a dependability analysis, a threat and vulnerability assessment, as well as an interdependencies analysis. Moreover, such a methodology should also include a stakeholder analysis to consider their opinions, assumptions and expectations.

3.4.5 Examples of real risk assessments

Techniques being used by utilities to assess smart grid risks include: collaborative and manual risk assessments based on a workshop approach, where experts met to collaboratively identify risks; use of an actual risk assessment methodology, such as the IS1 methodology from the UK.

3.4.6 Suitability of current risk assessment tool

According to experts belonging to DSOs in The Netherlands the current risk assessments tools used by DSOs are not good to deal with the very distributed nature of the Smart Grid, and in particular of the smart metering systems.

3.4.7 The role of risk assessments in product security certifications

According to several experts, and in order to identify which components of the Smart Grid should undergo a security certification process, a detailed risk-based analysis should be considered.

3.5 Certifications and the role of National Certification Authorities

3.5.1 The role of NCAs

A great majority of participants believe that National Certification Authorities have an important role to play. Some of the suggested roles include: 1) Guaranteeing that the critical components of the smart grid - including specific setups - are secure enough by checking against predefined protection profiles; 2) Certifying that organisational aspects (e.g. processes and people) of grid operators are consistent with the corporate security governance strategy.

3.5.2 European vs. national security evaluation schemes

There are two bodies of opinion on having a European-wide evaluation scheme that applies to all EU MS. There are experts that consider that such a process needs to be coordinated by a European entity, and not independently by each NCA at each MS. On the contrary, other experts argue that priorities on risks and threat levels might be different across Member States and should be addressed independently as a national security issue.

3.5.3 Possible reference standards and initiatives on device-oriented security certifications

In order to certify smart grid individual components and full set-ups, many experts declared that Common Criteria is a reference standard to be considered. Other general reference

standards that were mentioned include FIPS 140 and PCI PTS. Additionally, ISA 99 standard on security controls for embedded systems was also referenced several times. Finally, the The UK National Technical Authority for Information Assurance (CESG), part of the UK government, is currently designing an accreditation process for smart metering devices in the UK which can also be considered as a reference.

3.5.4 Common Criteria in the smart grid

According to the experts, CC is generic certification scheme. Therefore, to be applied in the smart grid environment, it should be extended to include specific security profiles for the Smart Grid, similar to those related to the Smart Card Industry, where a joint interpretation library was developed.

3.5.5 Alternatives to standards-driven device-oriented certifications

According to some experts, standards-driven certifications such as Common Criteria can be a burden for manufacturers and integrators due to their complexity. At the same time they need to be developed, which might take long time. Moreover, smart grid technology is not considered yet mature enough for such kind of certifications. For all these reasons, some experts proposed a more agile alternative, based on quick tests (e.g. white-box and code audits) as it is done in the US National SCADA Test Bed Programme. To this respect, WIB's requirements for vendors (currently IEC/PS 62443 and ISA 62443) are suggested as a possible reference.

3.5.6 Security governance certification for the smart grid

A certification on security governance for the smart grid should check the proper implementation of integral ISMS in grid operators and possibly other actors. A certification like this would provide a baseline for utilities and other stakeholders to measure themselves (i.e. benchmark and to assess the security posture) but also to compare them one to another. Experts suggested considering ISO 27K series of standards as a main reference that would need to be adapted – as it occurred with the telecommunications sector. Other suggested reference standards include ISA 99 and NISTIR 7628.

3.5.7 Alternative to governance certifications

Similarly to the strategy for product/device certification, experts declared that we should not only focus on deciding the best standard for security management (e.g. ISO 27K). In parallel, we should incentivize independent third party companies and organisations to carry out security assessments and penetration testing on DSOs in order to identify vulnerabilities and security flaws.

3.6 Basic aspects for a secure smart grid

3.6.1 Processes, people and technology as main pillars for a secure smart grid

Most of the experts consider that to improve security in the smart grid the first objective should be to secure existing processes and establish appropriate organizational structures for information security management. Additionally, people and technology should also be considered as two basic pillars.

3.6.2 The importance of ISMS

Information Security Management Systems (ISMSs) shall provide the necessary organizational structures, processes, policies and procedures to be able to respond to the ever evolving threat panorama, foster training and awareness rising among staff and deal with technological issues.

3.6.3 Security efforts should not only include smart meters

The current specific focus on smart meters should be further extended to other critical smart grid subsystems, especially: secondary distribution substations, primary distribution substations, transmission substations, micro grids, control centres, and IT and telecommunication systems linking them together.

3.6.4 Infrastructures at the consumer premises should be fool-proof

Home Area Networks are directly dependent on end consumers. Establishing an ISMS or even providing appropriated and updated training in this domain is impossible or highly difficult. Therefore, these systems need to be completely fool-proof, and for this purpose technology will play a key role.

3.6.5 Privacy/security by design and defence in depth strategies

The smart grid has to follow a privacy and security by design approach. Additionally, a defence in depth strategy is considered also a must. In any case, robustness and reliability of the whole grid have to be the guiding principles both from a physical and an ICT point of view.

3.6.6 Security training of operations staff and consumers

People have to be aware of the risks and threats – such as social engineering – that might affect their organisations and lives. In order to achieve this objective, periodic training is of key importance. Moreover, training needs to be adapted to each member of the staff according to the position they hold.

3.7 Smart grid cyber security challenges

3.7.1 Lack of expertise and budget limits in the root causes for dismissing cyber security

Cyber security is almost always considered as an important topic in any Smart Grid project. However, when it comes to a practical implementation is often ignored because of project budgets, scarce funding/incentives and lack of expertise.

3.7.2 A robust and resilient grid

It is agreed that it is necessary to have a robust and resilient grid able to overcome potential attacks, and particularly Denial of Service (DoS) attacks. The challenge is to maintain the current degree of stability in the grid, with similar or even better level of availability.

3.7.3 Data protection and secure data handling

Data protection (i.e. confidentiality, integrity and privacy) and secure data handling of consumer data as well as control and automation readings and commands processed by automated decision-making systems (e.g. distribution balancing) need to be addressed. Regarding personal data protection and secure handling of these data, two great challenges are envisioned by the experts: 1) The possibility of inferring relevant information (e.g. particular habits) from personal data; 2) Metering data will have to be securely accessible by several independent actors (e.g. DSO, service provider, the consumer).

3.7.4 Raising awareness among manufacturers and operators

For security tools and services providers and standardization bodies the greatest challenge is raising awareness and training among manufacturers, as they have to build secure devices, as well as provide expert support. A change of mentality is also necessary among utilities to avoid situations where cyber security is not considered an important issue until massive roll-outs.

3.7.5 Technical challenges

Other challenges pointed out by experts and mainly related with technical aspects include: 1) a proper integration of legacy systems into a robust and resilient grid will be of paramount importance; 2) having standard interfaces at smart grid devices, particularly in what refers to the interaction with security devices such as identity management systems, will be a short-term challenge; 3) unauthorized access to systems or devices; 4) segmentation between ICT infrastructures devoted to "competitive" aspects (e.g. added-value services for consumers) and non-competitive ones (e.g. metering or grid operations); 5) availability of traffic analyzers, communications monitoring and application log monitoring; 6) secure devices (e.g. trust and authentication capabilities).

3.7.6 Incomplete or inexistent regulations

Addressing the consequences of incomplete or inexistent regulations can be a great challenge. Examples on this include: 1) Current regulations promoting smart meter roll-outs not taking into account information security risks; 2) Lack of a complete regulation on the integration of different energy types (e.g. heat, gas and electricity) at the metering infrastructure. This could imply interdependencies and shared cyber security risks between businesses.

3.8 Current smart grid initiatives on cyber security

3.8.1 CEN/CENELEC/ETSI coordination group for Smart Grid, a reference for stakeholders

According to the survey, the most well known initiative dealing with smart grid cyber security is the CEN/CENELEC/ETSI association for Smart Grid standardisation. Moreover, the majority of the stakeholders coincide in pointing it as a reference for smart grids issues in general.

3.8.2 Ongoing initiative for a European smart grid standard architecture

The CEN/CENELEC/ETSI SG-CG will publish a standard architecture by the end of 2012. It is expected to have the final technical report approved by Member States by the end of this year. It will consider different granularity levels, ranging from a conceptual (block diagram) and/or functional architecture to a detailed architecture (including blocks and interconnections) for each one of the general blocks. It will be based on 400 use cases, on existing standards, and should also include security issues.

3.8.3 DG-CONNECT ad-hoc EG, a reference on smart grid cyber security

According to the survey, experts consider DG CONNECT ad-hoc expert group as one of the most important working groups concerning cyber security of the smart grid.

3.8.4 Lack of participation in cyber security related initiatives

Security providers and academia/R&D are by far less involved than other stakeholders in knowledge sharing platforms and other initiatives devoted to smart grid cyber security. However, now that it seems the electrical sector has recognized the high risks which might affect the Smart Grid, they are getting more active. Additionally, DSOs and TSOs should have a more active and leading role. Grid operators will have a central role in the development of the smart grid and should be the ones providing the largest number of security requisites.

3.8.5 Space for improvement in smart grid initiatives

Many experts consider that there is space for improving EU-wide and national initiatives. Some of the major criticisms include: 1) Lack of visibility of EU-wide initiatives; 2) Duplicity of topics across the EU in national initiatives; 3) Same experts in all initiatives; 4) Too much talking and no real work done; 5) Lack of a unified coordination.

3.8.6 Generalised satisfaction about the SG Task Force EG2

Most of the experts that participated in EG2 of the Smart Grid Task Force, on privacy issues of the Smart Grid, were quite satisfied with how the group functioned and on its composition. They consider that all the necessary stakeholders were present.

3.8.7 Opinions about EG2's report on data safety, data handling and data protection

The recommendations provided in the document are considered a high-quality work providing an overview of the problem of privacy and data protection as well as a reference for understanding the roles of the entities participating in smart grids. However, they are also seen as too general and not considering data protection and privacy under the broadest umbrella of cyber security. Additionally, it is suggested to periodically updating the report, extending its scope, and aligning it with other similar documents (e.g. NISTIR 7628, IEC TC57).

3.8.8 Concerns about the progress done by M490's SGIS WG

Relevant experts from the EC declared that it seems that the SGIS subgroup is not progressing at the appropriate pace. It is suggested that this may be the result of a lack of a concrete work programme with specific deliverables and milestones. Likewise, it was recognized that the lack of a standard architecture can be another reason.

3.8.9 Overlaps between M490's SGIS WG and DG-CONNECT ad-hoc EG

Several experts belonging to almost all stakeholder types consider that these two initiatives have overlapping work programmes. Additionally, around 50% of the experts in one group are also present in the other group, while at the same time there are complaints for not being able to cope with the work load of both initiatives.

3.8.10 Conciousness about the overlaps between SGIS and DG-CONNECT ad-hoc EG

Experts from SGIS and DG-CONNECT ad-hoc EG declared that a meeting was organised to clarify the scopes of the work programmes of both initiatives. These experts stated that clear orientation and non-overlapping scopes were agreed.

3.8.11 The need for a coordinating entity on smart grid cyber security and privacy initiatives

Several experts suggested that there should be a unique central coordinating committee with a global vision of all of the European initiatives dealing with cyber security and privacy issues. It should be in direct contact with the EC and other public bodies and standardisation organisations, and would include under its range of action initiatives such as DG CONNECT's ad-hoc EG, SGIS working subgroup, and OpenMeter. According to the needs identified by the experts, its main objectives could include: a) avoid duplicated work; b) enhance communication among task forces; c) define a clear and unified strategy; d) disseminate the work being done; e) establish a common dictionary of technical terms; f) manage lobbies.

