Smart Grid Security

Annex III. Survey and interview analysis

[Deliverable – 2012-11-27]

This document is Annex 3 (of 5) to the ENISA study 'Smart Grid Security: Recommendations for Europe and Member States, June 2012'.

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, S21sec.

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 expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For contacting ENISA or for general enquiries on CIIP & Resilience and, 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

Contents

List of figures

1 The approach

The study comprised two main phases. The first phase, 'stock-taking', was intended to gather all the data that will make up the work base for the study and divided in three main activities: desktop research, poll and interviews. During the desktop research more than 230 documents have been analysed including high reputational publications (i.e. technical reports, specialised books, good practices, standards, papers), other technical documents like whitepapers, product/services and sheets and latest news i.e. forums, mailing lists, twitter, blogs.

Over 304 experts were contacted for the study of which 50 participated in the poll. The experts were divided in categories such as:

- 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

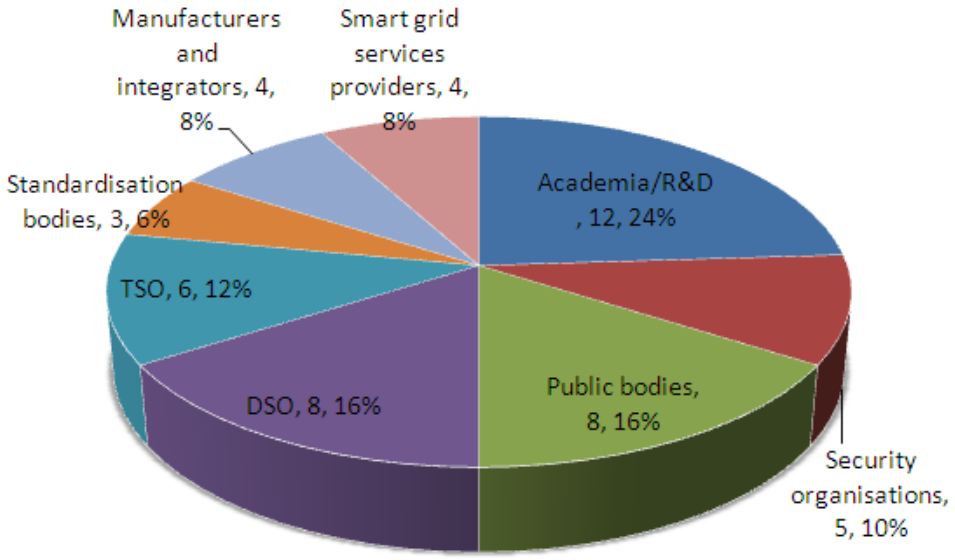

Figure 1: Categories of contacted stakeholders participated in the poll

Twenty three experts were interviewed. Experts participating in the interviews were enquired about topics such as:

- The importance of cyber security in the smart grid business case
- Smart grid pilots, and in particular on the how cyber security is being addressed
- Risk assessments, including new threats, interdependencies, the role of ICT, etc.
- Basic components of the smart grid, including infrastructures and services
- Knowledge on existing initiatives (i.e. R&D projects, information sharing platforms, working groups, etc.) and on how to improve them
- The impact of the Smart Grid Task Force EG2's report about "Regulatory recommendations for data safety, data handling and data protection"
- Main cyber security challenges of the smart grid
- The importance of technology, processes and people for making the smart grid secure
- How to measure the effectiveness of cyber security controls
- How to deal with pan-European cyber attacks and the role of CERTs in such scenarios

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. Finally, ENISA organised a validation workshop on 29th of February 2012 where the report was presented and the experts had the opportunity to validate the results of the study.

2 The smart grid business case and the importance of cyber security

Several topics on the smart grid business case are discussed in this section. Firstly the main drivers behind the adoption of the smart grid are analysed by the experts of the study. Secondly, this chapter presents a review on which could be the factors for the success of the future grid. Finally, thoughts about the importance of cyber security and privacy in the future smart grid have been structured for an easy comprehension by the reader.

2.1 Main drivers for the smart grid business case

It is interesting to see that a majority of respondents consider reliability and resiliency as well as optimization and efficiency (also mentioned as cost reductions) of the power grid as key factors driving the smart grids business case. In relation to having a reliable and resilient grid, several experts referred to the Fukushima disaster to illustrate the importance of these two factors.

There was also a high level of agreement on how important smart grids are for achieving a scalable power grid, and referred to "distributed energy generation" and specifically to customers becoming electricity producers – not only consumers, a new role which is normally called "prosumers" – as an essential aspect for grid scalability.

Additionally, some experts also provided ecological/environmental arguments (e.g. greenhouse gas emission reduction) as important reasons behind the smart grid business case. In particular they consider that an efficient and well-managed integration of renewable energy sources in the grid, as well as the incorporation of the Electric Vehicle (EV), will be essential – but not sufficient, since grid efficiency and optimization are also key factors – to achieve these goals.

Several experts also referred to the new added-value services for consumers and to a better management as other reasons supporting the smart grid business case.

To this regard, all stakeholders agree that the smart grid business case is being pushed – by companies and/or governments – to the market instead of growing from a need for better services for consumers. According to them, this is happening for a number of different reasons already mentioned (e.g. 20-20-20 objectives, new business opportunities, grid efficiency, etc.). Moreover, some experts stated that customers are not directly demanding smart grids, because they are not aware about what it is and how they can benefit from its implementation.

2.2 Factors of success in the adoption of the smart grid

Most of the experts also provided their point of view on those factors which they consider of major importance for the adoption of the smart grid.

- **Definition of the smart grid concept:** an agreement on a common definition of what the smart grid is and how to implement it is considered a relevant factor of success.