3.8.12 New initiatives on awareness raising and dissemination

Experts suggested creating initiatives targeting awareness-raising of C-level (e.g. CEO, CTO, etc.) staff in relation to the importance of the cyber security and data privacy in the Smart Grid. Additionally, some experts also consider important the creation of a dissemination working group targeting end consumers.

3.9 Measuring cyber security in the smart grid

3.9.1 Cyber security effectiveness metrics

DSOs, TSOs, and public bodies consider that cyber security must be measured in terms of robustness, resiliency or reliability of the network under attack conditions. Counting the number and impact (i.e. monetary, image, lives, etc.) of incidents, writing detailed reports about them and controlling the degree of robustness during the operation are some of the metrics/techniques enumerated by these experts.

3.9.2 Need for a European common framework

Many experts agreed on the necessity of having a standard common framework to ensure a minimum level of harmonisation on security and resiliency requirements across Member States, establishing the basis for a minimum set of auditable controls across Europe. This framework would allow National Regulatory Authorities (NRAs) to effectively measure the appropriate security controls and to make comparisons among different companies.

3.9.3 Components of the framework

According to the experts, such a framework should consider including the following elements: 1) A minimum set of standards and guidelines; 2) Certification schemes targeting products/devices and grid operators; 3) A certification authority organised as a PPP; 4) Articulating regulatory mechanisms asking for mandatory certifications and risks assessments; 5) A platform for knowledge sharing among DSOs and TSOs.

3.9.4 A minimum set of standards and guidelines

The following list of standards and guidelines was suggested by some of the experts participating in the study: 1) a common reference architecture; 2) a reference risk assessment methodology; 3) a methodology for assessing interdependencies, 4) an incident handling reference strategy, 5) technical requirements for products; 6) organisational requirements for legal entities playing a market role; 7) standard requirements matching requirements for products with organisational requirements (i.e. default secure reference configurations, guidance for technicians configuring setups, etc.); 8) standard requirements for security governance.

3.9.5 Considerations on regulatory mechanisms

Regarding the articulation of regulatory mechanisms asking for mandatory risk assessments and certifications, experts provided a number of interesting aspects that should be considered: 1) Requirements should be more stringent for systemic organisations; 2) In case of incompliance there should be regulatory pressures (e.g. monetary fines); 3) The European Directive 2008 114/EC should not only include TSOs but also DSOs; 4) (In)compliance results should be public while not revealing confidential information of the grid operator.

3.9.6 Assessing product security

Experts consider that, in order to determine if a product is secure, a development process evaluation and a verification of security functionalities are necessary. The first one is considered especially important for efficiency reasons, so as to avoid product redesigns, which would have costly consequences in a large life-cycle domain, such as is the case of Industrial environments as the Smart Grid.

3.10 Managing cyber attacks

3.10.1 Considerations on cyber security incidents

A cyber security incident can impact any domain along the value chain. For this reason, different stakeholders will have to be involved depending on the type of incident, ranging from electricity generators to consumers, and at all levels, from infrastructures to services and operations. It is important to pay attention to value-chain interdependencies, as for example among DSOs, with TSOs, retailers, etc. as well as to the impact on other critical infrastructures at the national and European levels.

3.10.2 Existing experience on incident handling

Several experts stated that TSOs and DSOs are used to dealing with incidents of different type (e.g. blowing of transformers due to an overload). Moreover, they declared that there are structures and mechanisms in place, at the organisational and coordination level and also at the technical level that should be considered so as to not reinvent the wheel; DSOs and TSOs are good already in restoring the power service since they've been doing it for the last 100 years.

3.10.3 DSOs and TSOs should be in charge of incident detection

Experts agreed that TSOs and DSOs need to perform monitoring actions to detect possible incidents affecting the European power grid as a whole and also in each MS. In European-wide incidents, many experts consider that TSOs should be the organisations in charge of monitoring and triggering alarms. Experts mentioned the IRRIS FP7 IP project as a reference for the creation of an alarming system for grid operators.

3.10.4 Technical aspects of cyber security incident detection

Experts provided relevant technical details on incident detection in Smart Grids: 1) Security monitoring sensors should be distributed across the grid gathering data that could be processed in a decentralised or centralised manner; 2) A central monitoring centre for data collection and analysis could adopt the structure of a Security Operations Centre (SOC); 3) Signature-based software will be needed in sensors; 4) Correlation and intelligence capabilities can be distributed across the grid or included in the SOC; 5) Intelligence implies being able to distinguish if the root cause of an incident is a cyber security event or any other event; 6) Monitoring centres could also perform research activities (i.e. write new signatures, study new threats, etc.).

3.10.5 Regulation on incident management

There should be a regulation obliging grid operators to report on incidents to a national or supranational entity.

3.10.6 A European entity for the coordination of large scale cyber security incidents

Several experts share a common view on the need for a pan-European entity which coordinates transnational structures (i.e. European TSOs) and national CIP agencies when managing a large scale cyber security incident. Such an entity should have the following characteristics: 1) A global overview on what is going on in the European grid; 2) It should be in charge of escalating alarms and acting upon them - final decisions (e.g. isolating a TSO) are considered a political issue; 3) It should understand interdependencies in the European grid and with other critical infrastructures; 4) It should have direct communication with normal crisis management structures in place.

3.10.7 Controversy on candidate organisations for large scale incidents coordination

An expert from academia considers that operators should be involved but should not take any decision in order to avoid conflicts of interest. Other experts suggest ENISA, ENTSO (European Network of TSOs), ACER (Agency for the Cooperation of Energy Regulators) as possible good candidates.

3.10.8 Alternatives to a European large-scale cyber incidents coordinating entity

There are several sceptic experts about the idea of having a centrally coordinating entity. They think that reaction times will be worse, since trying to address the incidents from a global point of view can be by far more complicated than solving individual problems. These experts suggest a more decentralized approach by simply improving communications and coordination procedures among directly related agents.

3.10.9 Role of CERTs[2] in smart grid incidents management

Experts agreed CERTs could play a role but should not be the central piece. They consider that there is room for ICS and smart grid CERT functionalities at the EU level, where the knowledge of the different countries would be combined. In cases of very large cyber incidents this entity should be advising the normal crisis management structures in place at the EU and MS, which would involve grid operators and public bodies.

3.10.10 Scope of CERTs addressing smart grid security issues

Experts consider that it is better to extend the scope of the current CERTs – both public and private ones – instead of creating CERTs focusing only on smart grid cyber security issues. An EU-level CERT dealing with smart grid aspects should also have a broader view on other critical infrastructures, telecommunication systems, etc. Moreover, some of the characteristics and services of these CERTs could include: 1) A unified point for information exchange among smart grid stakeholders; 2) A reference for valuable information (e.g. good practices distribution); 3) A central point for cyber security monitoring for power grids; 4) A leader in awareness rising activities; 5) A help point on cyber security certifications.

3.11 Research topics in smart grid security

3.11.1 Protection of grid controlling/monitoring systems

New services and highly automated systems in smart grids – at TSO, DSOs, retail, etc. – will need to monitor the grid more deeply than ever before by implementing new monitoring technologies (e.g. synchrophasors). It is necessary to have a security infrastructure capable of guaranteeing trusted large scale transactions (millions of devices that could be shut down for one hour at the scale of a country, which will result in lots of payment information transactions, etc.).

3.11.2 Architecture

This topic would include: self-healing and graceful degrading architectures; standard and secure interconnections among domains; management of processes associated with the use of cryptographic material (i.e. generation, distribution and storage of cryptographic material); active monitoring for attack detection and traceability.

3.11.3 End-to-end security

Cyber security strategies should be considered at a global level and not defined for each domain separately. Such a topic should include dependencies analysis (i.e. dependencies types, business process dependencies, impact propagation, etc.) across the whole smart grid,

[2] *It should be noted that, in general, the terms CERT and CSIRT (Computer Security Incident Response Team) are often interchanged, though the first is actually a registered trademark of Carnegie Mellon University.*

and include: security governance; use-case modelling; threat analysis; and the development of security mechanisms against distributed denial of service attacks and other attacks.

3.11.4 Trust and assurance

This topic would include: security metrics to measure the maturity level of security controls for each domain of the Smart grid; hardware-based one-way communications.

3.11.5 Security in dependable systems

This category would include subtopics such as: the definition of common procedures and interfaces; the overcome of hardware constraints limiting log management; encryption functionalities; application/network filtering capabilities.

3.11.6 Privacy and security by design

This topic would include research areas such as: protection against zero-day vulnerabilities; optimization of very specific cryptographic protocols to reduce processing load without reducing the security level.

3.11.7 Other topics

Experts also provided other topics which cannot be included in any of the abovementioned categories. These are: supply chain protection; usability, legal and economic issues; and smart grid and the cloud.

3.12 The smart grid business case

3.12.1 Balance between cost and benefits

The huge cost/investment of implementing the necessary infrastructures cannot be understood without the benefits deriving from the new services, applications and functionalities (e.g. reduced emissions, increased energy efficiency, demand-response, etc.).

3.12.2 Key drivers of the Smart grid business case

In addition to optiminization and efficiency, a majority of respondents also consider that reliability and resiliency are key factors driving the smart grids business case.

3.12.3 Other drivers of the Smart grid business case

Experts suggested other drivers of the smart grid business are: a need for a scalable power grid, DERs integration, integration of renewable energy sources, support the integration of the EV, and new business opportunities/value-added services for consumers.

3.13 Recommendations for Protecting Industrial Control Systems (ENISA report)

What follows is the list of recommendations provided in ENISA's previous study on ICS protection "Protecting Industrial Control Systems: recommendations for Europe and Member States" (9). They have been included here for completeness, since many of the abovementioned key findings complete and superceeds these general recommendations on industrial control systems in regards to the smart grids domain.

3.13.1 Creation of Pan-European and National ICS Security Strategies

The European Union should create a pan-European Strategy for European ICS Security activities and each Member State should develop a National Strategy for ICS Security. The strategies must be coherent with the European Union Council Directive 2008/114/EC for Critical Infrastructures, and leverage the existing initiatives addressing the problem of ICS Security (e.g. EuroSCSiE) as well as the national and Pan-European Public Private Partnerships (e.g. EP3Rs). The strategies have to serve as references for all state-members stakeholders, act as facilitators for sharing initiatives and foster research and education.

3.13.2 Creation of a Good Practices Guide for ICS security

The European Union should assume leadership and develop a consensus-reached document or set of documents regarding security good practices, integrating both physical and logical security aspects, to serve as reference for every type of stakeholder. This document should help all stakeholders ensure that best security practices are applied in the industry.

3.13.3 Creation of ICS security plan templates

The different National ICS Security Strategies should consider within their tasks the creation of ICS security plan templates, both for operator and infrastructures, which security experts could adapt to their particular situation. These plans should include operational and physical security, technical issues, training and awareness, security governance with roles and responsibilities, business impact measures and crisis management. These templates should severely decrease the cost of developing security plans and accelerate the adoption of comprehensive security measures within the industry.

3.13.4 Foster awareness and training

As part of national ICS-Security strategies, the Member States should foster dissemination and awareness activities through high quality events involving all kinds of stakeholders and with special attention to top management commitment. Training and awareness programmes and events should be created for all types of end users.

3.13.5 Creation of a common test bed, or alternatively, an ICS security certification framework

The Common ICS-Strategy should lead to the creation of a common test bed(s) at European level, as a Public-Private Partnership in which tests could be performed in order to guarantee that different systems interaction do not cause security failures. A common test bed will help all stakeholders to detect potential problems in a controlled environment, ensuring integrity and increasing the trustfulness in certified solutions.

Alternatively a security framework model adapted for ICS could be defined, based on existing efforts such as Common Criteria or FIPS. Member State existing certifying organisms would be responsible for the certification process based on this security framework.