- **Economical reasons:** energy fraud prevention and costs reduction are considered important mainly by security providers, DSOs and TSOs. However, there is a body of opinion among some of the respondents which argues that there is no real evidence that the smart grid adoption will lead to lower the price of the electric service to the final consumer.
- **Homeland security:** it is largely agreed that homeland security will be as relevant as the economical motive for a successful adoption of the smart grid, with a total agreement among the experts belonging to public bodies and academia/R&D. It is interesting to highlight that respondents showed no agreement regarding which, privacy or homeland security/cyber-security, are more relevant. Nevertheless, most of them accepted that they are absolutely related.
- **Customer privacy issues:** privacy issues affecting consumers are mainly considered by academia and R&D experts and public bodies, but also by DSOs and security providers, as an important success factor. They consider it necessary to guarantee user acceptance, especially regarding smart metering and the added-value services[2] that might be available in the future. They think that this is a cultural issue, that might be not so important outside the EU, but which is critical in many member states (MS). In fact, some public bodies and companies think that reasonable efforts are being made already (i.e. in The Netherlands or Nordic countries). Finally, it is interesting to highlight that some experts declared that, for providing some of the so-called added-value services, user profiling is of paramount importance (e.g. to guarantee and efficient energy provisioning), but at the same time it can collide with privacy and safety requirements.
- **Customer awareness and education:** some experts explicitly state that in order to foster customer acceptance, they have to be informed about the benefits of the smart grid (e.g. advantages of being a prosumer, modernisation of the grid, etc.). Most of the initiatives on this topic are related to privacy problems, and mostly led by consumer organizations. Additionally, the current power quality and security of supply, which are key aspects on customer satisfaction, are considered by European customers to be at the top level. There are only some complaints regarding cost increases, but users have an overall satisfaction on the service. Therefore, actions on customer awareness/education have to deal with these facts when trying to educate the consumer on the benefits of the smart grids.
- **Smart meters acceptance:** a small number of respondents expressed concerns regarding how smart meters would be paid and/or financed, as providers are finding difficulties to convince final customers to be the ones assuming it. Moreover, to achieve smart meters acceptance, customer awareness and education is essential. Some respondents explained the UK's case of success. The UK's Government decided

[2] *A few predict that some value-added services will emerge in the future, such as energy-comparison web-sites, efficiency advice for home energy management, or even energy management through smart appliances. They could be brought up by new companies or even energy marketers.*

that the smart meters roll-out had is led by energy suppliers instead of DSOs. Energy suppliers are the ones working on the new added-value services for consumers, and are keener to better explain its benefits on energy efficiency and savings.

2.3 The importance of privacy and cyber security

Acknowledging that both, cyber security and privacy, are key factors for making the smart grid a success, the experts participating in the study also provided the following appreciations on these two topics:

- A slight majority of experts think that not enough attention is being paid to cyber security and data privacy, as it is exemplified by current smart grid pilots which are focusing on other functionalities.
- Moreover, from a technical point of view, many vendors and security providers say that this issue is not being addressed appropriately. They consider that cyber security and privacy should be addressed already at the design phase, because leaving it for later will raise the associated costs.
- On the other hand, several experts stated that attention to cyber security is increasing in Europe and that this tendency will continue in the following years.
- A R&D interviewee declared that for the upcoming years, technology sophistication will lead to greater security needs.
- Some experts expressed their doubts regarding the importance of security and data privacy, especially considering that there is no objective data available or even a clear description on how the smart grid architecture will be in technically implemented.
- Regarding to the previous point, other experts also stated that prior to security and privacy, primary concepts of the smart grid (i.e. architecture, objectives, functionalities, services, etc.) need to be well addressed.
- A few experts also declared that the cost aspect of cyber security is not high when compared with all the rest, and at the same time its benefits are really high.

3 Smart grid test pilots and the role of cyber security at this phase

When asked for familiarity of projects that are being carried out worldwide on smart grids technology, a majority of experts confirmed the knowledge of various pilots related to different domains of the smart grids, as it can be seen from the diagram below.

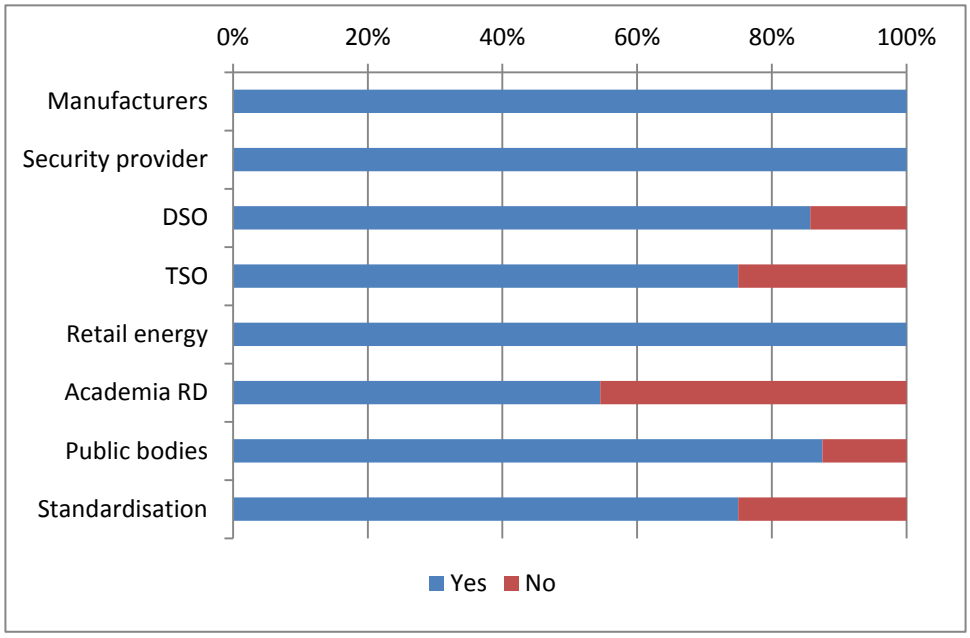

Figure 1 Percentage of respondents which are aware of existing pilots

Several experts declared they knew about the different projects because they have, to some extent, participated in at least one of these projects. However, most of them seem to simply know basic data about the pilots, gathered either through informal communications or from the pilot's website itself. Additionally, various experts also referred us to the Joint Research Centre (JRC) document [101], to inform us about the different projects that are being carried out in Europe. This document shows the development status of smart grids in Europe as a basis for discussion among the stakeholders and to promote the sharing of knowledge, experiences and best practices. However, it is interesting to highlight two relevant aspects. The first one is that the great majority of the experts know who is leading the pilots they know about. The second one is that several experts consider that the US is more active and advanced in what refers to smart grid pilots. Finally, we can say there is a lack of global perspective on the projects, resulting on each expert only knowing about those projects related to the topics of their interest.

Based on the answers to the questionnaire as well as on the interviews carried out, it could be stated that, in general terms, pilots are not considering cyber security at all (with very few

exceptions). Moreover, it can also be said that in those projects described by the stakeholders, there is a lack of security measures. Additionally, many of the projects they know about are at an early stage. Some experts declared that this the reason why pilots are focusing on testing smart grid applications and functionalities, which are considered essential, and not on cyber security which is considered a second line issue. The general opinion is that 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, pipelines, and lack of expertise, etc. An expert also stated that it would have been more rigorous to also test these important aspects during the pilot phase, to effectively check that the security aspects considered during the design phase were effective. We consider this a very important issue since there are contradictory points of view on what refers to considering cyber security at the design phase. There are experts who think that during this phase, both at the architectural and device levels, cyber security and privacy has been adequately considered. On the other hand there are also experts who stated that security has been considered as an overlay more than a very integral part of the design phase. Finally, it is important to highlight that some experts declared that cyber security and privacy are taken into account seriously once they start massive deployments, as it is happening already in the smart meters roll-out.

The complete list of pilots identified by the experts is included in Annex V. This list has been completed with a number of pilots identified during the desktop research phase.

4 Risk assessments considering ICT risks

This section details the knowledge of the experts with regards to the existence of risk assessments initiatives in the field of smart grids. Additionally, interesting opinions on how to address the protection of smart grids based on a risk-driven approach are also presented in combination with other interesting thoughts about risk assessments methodologies, strategies, etc.

4.1 Knowledge of risk assessment initiatives

In general terms, a wide majority of the stakeholders is aware of at least one specific project (either in their own companies or in other organisations) related to cyber security risks assessments for the smart grid. On the following chart, this information is presented by stakeholder type.

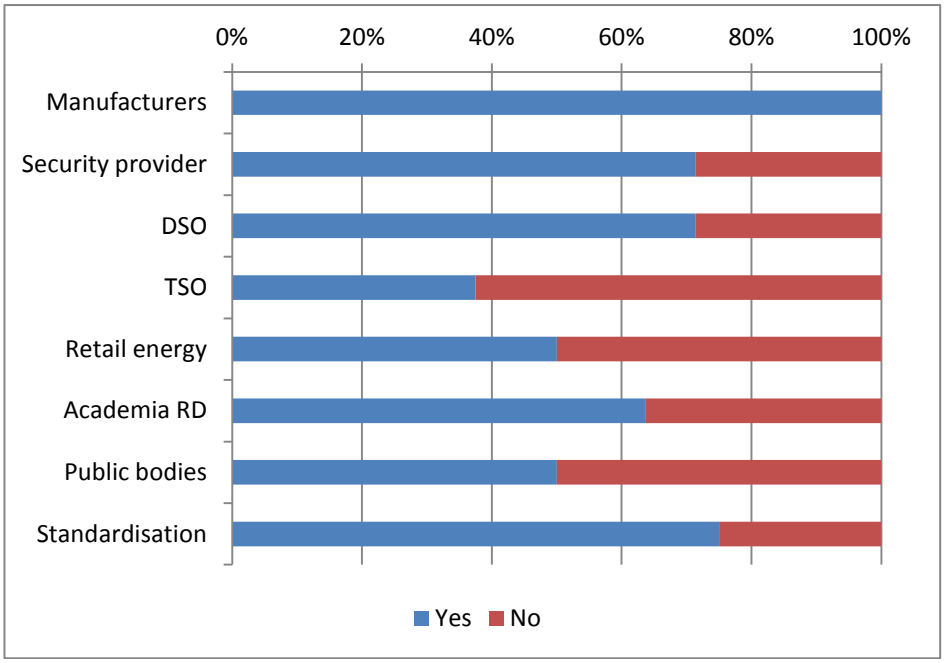

Figure 2 Percentage of respondents which are aware of existing risk assessment initiatives

The chart shows that all those experts belonging to the manufacturers (100%) stakeholder type are aware of initiatives related to cyber security risks assessments. On the opposite side we have TSOs. Surprisingly TSOs have the lowest knowledge (39%) about this kind of projects.

4.2 The best known initiatives on cyber security risk assessments

The experts who were aware of initiatives on cyber security risk assessments were asked to list and briefly describe them. As the reader will notice from the following list, experts provided a rich and varied spectrum of initiatives, which include specific projects, organizations and task forces addressing the topic, guidelines and articles, tools, etc., all of which are addressing ICT risks in the smart grid to some extent.

What follows is the complete list of initiatives provided by the experts participating in the study:

Official documents and articles:

- NIST IR 7628: "Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References"
- CEN/CENELEC/ETSI - SGIS: "M490's Risk assessment task"
- DG CONNECT's Ad-hoc Expert Group for the Security and the Resilience of Information Technology and Communication Networks of the Smart Grid: "Challenges and recommendations for ICT security and resilience of Smart Grids"
- UK HMG IA Standard No. 1: "Technical Risk Assessment"
- US Department of Energy: "Electricity Sector Cybersecurity Risk Management Process Guideline"
- National Rural Electric Cooperative Association: "Guide to Developing a Cyber Security and Risk Mitigation Plan"
- IEEE Security & Privacy magazine: "Security and Privacy Challenges in the Smart Grid"

Conferences, forums, congresses, and online resources:

- CIRED 2011
- IEEE-PES GM 2011
- Cigré Symposium 2011.
- smartgridsecurity.blogspot.com
- cissp.logicalsecurity.com

Tools and methodologies:

- OpenAMI
- IS1

Public bodies addressing the topic:

- NERC (Natural Environment Research Council)
- FERC (Federal Energy Regulatory Commission)
- UK HMG IA (UK Government's National Technical Authority for Information Assurance)
- IEEE (Institute of Electrical and Electronics Engineers)
- CIGRÉ (Council on Large Electric Systems)
- NIST (National Institute of Standards and Technology)
- Germany's BSI (Federal Office for Information Security)
- CPNI (Centre for the Protection of the National Infrastructure)

- Department of Homeland Security (USA)
- Department of Energy (USA)
- Netbeheer Nederland
- CEN (European Committee for Standardization)
- CENELEC (European Committee for Electrotechnical Standardization)
- ETSI (European Telecommunications Standards Institute)
- European Commission

Task forces:

- European Commission Smart Grid Task Force
- SGIS of the CEN/CENELEC/ETSI - SGCG (M490)
- Security Technical Expert Group (STEG).
- DG CONNECT's Ad-hoc Expert Group for the Security and the Resilience of Information Technology and Communication Networks of the Smart Grid

Private organizations addressing the topic:

- IBM
- Kema
- IO Active
- Detica
- Southern Company (USA)

4.3 Important aspects on risk assessments in smart grids

As far as the importance of the topic is concerned a high level of consensus is reached among the experts. They consider that, in order to determine the cyber security goals and needs for the protection of national energy infrastructures, public bodies should follow a risk-driven approach. Moreover, there are experts who consider that DSOs, and maybe also TSOs, should conduct mandatory risk assessments. To this regard, an expert expressed the necessity that such mandatory risk assessments should be based on a selected methodology, and which should include a dependability analysis, a threat analysis, and a vulnerability assessment. Other experts suggested 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. According to one expert, it should be recognised that priorities on risks and threat levels might be different across Member States.