3.13.6 Creation of national ICS-CERTs

Following the national ICS Security Strategies, national ICS-CERTs should be established, in cooperation with an adequate number of public and private CERTs. The ICS-CERTs activities should help all stakeholders to have a reference in order to share vulnerability information, disclosure it, coordinate actions and help in effectively dealing with risk management in ICS infrastructures. In order to address the challenges which span across the borders, the National ICS-CERTs should cooperate on the Pan-European level (e.g. with the aid of an ICS-Security information sharing platform such as EuroSCSiE).

3.13.7 Foster research in ICS security leveraging existing Research Programmes

The National and Common ICS Security Strategies should foster research to address current and future ICS threats and security challenges such as ICS-ICT integration, legacy/insecure equipment, targeted attacks or Smart grid issues. This should be done by leveraging existing European or National research programmes, such as the European Framework Programme.

4 Recommendations

Based on the key findings described above, this chapter presents 10 recommendations to achieve a future European smart grid. These recommendations focus on national and pan-European initiatives that should be implemented as soon as possible. They are intended primarily for public bodies and authorities and specifically to the national and European ones. However, they also target other stakeholders such as manufacturers and integrators, grid operators, energy producers, energy consumers, smart grid services providers, security tools and services providers, academia/R&D, and standardisation bodies.

The 10 recommendations address different smart grid security topics and can be considered as equally important. They are coherent among them and can be implemented independently even though there are clear bindings among each. For instance, recommendation 1 presents an enhanced regulatory framework on smart grid security asking for mandatory risk assessments and standards-driven compliance. Supporting these requirements, recommendation 5 suggests developing a minimum set of standards, including a risk assessment methodology and security requirements for organisations and products. Besides, recommendation 6 proposes fostering the development of security certification schemes based on these standards and supporting the policy and regulatory framework.

The detailed descriptions of the recommendations contain the following sections:

- Description: where the core content of the recommendation is presented. It can be considered as the “what” and the “how” parts of the recommendation.
- Objective: provides a more detailed description of what would be the benefits of this recommendation.
- Steps: suggests a number of possible phases to successfully implement the recommendation.

4.1 Recommendation 1: Improve the regulatory and policy framework

4.1.1 Description

The EC and MS competent authorities should take the lead and develop specific policy documents and regulations on cyber security and privacy of the smart grid in order to improve the current regulatory and policy framework. This extended framework should define and develop, by taking into account existing regulations and policies on smart grid, the root principles, challenges, goals and needs of a long-term European-wide cyber security and privacy strategy for the grid of the future. Policies and regulations should at least look for: 1) considering privacy and cyber security as two intrinsically interdependent topics; 2) defining security measures to be considered in current smart grid deployments (e.g. smart meter roll-outs); 3) demanding grid operators for mandatory risk assessments; 4) demanding manufacturers, integrators, services providers and grid operators to comply with specific

security certifications; 5) establishing regulatory pressures (e.g. fines) for not complying companies; 6) making public the compliance results; 7) demanding operators to report on cyber security related incidents to a national or supranational entity.

4.1.2 Objective

The articulation of a broad and complete regulatory and policy framework would bring cyber security to the front-line of action, recognizing these matters as key factors for its success and as an essential and fundamental part in the definition of smart grid business models, functionalities, services, etc. Establishing regulatory pressures for not complying companies will help change their mentality, which will be important for evaluating cyber security at the pilot phase or for avoiding companies dismissing cyber security for budgetary or lack of experience reasons. It would change the perception that Europe is not paying enough attention to cyber security and privacy in smart grids. Moreover, cyber security and privacy would be treated as a whole and not as two separate disciplines.

On the other hand, this legal framework would help harmonize existing policies and regulations addressing cyber security, and will be considered as a reference with which to align policies and regulations on other aspects. This would be the case of those promoting smart meter roll-outs or the integration of different energy types (e.g. heat, gas and electricity) at the metering infrastructure. In combination with other recommendations provided in this document, this new framework will ensure a minimum level of harmonisation on security and resiliency requirements across Member States, establishing the basis to allow National Regulatory Authorities (NRAs) to effectively measure security and to make comparisons among different companies.

4.1.3 Steps

- At the European level, the necessary contacts network has to be established: DG ENER, DG CONNECT, DSOs, TSOs, CEN/CENELEC/ETSI SGCG, Smart grid Task Force, etc.
- Regulatory pressures and other mechanisms are analysed in detail with the involved stakeholders
- The previous regulatory actions are analysed and considered as a basis
- A strategy for implementing the regulatory framework is defined
- Policy documents, EC communications and Directives are prepared and published according to the previous strategy

4.2 Recommendation 2: Foster the creation of a Public-Private Partnership (PPP) entity to coordinate smart grid cyber security initiatives

4.2.1 Description

The EC in cooperation with ENISA and the MS should foster the creation of a public-private partnership incorporating MS public bodies and the private sector. This PPP should act as a unique central coordinating entity at the EU-level with a global vision of all European and MS's initiatives dealing with cyber security and privacy issues. It should be in direct contact with the

EC, MS authorities and other public bodies and standardisation organisations. Under its range of action should include the coordination of the work done at EU-level initiatives such as DG CONNECT's ad-hoc EG, SGIS working subgroup, or OpenMeter. Its main objectives should target: 1) avoiding duplicated work; 2) enhancing communication among task forces and work groups; 3) defining a clear and unified strategy for ongoing and new initiatives; 4) Identifying synergies among national and European initiatives; 5) disseminating the work being done; 6) establishing a common dictionary of technical terms; 7) and managing lobbies.

4.2.2 Objective

Such a PPP would be a reference for the smart grid community. It would help disseminate the major achievements, facilitating the search for specific information on security topics (e.g. standardisation, policies, technologies, research, etc.) and minimizing the current lack of visibility of some of the current initiatives. Besides, it would articulate the global lines of action of the EC on cyber security aspects of the smart grid by coordinating existing initiatives or creating new ones to address them.

Additionally, the proposed coordinating entity will help: remove the current duplicity of topics across the EU; make the most of the available resources and experts volunteering to collaborate; coordinate roadmaps to avoid situations where an initiative is paralysed because of the lack of output from another; define and update the work programmes and establish requirements for new and existing initiatives; foster cooperation and alignment with sister initiatives outside the EU (e.g. US-EU collaborations); achieve a balanced and complete presence and leadership of stakeholders; etc.

4.2.3 Steps

- Identify initiatives of interest on smart grid security at the EU and national levels
- Analyse the current work programmes, expected results, interdependencies, potential synergies, gaps, duplicities, etc.
- Establish appropriate communication channels and procedures
- Define a common, coherent and clear strategy for current and future initiatives
- Establish the necessary mechanisms for managing dissemination activities
- Get MS public bodies and the private sector together in order to create the coordinating entity

4.3 Recommendation 3: Foster awareness raising and training initiatives

4.3.1 Description

Under the umbrella of the aforementioned PPP, EC, ENISA and the MS and the should foster the creation of initiatives targeting awareness-raising of C-level (e.g. CEO, CTO, etc.) staff of grid operators, electricity services providers, manufacturers and end consumers in relation to the importance of the cyber security and data privacy in the smart grid. Besides, specific training initiatives should also be created for manufacturers on how to build secure devices and applications, for grid operators on the threats and risks affecting the resiliency and

security of the grid, as well as for services providers and end consumers on fraud prevention, privacy, etc.

4.3.2 Objective

Fostering awareness and training will probably contribute to change the generalized perception that cyber security is not a first interest matter in the development of the smart grid. For instance it will probably help changing mentality to avoid situations where utilities do not consider cyber security as an important issue until massive roll-outs. Training, adapted to the profile of the trainees (e.g. specific training according to staff positions, end consumers, etc.), manufacturers, etc. will also contribute to establish a security culture in organisations and end consumers as well as raise their expertise in the field.

Among the basic objectives of CERT organisations contributing to raising security awareness is one of the most relevant. For this reason, CERTs – preferable those specialised in industrial ICT – are very well positioned to contribute to the purposes of this recommendation.

4.3.3 Steps

- Build a network of C-level contacts for the main grid operators and services providers in Europe.
- Identify the forums and events of interest of C-level staff.
- Prepare the appropriate media for raising awareness on smart grid security aspects of C-level staff.
- Participate in the identified forums and events.
- Organise through the appropriate channels (e.g. ENISA) specialised technical events for raising awareness and training.
- Analyse, in cooperation with CERTs and other platforms such as ENCS (former CyberTECH), the alternatives for fostering awareness rising and training.

4.4 Recommendation 4: Foster dissemination and knowledge sharing initiatives

4.4.1 Description

Under the umbrella of the aforementioned PPP, EC, ENISA and MS should actively involve security providers and academia in current knowledge sharing initiatives, as well as increase DSO/TSO leadership in cyber security initiatives. Besides, dissemination of the results of existing initiatives should be actively encouraged. Moreover, the creation of a platform for knowledge sharing among DSOs and TSOs – and possibly other stakeholder – should be analysed. To this respect CERTs could play a role as a unified point for information exchange among smart grid stakeholders as well as a reference for valuable information (e.g. good practices distribution).

4.4.2 Objective

Grid operators will have a central role in the development of the smart grid and should be the ones providing the largest number of security requisites. For this reason it is necessary that they have a leading role in cyber security initiatives. Additionally, encouraging existing initiatives to actively disseminate their work will help reduce their lack of visibility while an EU level coordinating entity for smart grid cyber security initiatives is created.

In addition to contributing to raising security awareness, CERT organisations are also expected to be a reference on valuable information about ICT security. For this reason, CERTs – preferable those specialised in industrial ICT – are very well positioned to contribute to the purposes of this recommendation.

4.4.3 Steps

- Build a network of C-level contacts for the main grid operators and services providers in Europe.
- Identify the forums and events of interest of C-level staff.
- Establish a global strategy for disseminating the activities and results being undertaken by active initiatives.
- Apply the dissemination strategy in a coordinated and coherent manner.
- Leverage the built network of contacts to achieve that DSOs and TSOs have a leading role in information sharing initiatives as well as to actively involve academia/R&D.
- Analyse, in cooperation with CERTs and other platforms such as ENCS (former CyberTECH), the alternatives for establishing a knowledge sharing platform.

4.5 Recommendation 5: Develop a minimum set of reference standards and guidelines

4.5.1 Description

The EC, in collaboration with ENISA and the MS competent authorities and the private sector, should develop, by leveraging existing initiatives, a minimum set of reference standards and guidelines on cyber security for the smart grid. The set should include at least: 1) a common reference architecture; 2) a reference risk assessment methodology; 3) technical requirements for smart grid systems; 4) guidelines on security governance for legal entities involved in the future grid; 5) guidelines for achieving fool-proof home networks. This body of standards and guidelines shall set a basis for conducting assessments and support the development of a European certification scheme for vendors and grid operators.

4.5.2 Objective

Smart grid companies along the value chain are getting more and more interconnected and interdependent. Therefore, there is the necessity of an end-to-end security approach, from the lowest levels (meters, physical, etc.) to the upper ones (application systems, integration with corporate systems, value-added services, etc.) and all along the smart grid value chain. It

is considered that having a standard architecture of the smart grid is on the basis of such a strategy. Moreover, a consensus-based reference standard architecture is central to avoid cyber security initiatives being “paralysed” from addressing challenges such as the secure integration of legacy systems in a robust, resilient and smart grid, or segmenting ICT infrastructures devoted to "competitive" aspects (e.g. added-value services for consumers) from non-competitive ones (e.g. metering or grid operations).