Some experts highlighted that a risk-based analysis is considered necessary to assess the consequences of using the Internet and other public networks in the smart grid, an important aspect for new value-added services. Likewise, in order to identify which components of the smart grid should undergo a security certification process, a detailed risk-based analysis should also be considered.

In relation to the methodologies for assessing ICT related risks in the smart grid, according to an expert belonging to a DSO 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. Therefore they decided to go for a manual risk assessment in collaboration with other Dutch DSOs based on a workshop approach, where experts met to collaboratively identify risks. Moreover in a second round they have started to use a more actual methodology, the IS1 methodology from the UK.

Some other experts supported the fact that there is not a good methodology for understanding/assessing the cyber risks of the smart grid, and they asked for a Programme to address this need, which focuses on the definition of a standard risk assessment methodology oriented to the security governance in utility companies. To this regard 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. Several experts also considered that such a methodology should include interdependencies analysis, among power grids from DSOs and/with TSOs. For some experts, another important factor is the inclusion of a stakeholder analysis. This means that an ideal standard methodology should consider the opinions, assumptions and expectations from those stakeholders which can eventually impact the utility in different ways, with a special attention on the customer and the supplier points of view. The stakeholders to be considered could include government, academia, manufacturers/vendors, customers, energy suppliers, retailers, DSOs, TSOs, etc. Experts from the standardisation field also suggested that a risk assessment methodology should consider the different use cases of the smart grid. Moreover, each use case can and should be classified into one of a number of predefined risk levels. Examples of these use cases include the management of Distributed Energy Resources (DER), demand-response applications and electricity market operations, interaction between consumers and marketing companies, etc.

Finally, some of the experts suggested that 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. New cyber security issues can originate in citizens and affect DSOs and TSOs.

5 The basic components of the smart grid

There are several points of view on what is the real scope of the smart grid, which will be discussed in detail in the following paragraphs. However, to defend the smart grid from a business case point of view, various experts concur in saying that the smart grid should be seen globally, as the electricity system of the future. They consider that 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.).

However, as we already mentioned, when addressing the details, not all the experts agree on what exactly the smart grid is. We will explain these different opinions in the following lines.

5.1 The horizontal view of the smart grid

Experts were asked about the components that should be considered part of the smart grids. 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.

An important characteristic which has been highlighted by many experts is the 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 resource at the end-users, such as batteries, solar panels on the roofs, etc. On the other hand, there is also a high consensus – especially among manufacturers, security tools and services providers and DSOs – on the fact that smart grid should be based on a supporting ICT infrastructure based on bidirectional communications.

Experts agree that the public and private sectors are undertaking prospective actions, business definition and enhancement in all areas by adding intelligence to the whole system, including generation, transmission, distribution, retail, etc. However, it is interesting to mention that DSOs and TSOs consider that Distribution and Transmission are respectively the most affected domains by the emergence of the smart grids. Other participants mention that small energy producers should not be left aside.

There is no clear agreement among experts when it comes to clarify whether AMI, smart homes and smart industry are part or not of the smart grid concept. For instance, there is a member from a public body who considers them as completely different concepts, while there are different experts stating that everything is interrelated and cannot be analysed separately. 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 – and should be the objective of smaller and more flexible companies such as energy marketers, home appliances manufacturers, etc. According to them, the DSO should be agnostic of what is going on inside the house. DSOs should provide signal prices to the smart meter and the house automation system should be in charge of switching off/on one appliance or another in

accordance to the energy management policy defined by the end user together with the energy marketer. Something similar occurs with micro-generation (e.g. solar panels on the top of buildings).

5.2 Vertical view of the smart grid

When the smart grid is presented as an underlying infrastructure supporting a number of new services and/or applications, there is no real agreement on what the smart grid is and what falls out of its scope.

A body of opinion states that the smart grid should include a very powerful communication infrastructure, with specific characteristics (e.g. it should reach any place necessary, with a good band-width, appropriate delays and vey high reliability) to support smart grid applications and services. 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).

On the other hand, there are some experts who consider that the smart grid is everything that is related with the grid operation and data communication, and therefore it should be separated from added-value services. The grid operator invests on the grid so that all the other actors can build services upon these investments. However, there is also one expert which consider that those services related to the management of the grid (e.g. demand-side management), could also be considered as part of it. Once again, the part of the grid closer to the final consumer is under controversy. Particularly, the majority of experts consider necessary to separate metering from value-added services oriented to the end user (i.e. services provided inside the HAN). A defined group of experts think that this type of services should not be part of the smart grid.

5.3 New applications and services

During the survey a number of value-added services and applications were enumerated by the experts. A DSO expert suggested that there are three great domains of applications in the smart grid: 1) AMI-based applications/services, 2) distributed generation management, 3) and advanced distribution/transmission automation. In the following lines we provide the full list of the applications and services enumerated by the experts classified into these three domains.

- **AMI or consumer-management oriented applications/services:** these include all those services and applications oriented to consumer management, including demand-side management, home-energy management, smart metering, etc. As supported by several DSO experts, these services are not necessarily provided by the DSO. However, DSOs can incentivise a shift in consumer behaviour of the energy consumption habits, for instance by signalling energy prices in real time to the smart meter.
- **Distributed generation management:** services and applications of this domain focus on the control and management of Distributed Energy Resources (DER). Most of the experts envision that, in the future, DERs will appear appropriately distributed all along

the grid so as to avoid great amounts of energy transfers (i.e. from bulk generation to the consumers). DERs can include roof sun panels, wind farms, batteries, etc. Actually, many experts referred to the Electric Vehicles (EV) as a relevant part of the distributed generation management, since they can be seen as batteries whose energy can be consumed locally or put back to the grid during the critical hours.

- **Advanced distribution/transmission automation:** which implies having a more robust and reliable grid in order to support the new applications and types of users connected. This will include substation automation, storage management, electricity distribution advanced applications, etc. For instance, several experts explained to us that in an emergency situation (e.g. faulty medium-voltage grid) islanding will be a technique to isolate an energy-autonomous segment till the service is resumed – as long as the local micro-generation power is enough to sustain basic services –. Integrating DER in the balancing equation of available energy and demand will also be part of the advanced distribution/transmission automation. This will bring great changes from an ICT and physical/electrical point of view. For instance, a DSO expert stated that the physical topology of the distribution network will need to be based on a ring structure so if there is a line cut in one area power can be rerouted to other parts of the grid. Likewise, another DSO expert explained that new controlling devices and sensors will need to be deployed all over the grid (i.e. at substations, transformer centres, lines, etc.).

In addition to the previous list of services, one of the experts also considered that macro-generation (i.e. bulk generation) will also be affected by the Smart Grid.

5.4 About a standard smart grid architecture

Based on the previous reasoning, it might become apparent that there is not a clear definition of what the smart grid is. The group of experts that represent the standardization bodies recognise that currently there is no clear standard for the architecture of the smart grid, and what is worse, some working groups are paralysed by this lack of definition. The lack for a standard architecture spans all the different domains (e.g. generation, distribution, etc.). In particular, some experts consider that the smart meter could be the central piece of the home energy services, but at the same time they declare that it might also happen that this device will only be in charge of providing information to a home automation system, which will be ultimately the system in charge of the aforementioned management features. Moreover, an expert declared that the aforementioned islanding features and demand-response functionalities are the kind of objectives that will be crucial in the evolution of the smart meter in the upcoming years. Therefore, it can be concluded that there is a need for consensus on the architecture. Such architecture has already presented in Annex I.

6 Knowledge and participation on smart grid initiatives

This section deals with taking stock of how well known are those initiatives dealing with smart grid cyber security issues, at the national and EU levels. Moreover, experts provide their points of view on what aspects could be improved and suggests valuable actions to that aim.

6.1 Knowledge on smart grid initiatives

The experts participating in the survey were firstly asked about their knowledge concerning organizations, working groups and R&D projects on smart grid somehow related with cyber security.

As we can observe on the diagram below, from the list provided there are some organizations and working groups which were selected by most of the stakeholders. It is especially interesting that experts belonging Academia and R&D are the best informed.

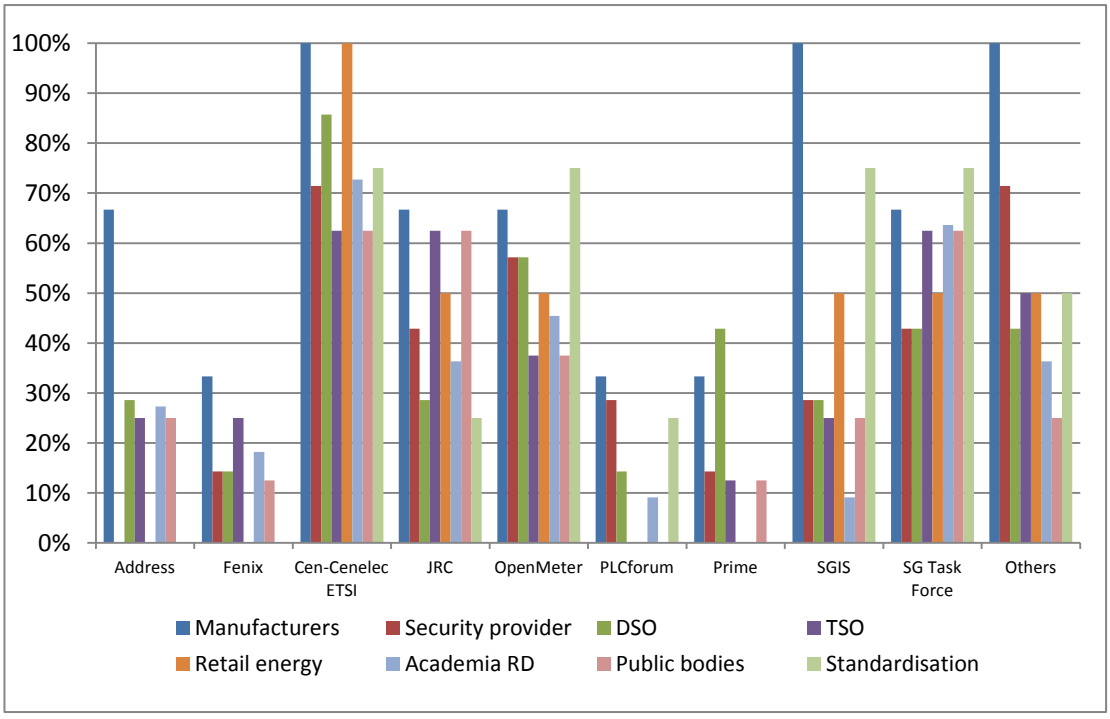

Figure 3 Degree of knowledge on initiatives related to cyber security

From the initiatives mentioned on the survey, the most well known is the CEN/CENELEC/ETSI association for smart grid standardisation. The majority of the stakeholders coincide in pointing it as a reference for smart grids issues. In contrast, PRIME Alliance is hardly known by any stakeholder type, with the exception of DSOs, which is quite logical since this alliance gathers manufacturers and DSOs. It is relevant that the Open Meter initiative is also well

known among most of the stakeholders. The Open Meter initiative looks to define a standard for AMI.

Apart from the closed list provided, several experts also suggested other initiatives. Many of them mentioned ESCoRTS (European network for the Security of Control and Real-Time Systems), CIGRE (International Council on Large Electric Systems) and EEGI (European Electricity Grid Initiative).

The rest of the initiatives mentioned have been studied by the authors of this study and are listed and described in Annex V.

6.2 Stakeholder involvement

Experts were also asked whether they participate or not in European and national information exchange platforms and other working groups devoted to smart grid cyber security issues. The results to this question are represented in the following chart.