The mandatory risk assessments being asked by the legal framework defined in recommendation 1 should be based on new methodology that should leverage the actual work being carried out on this topic by the SGIS European Working Group, the DG CONNECT’s ad-hoc expert group, and other US working groups. Moreover, it should consider the particular experiences of stakeholders, such as the case of utilities that conducted collaborative and manual risk assessments based on a workshop approach. According to the experts, the risk assessment methodology to be developed should include a dependability analysis, a threat and vulnerability assessment, as well as an interdependencies analysis. Moreover, such a methodology should also include a stakeholder analysis to consider their opinions, assumptions and expectations.

Cyber security and privacy should be addressed at the design phase so as to minimize costs and maximize security. Defining standard technical requirements for smart grid systems will allow vendors to take them into account during the design phase. Moreover, they would set a basis for defining a security certification scheme for smart grid products. These requirements should not only focus on smart meters but be further extended to other critical smart grid subsystems, especially secondary distribution substations, primary distribution substations, transmission substations, micro grids, control centres operated by SCADA systems, and the IT and telecommunication systems linking all them together. These technical standard requirements should be based in existing initiatives such as ISA 99 (10) on security controls for embedded devices or WIB’s requirements for vendors (11).

On the other hand, the creation of guidelines on security governance for legal entities involved in the future grid Information, will allow them easily adapt their Security Management Systems (ISMSs) to also include industrial equipment such as substations, AMI, SCADA systems, etc. A full scale ISMS will provide the necessary organizational structures, processes, policies and procedures to be able to respond to the ever evolving threat panorama, foster training and awareness rising among staff and deal with technological issues. Guidelines on security governance for smart grids should leverage existing initiatives such as ISO 27K, ISA99 (10) and NIST IR 7628 (12).

Both, security requirements for systems as well as security guidelines on security governance in the smart grid, should be developed considering at least the principles of robustness, resiliency and reliability of the grid and privacy of consumer data. According to many experts, cyber security should be measured according to these indicators and therefore security requirements should consider them as a security target.

Finally, since Home Area Networks are directly dependent of end consumers, associated systems need to be completely fool-proof, and for this purpose secure and security technology will play a key role. Specific guidance on this topic is necessary to allow defining the best suited architecture or selecting the most appropriate technologies (i.e. encryption).

4.5.3 Steps

- Analyse the current work being done by initiatives such as the SGIS working group or DG CONNECT's ad-hoc EG.
- Leverage existing information sharing platforms to fully understand industry expectations, compare them against existing work, and identify gaps.
- Achieving a common reference architecture should be set as the main priority
- Develop the common reference architecture.
- Leverage previous experience on smart grid risks assessment methodologies by actively involving DSOs and TSOs.
- Develop a risk assessment methodology coherent with the common reference architecture.
- Based on the common reference architecture, define a number of technical requirements for smart grid systems.
- Develop best practices guidelines on security governance, and for achieving a fool-proof HAN/IAN/BAN

4.6 Recommendation 6: Promote the development of security certification schemes for products and organisational security

4.6.1 Description

EC and MS competent authorities should foster the development of security certification schemes for product and organisational security, leveraging existing initiatives such as Common Criteria, ISA99, and ISO 27K. These certification schemes should harmonise security and resiliency requirements across Member States, establishing the basis for a minimum set of auditable controls across Europe. Security certificate issuance capabilities should be accredited to National Certification Authorities.

4.6.2 Objective

By raising the level of security and mitigating risk, accreditation and certification schemes would increase end consumers' confidence in smart grid services and systems and accelerate their acceptance. Moreover, certified service providers can be easily compared allowing for marketing strategies. Product certificates would provide grid operators and service providers with information on the level of security attached to a product or system they may wish to purchase, knowing if they will be secure enough for a specific smart grid application, as well as allowing them to compare with other products or systems of the competence. Likewise, a certification on security governance for the smart grid should check the proper implementation of integral ISMS in grid operators and possibly other actors. A certification

like this would provide a baseline for utilities and other stakeholders to measure themselves (i.e. benchmark and to assess the security posture) but also to compare them one to another.

On the other hand, during the study it became clear that in order to determine if a product is secure, a development process evaluation and a verification of security functionalities are necessary. The first one is considered especially important for efficiency reasons, so as to avoid product redesigns, which would have costly consequences in a large life-cycle domain, such as is the case of Industrial environments as the Smart grid. A well developed product certification scheme would allow for both types of assessments by defining the appropriate security assurance requirements.

This recommendation should leverage the set of standards promoted in recommendation 3, and specifically the technical requirements for smart grid systems and the guidelines on security governance for legal entities involved in the future grid. As it was already discussed in this recommendation, CC or ISO 27K were the most popular standards for developing the suggested certification schemes for smart grid. However none of them are directly applicable. According to the experts, CC is not specialised on control systems and other smart grid industrial elements. Therefore, to be applied in these environments, it should be extended to include specific security profiles for the smart grid, similar to those related to the smart card industry, where a joint interpretation library was developed. On the other hand experts suggested adapting ISO 27K series of standards as it occurred with the telecommunications sector.

4.6.3 Steps

- Conduct a risk-driven identification of those components and set-ups that should be security certified.
- Analyse previous experiences (e.g. smart card industry) on how to adapt existing standards and good practices (e.g. test beds) for defining smart grid security certification schemes.
- Develop certification schemes for products and set-ups as well as for organisational security
- Accredit NCAs as issuers of the corresponding security certificates.
- Accredit independent companies as evaluators of these certification schemes.

4.7 Recommendation 7: Foster the creation of test beds and security assessments

4.7.1 Description

MS competent authorities and EC should foster the creation of test beds to assess, by means of quick and agile tests, if products are secure according to basic security principles, such as those defined by WIB's requirements for vendors. Additionally, it should be incentivized that independent third party companies and organisations carry out security assessments and penetration testing on DSOs, TSOs and other smart grid actors so as to identify security flaws

at the organisational level. These actions should fill the gap while certification schemes are being developed. Moreover, the suggested test beds, which should preferably be organised as PPP, could eventually become accredited certification evaluators once the proposed certification schemes are ready.

4.7.2 Objective

The availability of test beds with the necessary infrastructure and qualified personnel to perform agile security tests (e.g. white-box and code audits) against standards such as WIB's requirements for vendors will be highly useful. Such test beds will allow manufacturers to quickly assess if their products and systems comply with a minimum set of security requirements, that operators associations are considering as basic. The verification of security functionalities in final devices is considered an essential element for many of the experts participating in the study. Besides, this will contribute to create a the breeding ground so as to manufacturers and vendors start thinking in the necessity of establishing mechanisms for evaluating security functionalities during the development process.

In the future, if the proposed certification schemes are developed, these test beds could assume the role of independent evaluators, accredited by MS governments that would prepare the evaluation report to be validated by National Certification Authorities. Moreover, their experience with the agile security tests will bring them to a privileged position to help develop the protection profiles of product certification schemes.

Additionally, such test beds could also be the perfect organisation to support the accomplishment of some others of the previous recommendations of this report. In addition to helping developing the product certification scheme, they might also play a role in supporting the development of improved industry standards applicable to smart grids. Likewise they might also contribute to knowledge sharing and dissemination by participating in conferences that include smart grid security topics where they would share information obtained through system assessments and analyses. Finally, such test beds could also be a training platform if they organised workshops to describe common cyber vulnerabilities found in control systems and other smart grid systems and providing effective methods for their mitigation.

The construction of test beds should be based on well-established approaches that allow the execution of scientifically rigorous security assessments in safe experimentation environments. The inter-disciplinary nature of Smart Grids as a scientific area will definitely represent a challenge for test bed creators that will struggle to cover all possible constraints and requirements. Therefore, it is likely that many geographically distributed test beds, each focusing on a different aspect of Smart Grids, will need to interconnect and share resources. For instance, cyber-security assessment test beds, e.g. the EPIC (13)(Experimental Platform for ICT Contingencies) test bed developed within the Joint Research Centre, might need to federate with other test beds focusing on the electrical grid, e.g. test beds at remote locations. A first effort for the creation of a thematic network of European experimental

facilities in the field of Industrial Control Systems and Smart Grids has already been started by the ERNCIP project (14).

4.7.3 Steps

- Coordinate a group to clearly define the purpose of such test beds.
- Identify the requirements and design the organisation of such a test bed.
- Involve the main actors: manufacturers, integrators, and security tools and services providers.
- Identify guidelines for reference on security requirements for technologies, products and set-ups
- Develop a set of guidelines for quick product/technology/set-up assessments: source code analysis, black-box assessment, etc.
- Further analyse how these test beds can be reconverted in accredited certification evaluators.

4.8 Recommendation 8: Refine strategies to coordinate large scale pan-European cyber incidents affecting power grids

4.8.1 Description

EC, ENISA and the MS competent authorities should further study strategies to coordinate the response to large scale cyber incidents affecting European power grids, studying the convenience of a central coordinating entity or alternatively a decentralised self-coordinated mesh of grid operators. These strategies should consider existing transnational electricity structures (i.e. European TSOs and DSOs) and national CIP agencies as well as other crisis management structures in place and CERTs. Besides, topics such as alarm scalation, political decisions (e.g. isolating a TSO) and pre-established incident handling procedures should also be discussed, taking into consideration existing and future interdependencies inside the European grid.

4.8.2 Objective

A cyber security incident can impact any domain along the value chain. Therefore, in order to develop strategies for handling cyber incidents, different stakeholders will have to be involved, ranging from electricity generators to consumers, and at all levels, from infrastructures to services and operations. Besides, structures and mechanisms in place, at the organisational and coordination level and also at the technical level should be considered so as to not reinvent the wheel. During the study experts agreed that TSOs and DSOs need to be the ones performing monitoring actions to detect possible incidents, affecting the European power grid as a whole and also in each MS. In European-wide incidents, many experts consider that TSOs should be the organisations in charge of monitoring and triggering alarms,

and mentioned the IRRIS FP7 IP project (13) as a reference for the creation of an alarming system for grid operators.

Experts provided relevant technical details on how to implement incident detection in smart grids, which should also be considered when discussing the creation of a pan-European entity to manage large-scale cyber incidents. Some of the suggestions that experts made include:

- Security monitoring sensors should be distributed across the grid gathering data that could be processed in a decentralised or centralised manner.
- A central monitoring centre for data collection and analysis could adopt the structure of a Security Operations Centre (SOC).
- Signature-based software will be needed in sensors.
- Correlation and intelligence capabilities can be distributed across the grid or included in the SOC.
- Intelligence implies being able to distinguish if the root cause of an incident is a cyber security event or any other event.
- Monitoring centres could also perform research activities (i.e. write new signatures, study new threats, etc.)

Another topic for discussion with respect to coordinating a global response to large scale cyber incidents is the degree of involvement of grid operators. It is widely accepted that operators should be involved in the detection and service restoration phases. However, it is not clear if they should be involved when decisions have to be taken so as to avoid conflicts of interest. Moreover, there are several candidates that could opt to be the germ of a central coordinating European entity. Experts suggest ENISA, ENTSO (European Network of TSOs), and ACER (Agency for the Cooperation of Energy Regulators) as possible good candidates. On the other hand there are several sceptic experts with respect to the idea of having a centrally coordinating entity. According to them, this approach would worsen reaction times, since trying to manage incidents from a global point of view can be by far more complicated than solving individual problems. These experts suggest a more decentralized approach where communications and coordination procedures among directly related agents are improved.

4.8.3 Steps

- Involve all stakeholders in an open discussion on the needs, advantages and disadvantages of an EU-level coordinating entity for large scale cyber incidents.
- Analyse current procedures and structures for handling large scale incidents so as to identify gaps.
- Analyse the role of ENTSO, ACER and ENISA in a future pan-European coordinating entity.
- Discuss the role of grid operators and CERTs in dealing with large scale cyber incidents.