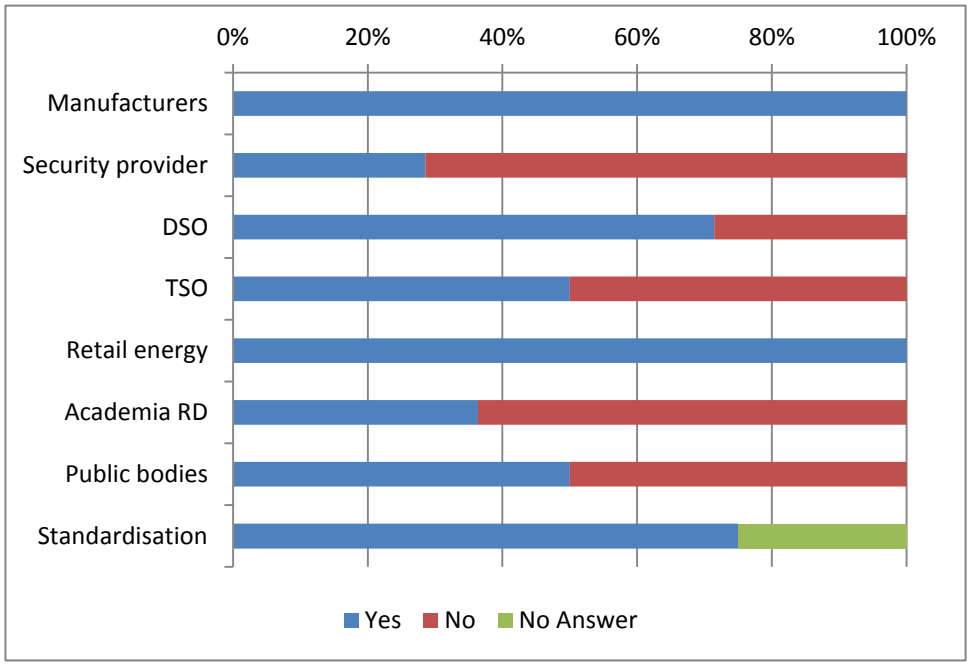

Figure 4 Degree of involvement on initiatives related to cyber security

It is relevant to highlight that the most active participants are representatives from standardisation, DSO, manufacturers and energy retailers. They are particularly active in sharing knowledge solutions in forums, workgroups and in public/private initiatives. It is relevant that DSOs are significantly more active than TSO, probably because the electrical distribution network will undergo a more significant change than the transmission grid.

The high level of participation from the standardization group is probably explained because of the efforts being done at national and the EU level to standardize the smart grid. Groups such as CEN/CENELEC/ETSI are developing standards for the EU commission supported and encouraged by specific work groups such as the DG-INFSO or the Smart Grid Task Force. Likewise, the high level of participation shown by manufacturers is probably explained because they are a stakeholder heavily affected by any standardisation activity.

Security providers, Academia and R&D are beginning to participate in the groups, especially now that it seems the electrical sector has recognized the high risks which might affect the smart grid. However, they are still far behind other stakeholders.

Additionally, experts were asked to provide the name and a description of those initiatives where they participate. Moreover, they were also inquired about what could be improved. Answers were varied but the groups which appeared more times were DG CONNECT ad-hoc expert group and EuroSCSIE but without an outstanding presence. Experts consider DG CONNECT ad-hoc expert group as one of the most important working groups concerning cyber security of the smart grid.

The rest of the initiatives mentioned have been studied by the authors of this study and are included in Annex V.

6.3 Thoughts on the initiatives

In general terms, experts participating in the study expressed different opinions about how European cyber security initiatives are being managed, organised and coordinated. A minority of them were absolutely satisfied; while the majority consider that there is space for improvement. Additionally, an expert from the EC, who is directly involved in one of these initiatives, declared that the general impression is that people are not happy on how things are being done in these groups. This same expert emphasized that this might be the result of a generalized perception that cyber security is not at the front-line of the smart grid priorities. He stated that other topics such as funding, incentives or customer acceptance are considered more important for the development of the smart grid.

Additionally, there are also some experts that complained because these initiatives lack from visibility. An expert declared that MS critical infrastructure protection agencies are not doing much to advertise them.

Two experts belonging to the TSO stakeholder type expressed their concern about the existence of dozens of initiatives – specifically working groups – addressing the same issues all across the EU – this does not only happens with cyber security initiatives – , at the European, national, regional and municipal level. According to these experts this is a consequence of how the EU is organised, where all regions address the same topics. Moreover, they also declared that in many of these initiatives around 80% of the people are the same and always talk about the same topics. Actually they consider that in most of these initiatives experts only talk but no real work is done, something that in the US does not happen so often.

When the experts were asked about specific initiatives, interesting points of view arose.

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.

Of special interest was the discussion on the overlapping and lack of coordination between DG CONNECT's ad-hoc EG and the Smart Grid Information Security (SGIS) working subgroup. Several experts belonging to almost all stakeholder types consider that these two initiatives have overlapping work programmes. Experts from both groups were enquired on this issue, and declared that a meeting was organised to clarify the scopes of the work programmes. These experts stated that clear orientation and non-overlapping scopes were agreed. Specifically DG CONNECT's ad-hoc EG work will address national-wide or European-wide aspects, considering the highest level of security with focus on regulatory authorities in Europe for influencing on European policies. On the other hand SGIS WG mission will continue to be based on the M490 mandate, and therefore ESOs will identify the standard framework for providing end-to-end information security to the smart grid.

However, another issue affecting both groups was raised by one expert of the EC, which declared that around 50% of the experts in one group are also present in the other group and at the same time, these experts complain because they do not have enough resources to commit to the work expected to be done in these two initiatives. He thinks that the number of experts on the cyber security topics of the smart grid is not very large and it is responsibility of the EC to make the most of it; having two different initiatives might not be efficient. Under his point of view, the SGIS subgroup should be maintained since it is under the umbrella of the European Directive for the standardization of the smart grid, and therefore there is a solid legal basis supporting it. On the other hand, other experts participating in the study declared that there is room for the two working groups since their target objectives are different.

Finally, this same expert also declared that it seems that the SGIS subgroup is not progressing at the appropriate pace. Moreover, he thinks that the reason for this is the lack of a concrete work programme with specific deliverables and milestones. However MS also recognizes that the lack of a standard architecture makes difficult to make an appropriate risk analysis to advance in concrete cyber security proposals.

6.4 Suggestions for improvement

Regarding the suggestions on how to improve the current initiatives on cyber security, the most outstanding consideration was the need for a better coordination so as to avoid duplicated work, same topics, etc. According to the experts, current workgroups are dealing with the same issues. However there is a lack of fluid communication among them which is not efficient from an investment/monetary point of view. At the European level, 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. This committee or group would be in direct contact with the EC and other public bodies and standardisation organisations, and would include under its umbrella not only initiatives as DG

CONNECT's ad-hoc EG or SGIS working subgroup, but also initiatives as OpenMeter and the like.