4.9 Recommendation 9: Involve CERTs to play and advisory role in dealing with cyber security issues affecting power grids

4.9.1 Description

EC and the MS competent authorities should encourage competent CERT[3]s to extend their capabilities to deal with smart grid cyber security issues. These CERTs should also have a broader scope, including other critical infrastructures (e.g. telecommunication systems or transportation systems) that are directly interdependent on the power grid. Particularly, in the case of very large cyber incidents, these entities should advise the normal crisis management structures in place at the EU and MS levles, including grid operators and public bodies and in full alignment with the strategies to be defined according to recommendation 8.

4.9.2 Objective

In order to deal with cyber incidents affecting the current power grid and future smart grids in Europe, coordination with CERTs could be very valuable and probably needs to be further studied. The experts of this study agreed that CERTs could play a role in incident management but should not be the central piece. For instance, in the case of very large cyber incidents, this entity should be advising the normal crisis management structures in place at the EU and MS.

Experts consider that it is better to extend the scope of the current CERTs – both public and private ones – instead of creating CERTs focusing only on smart grid cyber security issues. CERTs dealing with smart grid aspects should also have a broader view on other critical infrastructures, telecommunication systems, etc. Moreover, during the interviews and the survey, the experts identified some of the characteristics and services for these CERTs. These include being: 1) a unified point for information exchange among smart grid stakeholders; 2) a reference for valuable information (e.g. good practices distribution); 3) a central point for cyber security monitoring for power grids; 4) a leader in awareness rising activities; 5) a help point on cyber security certifications.

4.9.3 Steps

- Consider other initiatives to find synergies and avoid duplicated efforts, such as the already recommended ICS-CERT
- Contact Member State authorities to coordinate the collaboration with national public and private CERTs
- Define smart grid computer emergency response capabilities as well as functional and operational duties
- Clearly define the contributions from every public and private CERT

[3] *Some CERTs might be private.*

- Collaborate with ongoing initiatives addressing the definition of management strategies for dealing with large-scale cyber security incidents affecting power grids in Europe

4.10 Recommendation 10: Foster research in smart grid cyber security leveraging existing research programmes.

4.10.1 Description

EC and the MS research and development competent authorities in cooperation with the Academia and R&D sector should assure that existing and future national and European research programmes, such as FP7 and Horizon 2020 (14), will incorporate into their work programmes research lines on smart grid related cyber security aspects. Some of these research lines are:

- Protection of monitoring functionalities and automated decision making systems of the smart grid
- Robust, secure and resilient architectures: self-healing and graceful degradation; generation, distribution and storage of cryptographic material
- Trust and assurance and end-to-end security: dependencies and threat analysis and use-case modelling; active monitoring for incident detection; security metrics; security mechanisms against DoS attacks
- Security in dependable systems: legacy systems; encryption functionalities; application/network filtering
- Privacy and security by design: common procedures and interfaces, protection against zero-day vulnerabilities, optimization of cryptographic protocols.
- Supply chain protection
- Secure smart grid in the cloud
- Legal and economic aspects of cyber security in the smart grid

4.10.2 Objective

The general objective is to help overcome the cyber security challenges of the grid of the future, by achieving highly reliable and robust grids able to cope with an ever evolving threat landscape. Prosumer is also considered a major target by addressing privacy issues but also by acknowledging their importance in the operation and stability of the new grid.

Data protection (i.e. confidentiality, integrity and privacy) and secure data handling, of consumer data as well as control and automation readings and commands processed by automated decision-making systems (e.g. distribution balancing) will be of paramount importance. The abovementioned research topics will help develop the necessary technology and strategies to address this important challenge.

Moreover, other challenges that have been identified by the experts participating in the study and which will have to be addressed by research include:

- A proper integration of legacy systems into a robust and resilient grid

- Having standard interfaces at smart grid devices, particularly in what refers to the interaction with security devices such as identity management systems
- Unauthorized access to systems or devices
- Segmentation between ICT infrastructures devoted to "competitive" aspects (e.g. added-value services for consumers) and non-competitive ones (e.g. metering or grid operations)
- Availability of traffic analyzers, communications monitoring and application log monitoring
- Secure devices (e.g. trust and authentication capabilities).

4.10.3 Steps

- Establish priorities for the different research objectives
- Make contact with existing security programmes at EU and National levels, such as the European Framework Programme and Horizon 2020
- Work together with appropriate organisations and bodies (e.g. Framework Programme Committee and Advisory Groups, Technology Platforms, etc.) to define an appropriate Work Programme
- Emphasize the importance of disseminating results

5 Conclusions

This study proposes 10 recommendations to the public and private sector involved in the definition and implementation of the smart grids. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing co-operation, raising awareness, developing new measures and good practices, and reducing barriers to information sharing. ENISA considers that these recommendations are effective, achievable, and urgent. This opinion is also shared by the experts who attended the validation workshop in which these recommendations were presented. Moreover, they showed their strong support for improving the recommendations and their willingness to help in their implementation.

ENISA considers that the implementation of these recommendations is urgent because the smart grid, which is being built at the same time is being defined, is the greatest revolution of the electricity power grids since their creation. It is a major upgrade that prepares our power systems for the 21st century and for which Information and Communication Technology (ICT) is of paramount importance. Thanks to ICT, the grid of the future will become smarter so as to improve reliability, security, and efficiency of the electric system through information exchange, distributed generation, storage sources, and the active participation of the end consumer. The development of smart grids exemplifies the increasing dependency of European economy and society on Information and Communication Technologies.

The implementation of these recommendations will be challenging. Many of them will require the active collaboration between the public organizations and the private sector. Additionally, European institutions will have to take the lead in a field that has been addressed only quite recently. However ENISA believes that with a strong involvement of all engaged parties this will be an achievable task.

6 Bibliography

1. **Commission of the European communities.** *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Smart Grids: from innovation to deployment. COM(2011) 202 final.* 2011.

2. *Smart Grids Task force.* [Online] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

3. **Dow Jones & Company, Inc.** *The Wall Street Journal.* [Online] http://europe.wsj.com/home-page.

4. **Commission of the European communities.** *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.* 2006.

5. —. *Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* 2008.

6. —. *Communication from the commission to the European parliament. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* 2009.

7. —. *Communication from the Commission to the European Parliament on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' COM(2011) 163.* 2011.

8. **Giordano, Vincenzo, et al., et al.** *Smart Grid Projects in Europe: lessons learned and current developments.* 2011.

9. **European Network and Informations Security Agency (ENISA).** *Protecting Industrial Control Systems - Recommendations for Europe and Member States.* 2011.

10. **International Society of Automation (ISA).** ISA99 Committee - Home. [Online] http://isa99.isa.org/ISA99 Wiki/Home.aspx.

11. **International Instruments Users' Association (WIB).** *Process control domain - Security requirements for vendors.* EWE (EI, WIB, EXERA). 2010.

12. **National Institute of Standards and Technology (NIST).** *NISTIR 7628: Guidelines for Smart Grid Cyber Security.* Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

13. **European, Commision.** *EPIC - Experimental Platform for Internet Contingencies, [Online: http://sta.jrc.ec.europa.eu/index.php/internet-stability-and-security/201-epic-experimental-platform-for-internet-contingencies].*

14. **European, Commission.** *EU Reference Network for Critical Infrastructural Protection, https://erncip.jrc.ec.europa.eu/.*

15. **IRRIIS Project.** Homepage of the IRRIIS project. [Online] 2006. http://www.irriis.org.

16. **European Commission. Europ2 2020.** *Europe 2020 targets.* [Online] http://ec.europa.eu/europe2020/reaching-the-goals/targets/index_en.htm.

17. *Security of Industrial Control Systems, What to Look For.* **Zwan, Erwin van der.** 2010, ISACA Journal Online.

18. **Zhang, Zhen.** *Smart Grid in America and Europe: Similar Desires, Different Approaches (Part 2). .* 2011.

19. —. *Smart Grid in America and Europe: Similar Desires, Different Approaches (Part 1). .* 2011.

20. **Yin Hong, Chang.** *Cyber Security of a Smart Grid: Vulnerability Assessment.* s.l. : http://www.ece.nus.edu.sg/stfpage/elejp/FYP/CYH09.pdf, 2010.

21. **West, Andrew.** SCADA Communication protocols. [Online] http://www.powertrans.com.au/articles/new pdfs/SCADA PROTOCOLS.pdf.

22. **Weiss, Joseph.** *Protecting Industrial Control Systems from Electronic Threats.* s.l. : Momentum Press, 2010.

23. **Tsang, Rose.** *Cyberthreats, Vulnerabilities and Attacks on SCADA networks.* 2009.

24. **Theriault, Marlene and Heney, William.** *Oracle Security.* First Edition. s.l. : O'Reilly, 1998. p. 446. 1-56592-450-9.

25. **Syngres, Eric Knapp.** *Industrial Network Security. Securing critical infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems. .*

26. **Suter, Manuel and Brunner, Elgin M.** *International CIIP Handbook 2008 / 2009.* 2008.

27. **Stouffer, K. A., Falco, J. A. and Scarfone, K. A.** *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).* s.l. : National Institute of Standards and Technology, 2011.

28. **Snyder, Mike.** *Smart Grid Synergy.* [Online] http://ict2020.tiaonline.org/may_june_2009/policy_stimulus.cfm.

29. **Smith, Steven S.** *The SCADA Security Challenge: The Race Is On.* 2006.

30. *Identifying, understanding, and analyzing Critical Infrastructure Interdependencies.* **Rinaldi, Steven M., Peerenboom, James P. and Kelly, Terrence K.** 2001, IEEE Control Systems Magazine.

31. **Mo, Yilin, et al., et al.** *Cyber–Physical Security of a Smart Grid Infrastructure.* s.l. : http://sparrow.ece.cmu.edu/group/pub/Mo-Kim-etal-ProcIEEE-2011.pdf, 2011.

32. **Masica, Ken.** *Securing WLANs using 802.11i. Draft. Recommended Practice.* 2007.

33. —. *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.* 2007.

34. **Lewis, Adam.** *ERN-CIP: European reference network for critical infrastructure protection.* [Online] http://www.creatif-network.eu/workshop1/Lewis_session3.pdf.

35. **Lenzini, G., Oostdijk, M. and Teeuw, W.** *Trust, Security, and Privacy for the Advanced Metering Infrastructure.* s.l. : https://doc.novay.nl/dsweb/Get/Document-100649, 2009.

36. **Kwasinski, A.** *Implication of Smart-Grids development for communication systems in normal operation and during disasters.* 2010.

37. **Jeff Trandahl, Clerk.** USA Patriot Act (H.R. 3162). [Online] 2001. http://epic.org/privacy/terrorism/hr3162.html.

38. **International Organization for Standardization (ISO), International Electrotechnical Commission (IEC).** *Information technology — Security techniques — Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission. 2005.

39. **Huntington, Guy.** *NERC CIP's and identity management.* Huntington Ventures Ltd. 2009.

40. **Holstein, Dennis Cease, Li, Haiyu L and Meneses, Albertin,.** *The Impact of Implementing Cyber Security Requirements using IEC 61850.* 2010.

41. **Holstein, Dennis K.** *P1711 "The state of closure".* s.l. : PES/PSSC Working Group C6, 2008.

42. **Hayden, Ernie.** *There is No SMART in Smart Grid Without Secure and Reliable Communications.* s.l. : http://www.verizonbusiness.com/resources/whitepapers/wp_no-smart-in-smart-grid-without-secure-comms_en_xg.pdf.

43. **Hart, D.G.** *Using AMI torealize the Smart Grid. En Powerand energy society general meeting -Conversion and delivery of electrical energy in the 21st Century.* s.l. : IEEE 2008, 2008.

44. **Green, Brian D., Cote, J. R. and Simmins, John.** Smartgridinformation.info. [Online] 17 8 2010. [Cited: 30 12 2011.] http://www.smartgridinformation.info/pdf/2663_doc_1.pdf.

45. **Gorman, Siobhan.** *Electricity Grid in U.S. Penetrated By Spies.*

46. **Goméz, J. Antonio.** *III Curso de verano AMETIC-UPM 2011 hacia un mundo digital: las e-TIC motor de los cambios sociales, económicos y culturales.* 2011.

47. **Glöckler, Oszvald.** IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in NPPs. [Online] 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/Day-3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf.

48. **Ginter, Andrew.** *An Analysis of Whitelisting Security Solutions and Their Applicability in Control Systems.* 2010.

49. **Flick, Tony and Morehouse, Justin.** *Securing the Smart Grid. Next Generation Power Grid Security.* 2011.

50. **Fan, Jiyuan and Zhang, Xiaoling.** Feeder Automation within the Scope of Substation Automation. [Online] 10 31, 2006. [Cited: 12 29, 2011.] http://www.ieee.org/portal/cms_docs_pes/pes/subpages/meetings-folder/PSCE/PSCE06/panel24/Panel-24-3_Feeder_Automation.pdf.

51. **Fan, Jiyuan, du Toit, Willem and Backschneider, Paul.** *Distribution Substation Automation in Smart Grid.*

52. **Falliere, Nicolas, Murchu, Liam O and Chien, Eric.** *W32.Stuxnet Dossier.* Symantec. 2011.

53. **Ericsson, Göran.** *Managing Information Security in an Electric Utility.* Cigré Joint Working Group (JWG) D2/B3/C2-01.

54. **Ebinger, Charles and Massy, Kevin.** *Software and hard targets: enhancing Smart Grid cyber security in the age of information warfare.* s.l. : http://www.brookings.edu/~/media/Files/rc/papers/2011/02_smart_grid_ebinger/02_smart_grid_ebinger.pdf, 2011.

55. **Díaz Andrade, Carlos Andrés and Hernandez, Juan Carlos.** *Smart grid: Las TICs y la modernización de las redes de energía eléctrica – Estado del arte.* 2011.

56. **Davis, Mike.** *SmartGrid Device Security. Adventures in a new medium.* s.l. : https://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf, 2009.

57. **Conant, Rob.** *Toward a Global Smart Grid - The U.S. vs. Europe.* [Online] http://www.elp.com/index/display/article-display/2702271845/articles/utility-automation-engineering-td/volume-15/Issue_5/Features/Toward_a_Global_Smart_Grid_-_The_US_vs_Europe.html .

58. —. *Toward a Global Smart Grid - The U.S. vs. Europe.* [Online] http://www.elp.com/index/display/article-display/2702271845/articles/utility-automation-engineering-td/volume-15/Issue_5/Features/Toward_a_Global_Smart_Grid_-_The_US_vs_Europe.html.

59. **Coll-Mayor, Debora.** *Overview of strategies and goals.* [Online] http://www.4thintegrationconference.com/downloads/Strategies & Goals of Smartgrid in Europe.pdf.

60. **Cleveland, Frances.** *White Paper: Cyber Security Issues for the Smart Grid.* s.l. : http://www.xanthus-consulting.com/Publications/White_Paper_Cyber_Security_Issues_for_the_Smart_Grid.pdf, 2009.

61. **Clemente, Jude.** *The Security Vulnerabilities of Smart Grid.* s.l. : http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345, 2009.

62. **Chebbo, Maher.** *Recommendations of the SmartGrid ICT consultation Group to the European Commision.* 2010.

63. **Carpenter, Matthew and Wright, Joshua.** *Advanced metering infrastructure attack methodology.* 2009.

64. **Brodsy, Jacob and McConnell, Anthony.** *Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks.* 2009.

65. **Boyer, Stuart A.** *SCADA: Supervisory Control and Data Acquisition.* Iliad Development Inc., ISA. 2010.

66. —. *SCADA Supervisory and Data Acquisition.* 2004.

67. **Berkeley III, Alfred R. and Wallace, Mike.** *A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council.* s.l. : National Infrastructure Advisory Council, 2010.

68. **Bartels, Guido.** *Combating Smart Grid Vulnerabilities.* s.l. : http://www.ensec.org/index.php?option=com_content&view=article&id=284:combating-smart-grid-vulnerabilities&catid=114:content0211&Itemid=374, 2011.

69. **Bailey, David and Wright, Edwin.** *Practical SCADA for Industry.* s.l. : Newnes, 2003.

70. **Asad, Mohammad.** Challenges of SCADA. [Online] http://www.ceia.seecs.nust.edu.pk/pdfs/Challenges_of_SCADA.pdf.

71. **Anderson, Roger N., et al., et al.** *Computer-Aided Lean Management for the Energy Industry.* 2008.

72. **Amin, Saurabh, Sastry, Shankar and Cárdenas, Alvaro A.** *Research Challenges for the Security of Control Systems.* 2008.

73. **Amin, S. Massoud.** *Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control.* s.l. : http://central.tli.umn.edu/CDC_Semi_plenary_Smart%20Grids_Massoud%20Amin_final.pdf, 2011.

74. **Abbott, Ralph E.** *The Successful AMI Marriage: When Water AMR and Electric AMI Converge.* [Online] http://www.waterworld.com/index/display/article-display/328763/articles/waterworld/volume-24/issue-5/editorial-feature/the-successful-ami-marriage-when-water-amr-and-electric-ami-converge.html.

75. **ZigBee.** ZigBee Home Automation Overview. [Online] http://www.zigbee.org/Standards/ZigBeeHomeAutomation/Overview.aspx.

76. **International Federation of Automatic Control (IFAC).** Working Group 3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/5/4/working-groups/copy2_of_working-group-1-decentralized-control-of-large-scale-systems.

77. **WirelessHART.** *WirelessHART.* [Online] http://www.hartcomm.org/protocol/wihart/wireless_technology.html.

78. **Institute of Electrical and Electronics Engineers (IEEE).** *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

79. —. *WGC1 - Application of Computer-Based Systems.* http://standards.ieee.org/develop/wg/WGC1.html.

80. **Web application Security Consortium.** Web Application Firewall Evaluation Criteria. [Online] 2009. http://projects.webappsec.org/w/page/13246985/Web Application Firewall Evaluation Criteria.

81. **VIKING Project.** Vital Infrastructure, Networks, Information and Control Systems Management. [Online] 2008. http://www.vikingproject.eu.

82. **VDI/VDE.** *VDI/VDE 2182: IT security for industrial automation.* 2011.

83. **United States Computer Emergency Readiness Team (US-CERT).** US-CERT: United States Compueter Emergency readiness Team. [Online] http://www.us-cert.gov.

84. **ISO/IEC.** *UNE-EN 45011: General requirements for bodies operating product certification systems.* 1998.

85. **KEMA and ENA.** UK Smart Grid Cyber Security Report. *http://ses.jrc.ec.europa.eu/.* [Online] 2011. http://energynetworks.squarespace.com/storage/UK Smart Grid Cyber Security Report.pdf.

86. **Institute of Electrical and Electronics Engineers (IEEE).** *Transmission & Distribution Exposition & Conference 2008 IEEE PES : powering toward the future.* Institute of Electrical and Electronics Engineers. 2008.

87. **Pacific Northwest National Labortory, U.S. Department of Energy.** *The Role of Synchronized Wide Area Measurements for Electric Power Grid Operations.* 2006.

88. **EURELECTRIC Networks Committee.** *The Role of Distribution System. Operators (DSOs) as Information Hubs.* 2010.

89. **The 451 Group.** *The adversary: APTs and adaptive persistent adversaries.* 2010.

90. **SANS.** The 2011 Asia Pacific SCADA and Process Control Summit - Event-At-A-Glance. [Online] 2011. http://www.sans.org/sydney-scada-2011.

91. **International Energy Agency (IEA).** *Technology Roadmap. Smart Grids.* France : OCDE/IEA, 2011.

92. **EPRI.** *Technical and System Requirements for Advanced Distribution Automation.* 2004.

93. **International Federation of Automatic Control (IFAC).** TC 6.3. Power Plants and Power Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/6/3.

94. —. TC 3.1. Computers for Control — IFAC TC Websites. [Online] http://tc.ifac-control.org/3/1.

95. **ESCoRTS Project.** *Survey on existing methods, guidelines and procedures.* 2009.

96. **CEN/CENELEC/ETSI Joint Working Group.** *Standards for Smart Grids.* 2011.

97. **European Commission. Directorate-General for Energy.** *Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. M/490.* s.l. : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf.

98. Smart Substations. *Smart Substations:Desing, Operations and Maintenance.* [Online] http://www.smartsubstations.com.au/Event.aspx?id=664622.

99. **EnergieNed.** *Smart Meter Requirements. Dutch Smart Meter specification and tender dossier.* s.l. : http://www.energiened.nl/_upload/bestellingen/publicaties/288_Dutch%20Smart%20Meter%20%20v2.1%20final%20Main.pdf, 2008.

100. **U.S. Department of Energy.** *Smart Grid System Report.* 2009.

101. **Industrial Defender.** *Smart Grid Safety vs Confidentiality.* s.l. : http://blog.industrialdefender.com/?p=756, 2011.

102. **Enerweb.** *Smart grid Information Report.* s.l. : http://enerweb.co.za/brochures/Smart%20Grid%20Information%20Report.pdf, 2011.

103. **IEEE Smart grid.** *Smart Grid Conceptual Model.* [Online] http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model.

104. **Sonoma innovation.** *Smart Grid Communications Architectural Framework.* 2009.

105. **EU Commission Task Force for Smart Grids. Expert Group 4.** *Smart Grid aspects related to Gas.* 2011.

106. **European Commision.** Smart electricity Systems. *European CommisionJoint Research Centre.* [Online] http://ses.jrc.ec.europa.eu/.

107. **Siemens.** Smart Distribution. Distribution Automation and Protection. [Online] [Cited: 29 12 2011.] http://www.energy.siemens.com/fi/en/energy-topics/smart-grid/smart-distribution/distribution-automation-and-protection.htm.

108. **The Climate Group.** *smart 2020: enabling the low carbon economy in the information age.* [Online] 2008.

109. **Treehugger.** *SMART 2020 Report: Smart Grids Can Cut CO2 Emissions by 15 Percent.* [Online] 2011. http://www.treehugger.com/clean-technology/smart-2020-report-smart-grids-can-cut-co2-emissions-by-15-percent.html.

110. **smart 2020.** *Smart 2020 .* [Online] 2009. http://www.smart2020.org/.

111. **Smart Grid Interoperability Panel (SGIP).** SGIP Cyber Security Working Group (SGIP CSWG). [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

112. **The AMI-SEC Task Force (UCAIug) and The NIST Cyber Security Coordination Task Group.** *SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE.* 2010.

113. **ESCoRTS Project.** Security of Control and Real Time Systems. [Online] 2008. http://www.escortsproject.eu.

114. **ABB.** *Security in the smart grid.* s.l. : http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf, 2009.

115. **American Petroleum Institute (API) energy.** *Security Guidelines for the Petroleum Industry.* American Petroleum Institute. 2005.

116. **Technical Support Working Group (TSWG).** *Securing Your SCADA and Industrial Control Systems.* Departmet of Homeland Security. 2005.

117. **Rijksoverheid.** Scenario's Nationale Risicobeoordeling 2008/2009. [Online] 2009. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/21/scenario-s-nationale-risicobeoordeling-2008-2009.html.

118. **SANS.** SCADA Security Advanced Training. [Online] 1989. http://www.sans.org/security-training/scada-security-advanced-training-1457-mid.

119. **Water Sector Coordinating Council Cyber Security Working Group.** Roadmap to Secure Control Systems in the Water Sector. 2008.