Regarding SGIS and DG CONNECT's ad-hoc EG, a DSO expert considers that there is room for a higher participation and leadership from the DSOs and also TSOs in the two groups. Under his point of view, DSOs are the ones implementing the largest portion of the smart grid. Therefore, and in order to fully understand the requirements of the smart grid, this is an important aspect. He considers very good news that solution providers are teaming up, but there should be more requirements coming from the DSOs.

In any case, most of the experts consider important that all types of stakeholders take part in cyber security working groups, so as to make the collaboration more successful.

Other aspects for improvement were also suggested. What follows is the list of these suggestions:

- All initiatives should have a clear strategy for results dissemination.
- Moreover, a small number of experts considered important the creation of a dissemination working group targeting end consumers.
- There should be initiatives targeting awareness-raising of C-level (e.g. CEO, CTO, etc.) staff on the importance of the cyber security and data privacy in the smart grid.
- Initiatives on smart grid cyber security should count on with operational technology staff (OT) and information technology staff (IT).
- There should be initiatives with higher technical level.
- Terminology (e.g. smart grid components/architectural model) discrepancies should be clarified across all initiatives.
- There are great economic interests that should be appropriately managed to avoid lobbies pushing for their own interests.

7 Outlook on the report "Regulatory recommendations for data safety, data handling and data protection"

All the stakeholders are asked about their knowledge regarding recommendations of data privacy and data protection, published in the report: "Regulatory recommendations for data safety, data handling and data protection" of the DG Energy's Smart Grid Task Force EG2.

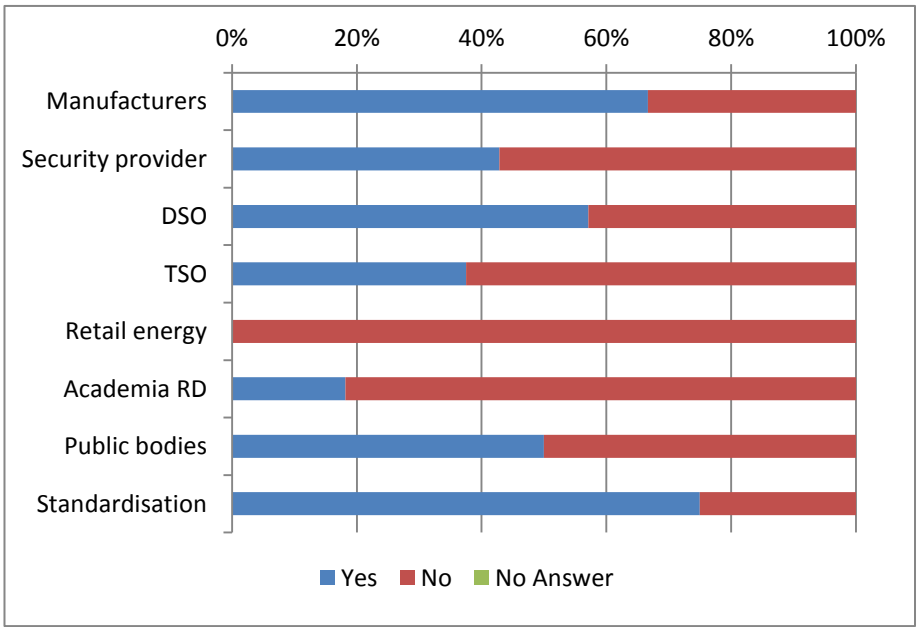

Figure 5 Degree of knowledge of the final report from EG2

The above graph shows a certain lack of awareness regarding these recommendations gathered on the report published by the EG2. Only manufacturers, standardization experts and DSOs crossed the threshold of 50%. The standardization group shows the highest level of knowledge, crossing the threshold of 75%.

We have also asked the stakeholders who have answered affirmatively to give their opinion about these recommendations. Most of them agree with the following appreciations:

- The provided recommendations are very positive and a high-quality work, and can be used as the starting point regarding privacy and data protection in the smart grid.
- The report is a useful compendium that takes, as a reference, technical and legislative "established" issues on data privacy and information security included in the European framework to analyze the specific roles and responsibilities of entities operating in the new grid context.

- Privacy requirements will evolve over time as the delivery of energy is a careful balance between the need to maintain supply, protect critical national infrastructure and allow for commercial services to develop. What is required therefore is a process for periodic review and amendment to the data use regimes.

Other individual opinions which were relevant are listed in the following lines:

- The recommendations and requirements provided are only an overview of the problem; they are too general. It is necessary to go into the details in what concerns to application development and related regulations, for instance by detailing the necessary technologies.
- These recommendations focus only on the privacy aspect of the smart grid. The document does not contemplate cyber security which is intimately related to data privacy and data protection. Moreover resilience, robustness and flexibility of the electrical system should also be considered altogether.
- Recommendations need to be further extended and aligned with other similar documents, especially with NISTIR-7628 and IEC TC57.
- The report should stress the importance on the need to share information among the stakeholders about incidents, threats, vulnerabilities and good practices in a secure way.
- The report establishes a useful list of recommendations which supplements the requirements that are set out in the data protection acts (and are backed up through the Human Rights legislation). However it might be necessary to provide a definition of what constitutes 'regulated' (i.e. permissible under a licensed activity of an energy supplier or network operator) uses of energy consumption data.

8 The main cyber security challenges in the smart grid

Experts were asked about the main cyber security challenges that the smart grid faces.

All stakeholders agreed that one of the main challenges is having a robust grid to overcome potential attacks, and particularly Denial of Service (DoS) attacks. Another important challenge for most of the experts is data protection, including consumer data as well as control and automation readings and commands. With respect to consumer data, it is of particular interest to be able to protect consumers from those situations in which personal information can be inferred from personal data (e.g. particularly on habits). On the other hand, guaranteeing integrity and authenticity of the data processed by automated decision-making systems in the smart grid (i.e. automatic distribution balancing, automatic current disruptions, etc.) is considered critical. To this regard, an expert from a DSO explained that, in the new grid, there will be many more stakeholders than in the past. Service providers, the DSO itself and the end-consumer might need to have access to the same metering data. Providing a secure access to the necessary information is a great challenge that will have to be solved.