120. **RISI.** *Repository of Industrial Security Incidents.* [Online] http://www.securityincidents.org/.

121. **United States Nuclear Regulatory Commission.** *Regulatory Guide 5.71: Cyber security programs for nuclear facilities.* 2010.

122. **Department of Homeland Security (DHS).** Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. 2009.

123. **Wikipedia.** Recloser. [Online] [Cited: 12 26, 2011.] http://en.wikipedia.org/wiki/Recloser.

124. **Iberdrola.** Proyecto tipo para Centro de Transformación intemperie compacto. [En línea] Abril de 1997. [Citado el: 29 de Diciembre de 2011.] http://www.coitiab.es/reglamentos/electricidad/reglamentos/jccm/iberdrola/mt_2-11-05.htm.

125. **Centre for the Protection of National Infrastructure (CPNI).** *Process control and SCADA security. Guide 7. Establish ongoing governance.* Centre for the Protection of National Infrastructure.

126. —. *Process control and SCADA security. Guide 6. Engage projects.* Centre for the Protection of National Infrastructure.

127. —. *Process control and SCADA security. Guide 5. Manage third party risk.* Centre for the Protection of National Infrastructure.

128. —. *Process control and SCADA security. Guide 4. Improve awareness and skills.* Centre for the Protection of National Infrastructure.

129. —. *Process control and SCADA security. Guide 3. Establish response capabilities.* Centre for the Protection of National Infrastructure.

130. —. *Process control and SCADA security. Guide 2. Implement secure architecture.* Centre for the Protection of National Infrastructure.

131. —. *Process control and SCADA security. Guide 1. Understand the business risk.* Centre for the Protection of National Infrastructure.

132. —. *Process control and SCADA security.* Centre for the Protection of National Infrastructure.

133. **Institute of Electrical and Electronics Engineers (IEEE).** *P2030: IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.* 2011.

134. **Wikipedia.** *Outage management system.* [Online] http://en.wikipedia.org/wiki/Outage_management_system.

135. **Open Smart Grid.** Open Smart Grid. [Online] http://osgug.ucaiug.org/default.aspx.

136. **OpenSG.** Open Smart Grid. *http://osgug.ucaiug.org.* [Online]

137. **Norwegian Oil Industry Association (OLF).** *OLF Guideline No.110: Implementation of information security in PCSS/ICT systems during the engineering, procurement and commissioning phases.* Norwegian Oil Industry Association. 2006.

138. —. *OLF Guideline No. 104: Information Security Baseline Requirements for Process.* Norwegian Oil Industry Association. 2006.

139. **National Institute of Standards and Technology (NIST).** *NISTIR 7176: System Protection Profile - Industrial Control Systems.* Decisive Analytics. 2004.

140. —. *NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology. 2011.

141. —. *NIST SP 800-53: Information Security.* National Institute of Standards and Technology. 2009.

142. —. *NIST SP 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* 2010.

143. **The White House.** National Strategy for Information Sharing. [Online] 2007. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

144. **Department of Homeland Security (DHS).** *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Department of Homeland Security. 2009.

145. **NAMUR.** *NAMUR NA 115 IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries.* 2006.

146. **Centre for the Protection of Critial Infrastructure (CPNI).** Meridian Process Control Security Information Exchange (MPCSIE). [Online] http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie.

147. **Meridian.** Meridian. [Online] http://www.meridian2007.org.

148. **European Commision.** *M/441:* . http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf : s.n., 2009.

149. **International Society of Automation (ISA).** LISTSERV 15.5 - ISA67-16WG5. [Online] http://www.isa-online.org/cgi-bin/wa.exe?A0=ISA67-16WG5.

150. **International Electrotechnical Commission (IEC).** *ISO/IEC 15408: Information technology. Security techniques. Evaluation criteria for IT security.* 2009-2011.

151. **International Society of Automation (ISA).** *ISA100, Wireless Systems for Automation.* [Online] www.isa.org/isa100.

152. **INTERSECTION Project.** INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks (INTERSECTION). [Online] 2008. http://www.intersection-project.eu.

153. **European Network and Informations Security Agency (ENISA).** *Information Security Certifications. A Primer: Products, people, processes.* s.l. : http://www.epractice.eu/files/media/media1872.pdf, 2007.

154. **Norwegian Oil Industry Association (OLF).** *Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems.* Norwegian Oil Industry Association. 2009.

155. **INSPIRE Project.** INcreasing Security and Protection through Infrastructure REsilience. [Online] 2008. http://www.inspire-strep.eu.

156. **International Federation for Information Processing (IFIP).** IFIP WG 1.7 Home Page. [Online] http://www.dsi.unive.it/~focardi/IFIPWG1_7.

157. —. IFIP Technical Committees. [Online] http://ifiptc.org/?tc=tc11.

158. —. IFIP TC 8 International Workshop on Information Systems Security Research. [Online] http://ifip.byu.edu.

159. **Institute of Electrical and Electronics Engineers (IEEE).** *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.* 2007.

160. —. *IEEE Standard C37.1-1994: Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.* Institute of Electrical and Electronics Engineers. 1994.

161. —. IEEE Power & Energy Society. [Online] http://www.ieee-pes.org.

162. —. IEEE PES Computer and Analytical Methods SubCommittee. [Online] 2000. http://ewh.ieee.org/cmte/psace/CAMS_taskforce.html.

163. **International Electrotechnical Commission (IEC).** *IEC TS 62351-7: Power systems management and associated information exchange – Data and communications security. Part 7: Network and system management (NSM) data object models.* International Electrotechnical Commission. 2010.

164. —. *IEC TS 62351-6: Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850.* International Electrotechnical Commission. 2007.

165. —. *IEC TS 62351-5: Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives.* International Electrotechnical Commission. 2009.

166. —. *IEC TS 62351-4: Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS.* International Electrotechnical Commission. 2007.

167. —. *IEC TS 62351-3: Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP.* International Electrotechnical Commission. 2007.

168. —. *IEC TS 62351-2: Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms.* International Electrotechnical Commission. 2008.

169. —. *IEC TS 62351-1: Power systems management and associated information exchange – Data and communications security. Part 1: Communication network and system security – Introduction to security issues.* International Electrotechnical Commission. 2007.

170. —. *IEC TR 62210: Power system control and associated communications – Data and communication security.* 2003-05.

171. —. *IEC 62443: Security for Industrial Process Measurement and Control: Network and System Security.* 2010.

172. —. *IEC 61970: Common Information Model (CIM) / Energy Management.*

173. —. *IEC 61968: Common Information Model (CIM) / Distribution Management.*

174. —. *IEC 61850-7-2: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI).* International Electrotechnical Commission. 2010.

175. —. *IEC 61850: Communication networks and systems in substations.* 2011.

176. —. *IEC 60870-6: Telecontrol equipment and systems.* 2005.

177. —. *IEC 60870-5: Telecontrol equipment and system.* 2007.

178. **ICT4SMARTDG.** *ICT Solutions to enable Smart Distributed Generation.* 2011.

179. **International Atomic Energy Agency (IAEA).** IAEA Technical Meeting on Newly Arising Threats in Cybersecurity of Nuclear Facilities. [Online] 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/files/InfoSheet-CybersecurityTM-May-2011.pdf.

180. **Energie Vortex.** *http://www.energyvortex.com.* [Online] http://www.energyvortex.com/energydictionary/blackout__brownout__brown_power__rolling_blackout.html.

181. **Department of Homeland Security (DHS).** Homeland Security Presidential Directive-7. [Online] 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

182. **Department of Energy (DoE).** Hands-on Control Systems Cyber Security Training of National SCADA Test Bed. [Online] 2008. http://www.inl.gov/scada/training/d/8hr_intermediate_handson_hstb.pdf.

183. **BBC news.** *Hackers 'hit' US water treatment systems.* s.l. : http://www.bbc.co.uk/news/technology-15817335, 2011.

184. **Swedish Civil Contingencies Agency (MSB).** *Guide to Increased Security in Industrial Control Systems.* Swedish Civil Contingencies Agency. 2010.

185. **Commission of the European communities.** *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.* 2005.

186. **National Infrastructure Security Coordination Centre (NISCC).** *Good Practice Guide Process Control and SCADA Security.* PA Consulting Group. 2006.

187. —. *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* British Columbia Institute of Technology (BCIT). 2005.

188. **McAfee.** Global Energy Cyberattacks: “Night Dragon”. [Online] 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

189. **National Infrastructure Security Coordination Centre (NISCC).** *Firewall deployment for scada and process control networks. good practice guide.* National Infrastructure Security Coordination Centre. 2005.

190. **Centre for the Protection of National Infrastructure (CPNI).** *Firewall deployment for scada and process control networks.* Centre for the Protection of National Infrastructure. 2005.

191. **National Institute of Standards and Technology (NIST).** FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems.* [Online] 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

192. —. *Field Device Protection Profile for SCADA Systems in Medium Robustness Environments.* 2006.

193. **EU Commission Task Force for Smart Grids.** *Expert Group 1: Functionalities of smart grids and smart meters.* 2010.

194. **The White House.** Executive Order 13231. [Online] 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

195. *Eur Lex.* [Online] http://eur-lex.europa.eu/en/index.htm.

196. **European Network and Informations Security Agency (ENISA).** *EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection.* [Online] 2010. http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1.

197. **Instituto de Investigaciones Eléctricas de México.** *Estado del arte en Redes Inteligentes "Smart Grids". Automatización de la Distribución en las Redes Inteligentes.* México : s.n.

198. **eSEC.** eSEC. *Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza.* [Online] http://www.idi.aetic.es/esec.

199. **Energie.gov.** *Energy Storage.* [Online] http://energy.gov/oe/technology-development/energy-storage.

200. **Department of Energy (DoE).** *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities.* Department of Energy. 2002.

201. *Energy Independence and Security Act of 2007.* s.l. : http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf, 2007.

202. **Energiened.** Energiened Documentation. [Online] http://www.energiened.nl/Content/Publications/Publications.aspx.

203. **U.S. Department of Energy.** *Electricity sector cyber-security risk management process guideline.* 2011.

204. **Government Accountability Office (GAO).** *Electricity grid modernization. Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed.* s.l. : http://www.gao.gov/new.items/d11117.pdf, 2011.

205. **Institute of Electrical and Electronics Engineers (IEEE).** *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

206. **Smarter Grid Solutions.** *Dynamic Line Rating - managing capacity.* [Online] http://www.smartergridsolutions.com/index.html?pid=153.

207. **National Institute of Standards and Technology (NIST).** *Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.* 2011.

208. **DLMS User Association.** *DLMS/COSEM: Conformance Testing Process.* 2010.

209. —. *DLMS/COSEM: Architecture and Protocols.* 2009.

210. **Wikipedia.** *Distribution mangagement system.* [Online] http://en.wikipedia.org/wiki/Distribution_mangagement_system.

211. **Commission of the European communities.** *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* 1995.

212. **DigitalBond.** DigitalBond. *ICS Security Tool Mail List.* [Online] http://www.digitalbond.com/tools/ics-security-tool-mail-list.

213. **Department of Homeland Security (DHS).** DHS officials: Stuxnet can morph into new threat. [Online] 2011. http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat.

214. **Department of Energy (DoE).** Cybersecurity for Energy Delivery Systems Peer Review. [Online] 2010. http://events.energetics.com/CSEDSPeerReview2010.

215. **Department of Homeland Security (DHS).** *Cyber storm III Final Report.* Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division. 2011.

216. **Centre for the Protection of National Infrastructure (CPNI).** *Cyber security assessments of industrial control systems.* Centre for the Protection of National Infrastructure. 2011.

217. **CRUTIAL Project.** CRitical Utility InfrastructurAL resilience. [Online] 2006. http://crutial.rse-web.it.

218. **Thales.** *Critical Infrastructure Security. A Holistic Security Risk Management Approach.* s.l. : http://www.securitymanagement.com.au/content/file/CriticalISThales.pdf?asm=ad05637d37e2a8c1afeeda016804c85, 2008.

219. **United States General Accounting Office (GAO).** *Critical infrastructure protection. Challenges and Efforts to Secure Control Systems.* United States General Accounting Office. 2004.

220. **CI2RCO Project.** Critical information infrastructure research coordination. [Online] 2008. http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=79305.

221. **SINTEF.** *CRIOP: A scenario method for Crisis Intervention and Operability analysis.* 2011.

222. **Centre for the Protection of Critical Infrastructure (CPNI).** CPNI. [Online] http://www.cpni.gov.uk/advice/infosec/business-systems/scada.

223. *Council decision on a Critical Infrastructure Warning Information Network (CIWIN) COM(2008) 676».* **Commission of the European communities.** 2008.

224. **DLMS User Association.** *COSEM: Identification System and Interface Classes.* 2010.

225. —. *COSEM: Glossary of Terms.* 2003.

226. **Department of Energy (DoE).** Control Systems Security Publications Library. [Online] http://energy.gov/oe/control-systems-security-publications-library.

227. **United States Computer Emergency Readiness Team (US-CERT).** Control Systems Security Program: Industrial Control Systems Joint Working Group. [Online] http://www.us-cert.gov/control_systems/icsjwg/index.html.

228. —. Control Systems Security Program: Industrial Control Systems Cyber Emergency Response Team. [Online] http://www.us-cert.gov/control_systems/ics-cert/.

229. **Interstate Natural Gas Association of America (INGAA).** *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry.* Interstate Natural Gas Association of America. 2011.

230. **ICT4SMARTDG.** *Consensus on ICT solutions for a Smart Distribution at Domestic Level.* 2011.

231. **Centre for the Protection of National Infrastructure (CPNI).** *Configuring & managing remote access for industrial control systems.* Centre for the Protection of National Infrastructure. 2011.

232. **Commission of the European communities.** *Communication from the commission. Energy infrastructure priorities for 2020 and beyond – A Blueprint for an integrated European energy network. COM(2010) 677.* 2010.

233. —. *Communication from the commission to the European parliament, the European economic and social commitee and the commitee of the regions. Achievements and next steps: towards global cyber-security.* 2011.

234. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions: A Digital Agenda for Europe. COM(2010)245 final.* 2010.

235. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Energy 2020: A strategy for competitive, sustainable and secure energy. COM(2010) 639 final.* 2010.

236. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Digital Agenda for Europe. COM(2010) 245.* 2010.

237. —. *Communication from the commission to the council, the European parliament, the European economic and social commitee and the commitee of the regions. A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment' COM(2006) 251.* 2006.

238. —. *Communication from the commission to the council and the European parliament. Prevention, preparedness and response to terrorist attacks COM(2004) 698 final.* 2004.

239. —. *Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final.* 2004.

240. **North American Electric Reliability Corporation (NERC).** *CIP-009-4: Cyber Security — Recovery Plans for Critical Cyber Assets.* North American Electric Reliability Corporation (NERC). 2011.

241. —. *CIP-008-4: Cyber Security — Incident Reporting and Response Planning.* North American Electric Reliability Corporation. 2011.

242. —. *CIP-007-4: Cyber Security — Systems Security Management.* North American Electric Reliability Corporation. 2011.

243. —. *CIP-006-4: Cyber Security — Physical Security.* North American Electric Reliability Corporation. 2011.

244. —. *CIP-005-4: Cyber Security — Electronic Security Perimeter(s).* North American Electric Reliability Corporation. 2011.

245. —. *CIP-004-4: Cyber Security — Personnel and Training.* North American Electric Reliability Corporation. 2011.

246. —. *CIP-003-4: Cyber Security — Security Management Controls.* North American Electric Reliability Corporation. 2011.

247. —. *CIP-002-4: Cyber Security — Critical Cyber Asset Identification.* North American Electric Reliability Corporation. 2011.

248. —. *CIP-001-1a: Sabotage Reporting.* North American Electric Reliability Corporation. 2010.

249. —. *Categorizing Cyber Systems. An Approach Based on BES Reliability Functions. Cyber Security Standards Drafting Team for Project 2008-06 Cyber Security Order 706.* 2009.

250. **Department of Homeland Security (DHS).** *Catalog of Control Systems Security: Recommendations for Standards Developers.* 2009.

251. **Council of the European Union.** *Brussels European Council 8/9 march 2007. Presidency conclusions.* 2007.

252. **Power Systems Engineering Research Center.** *Automated Circuit Breaker Monitoring.* 2007.

253. **Gartner.** Assessing the Security Risks of Cloud Computing. *Gartner.* [Online] 2008. http://www.gartner.com/DisplayDocument?id=685308.

254. **American Petroleum Institute (API) energy.** *API Standard 1164. Pipeline SCADA Security.* American Petroleum Institute. 2009.

255. **American National Standard (ANSI).** *ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems.* International Society of Automation (ISA). 2007.

256. —. *ANSI/ISA–99.02.01–2009 Security for Industrial Automation and Control Systems. Part 2: Establishing an Industrial Automation and Control Systems Security Program.* International Society of Automation (ISA). 2009.

257. —. *ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models.* International Society of Automation (ISA). 2007.

258. —. *ANSI C12.21: American National Standard for Protocol Specification for Telephone Modem Communication.* 2006.

259. —. *ANSI C12.19: American National Standard for Utility Industry End Device Data Tables.* 2008.

260. —. *ANSI C12.18: American National Standard for Protocol Specification for ANSI Type 2 Optical Port.* 2006.

261. **AMI-SEC-ASAP.** *AMI System Security Requirements.* 2008.

262. —. *AMI Security Implementation Guide.* 2009.

263. **American Gas Association (AGA).** *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 2 Performance Test Plan.* American Gas Association. 2006.

264. —. *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 1 Background, policies and test plan.* American Gas Association. 2006.

265. **Wikipedia.** Advanced Distribution Automation. [Online] [Cited: 02 01 2012.] http://en.wikipedia.org/wiki/Advanced_Distribution_Automation.

266. **IBM Global Services.** *A Strategic Approach to Protecting SCADA and Process Control Systems.* 2007.

267. **Europe 2020.** *A resource-efficient Europe – Flagship initiative of the Europe 2020 Strategy.* [Online] http://ec.europa.eu/resource-efficient-europe/index_en.htm.

268. **EOS Energy Infrastructure Protection & Resilience Working Group.** *A global european approach for energy infrastructure protection & resilience.* s.l. : http://www.eos-eu.com/LinkClick.aspx?fileticket=DEvuI/4l1jU=&tabid=232, 2009.

269. **Department of Energy (DoE).** *21 Steps to Improve Cyber Security of SCADA Networks.* Department of Energy.

270. ENERGY.GOV - Office of Electricity Delivery & Energy Reliability. *National SCADA Test Bed.* [Online] [Cited: 29 03 2012.] http://energy.gov/oe/national-scada-test-bed.

271. *Power Blackout Risks. Risk Management Options. Emerging Risk Initiative - Position Paper.* **CRO FORUM.** 2011.

7 Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
ADA	Advanced Distribution Automation
AMI	Advanced Metering Infrastructure
AMR/AMM	Advanced Metering Reading/Measures
ANSI	American National Standards Institute
AoR	Assessment of the Resilience
BAN	Building Area Networks
BPL	Broadband over power line
C&DM	Control & Data Management
CC	Common Criteria
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEO	Chief Executive Officer
CERT	Centre Emergency Response Team
CIA	Confidentially, Integrity and Availability
CIWIN	Critical Infrastructure Warning Information Network
C-level	Chief level (CEO, CIO, ...)
CO2	Carbon dioxide
COTS	Commercial of the Self
CS	Control Systems
CZ	Czech Republic
DAE	Digital Agenda for Europe
DCA	Distribution Contingency Analysis
DE	Germany
DER	Distributed Energy Resources
DG ENER	Directorate-General for Energy
DK	Denmark
DLF/DLE	Distribution Load Forecasting and Estimation
DLMS/COSEM	Device Language Message specification/COmpanion Specification for Energy Metering
DLR	Dynamic Line Ratings
DMS	Distribution Management System
DoS	Denial of Service
DPF	Distribution Power Flow
DSE	Distribution State Estimation
DSM	Demand Side Management
DSO	Distribution System Operators
EACI	European Association for Creativity and Innovation

EC	European Commission
ECI	European Critical Infrastructures
EG	Expert Group
EII	European Industrial Initiatives
EISAS	European Information Sharing and Alert System
EL	Greek
EMS	Energy Management System
ENISA	European Network and Information Security Agency
ENTSO	European Network of Transmission System Operators for Electricity
EP3R	European Public Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
ES	Spain
ESI	Energy service interface
ETN	Electrical Transmission Network
ETP	Executive Training Programme
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
FAN	Field Area Network
FDIR	Fault Detection Isolation and Restoration
FP7	Framework Programme 7
FTP	File Transfer Protocol
GDP	Gross domestic product
GHG	Greenhouse Gas
GIS	Geographic Information System
GPRS	General Packet Radio Service
HAN	Home Area Network
HMI	Human Machine Interface
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVDC	High-Voltage Direct Current
HW	Hardware
IAC	Integrity, Availability, Confidentiality
IAN	Industrial Area Networks
ICS	Industrial Control Systems
ICT	Information and communications technology
IE	Information Exchange
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IoE	Internet of Energy
IPS/IDS	Intrusion Protection/Detection System
IP-Sec	Internet Protocol Secure
ISA	International Society of Automation
ISM	Information Security Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
IST	Information Society Technologies
IT	Information Technology
IT	Italy
IVVC	Integrated Voltage/Var Control
JHA	Justice and Home Affairs
JRC	Joint Research Center
JWG	Joint Working Group
KF	Key Finding
LAN	Local Area Network
LV	Low Voltage
MAN	Metropolitan Area Network
MDMS	Meter data management system
MID	Measuring Instruments Directive
MPLS	Multiprotocol Label Switching
MS	Member State
MV	Medium Voltage
NAN	Neighbourhood Area Network
NCA	National Certification Authorities
NCI	National Critical Infrastructures
NERC	North American Electric Reliability Corporation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NL	Nederland
NO	Norway
NRA	National Regulatory Authorities
OFC	Optimal Feeder Configuration
OFDM	Orthogonal Frequency Division Multiplexing
OMS	Outage Management System
OWASP	Open Web Application Security Project
PCD	Process Control Domain
PLC	Power Line Communications

PMU	Phasor Measurement Units
PP	Protection Profiles
QoS	Quality of Service
R&D	Research and Development
RBAC	Role Based Access Control
RF	Radio Frequency
RISI	Repository of Industrial Security Incidents
RMP	Risk Management Process
RTD	Research and Technology Development
RTP	Real-Time Pricing
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SES	Smart Electricity System
SFTP	Secure File Transfer Protocol
SG	Smart Grid
SGIS	Smart Grid Information Security
SIEM	Security information and event management
SL	Slovenia
SMART	Standardization, Monitoring, Accounting, Rethink, Transformation
SOC	Security Operations Centre
SSH	Secure Shell
ST	Security Targets
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunications Network
TF	Task Force
TOE	Target of Evaluation
TP	Topology Processor
TSO	Transmission System Operators
UK	United Kingdom
USA/US	United States of America
USB	Universal Serial Bus
VPN	Virtual Private Network
WAAPCA	Wide-Area Adaptive Protection, Control and Automation
WAMS	Wide Area Monitoring System
WAN	Wide Area Networks
WASA	Wide-Area Situational Awareness
WG	Working Group
WMD	Weapon of Mass Destruction

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