The abovementioned challenges were pointed out by at least one expert of each stakeholder type. Besides, there are other important challenges that were also quoted and which are presented in the following lines following a classification which is based on the types of stakeholders who mentioned them.

- For manufacturers and academia/R&D, the main challenges are related to unauthorized access to systems or devices, which might derive in escalation of privileges, denial of service attacks, exploit injections, man in the middle attacks, etc.
- For security tools and services providers and standardization bodies, the main challenge is raising awareness and training among manufacturers, as they have to build secure devices, as well as provide expert support.
- Security tools and services providers consider that a change of mentality is also necessary among utilities to avoid situations where cyber security is considered an important issue until it comes to practical implementations when is often ignored because of project budgets, pipelines, lack of expertise, etc.
- Security providers and public bodies also refer to necessity of an end-to-end security, 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. Smart grid companies along the value chain are getting more and more dependent on each other and they need to get securely interconnected.
- A DSO expert stated that it is necessary to understand that smart grid systems (i.e. SCADA, control devices, metering equipment, sensors, etc.) will not be physically isolated anymore since we are moving towards a network of systems.
- To this regard, TSOs and retail energy providers declared that it will be a challenge to separate the competitive part (value-added services for consumers, customer/supplier relationship, etc.) from the non competitive part (remote meter reading, network

operations, etc.). This will be necessary to minimize the chance that cyber security issues affecting end-consumers have an impact on grid operational facilities (i.e. control centres, substation automation equipment, etc.), so as to keep a controlled and stable electricity network.

- For Public bodies and Academia and R&D, the challenge is to maintain the current degree of stability in the grid, with similar or even less black-outs or brown-outs. The inclusion of ICT services must not negatively affect such statistics.
- An expert from a public body considers that it will be challenging to transition from the current grid to the future smart grid. To this end a proper integration of legacy systems into a robust and resilient grid will be of paramount importance.
- Public bodies and DSOs also highlighted that the future integration of different energy types (e.g. heat, gas and electricity) at the metering infrastructure could derive into interdependencies and shared cyber security risks among operators and service providers dealing with critical infrastructures of different nature.
- An expert from a European public agency declared that addressing the consequences of incomplete regulations can be a great challenge. He pointed out to the European regulation that requires smart meters to be deployed into houses in a short period of time not taking into account information security risks, which is a basic aspect for addressing privacy issues.
- Grid monitoring is considered a great challenge for academia and R&D. Availability of specific traffic analyzers, communication monitoring and application log monitoring and related technologies will be a hot topic in the short/medium term.
- A R&D expert declared that 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.
- Finally, DSOs and Academia and R&D experts believe that defining a standard architecture of the smart grid is necessary in order to develop secure devices and provide holistic security solutions.

When the experts participating in the study were asked to choose the top 1 cyber security challenge, generally different answers were provided by different stakeholder types.

For Manufacturers and Academia/ R&D, having secure devices is the top priority. On the contrary, TSOs, security tools and services providers and manufacturers consider that data privacy and information and communications security is the key challenge. Finally public and standardization bodies coincide in that the most relevant aspect is to have a reliable power grid through proper integration of all components.

In any case, many experts suggested that, in order to identify the most relevant challenges, a risk-driven approach should be followed. Each organisation is different and such an approach would help decide the most adequate strategy for protecting the infrastructure end-to-end.

9 The main pillars of smart grid cyber security

Stakeholders were asked to choose out from the topics technology, processes and people, which is most relevant one when addressing cyber security in smart grids.

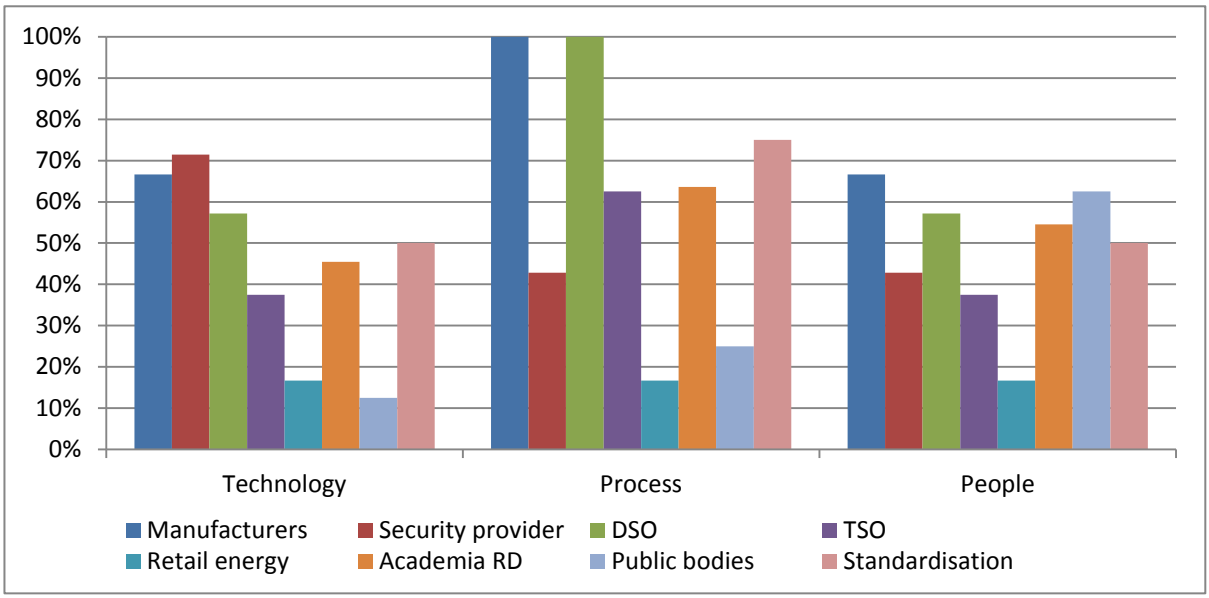

Figure 6 Importance of technology, processes and people for making the smart grid secure

If we analyse the raw numbers, processes obtains the first position of the rank, people the second and technology the third. The great majority of the experts consider that processes are the most relevant aspect to pay attention to when dealing with cyber security. People and technology – second and third in the rank – got a similar grade with only three points of different in favour of people.

If we analyse the results on a per stakeholder basis the results present slight differences. For manufacturers, DSOs, TSOs, academia and standardization bodies, processes are the most important aspect to address. On the contrary, technology is the factor that has a greatest impact according to security tools and services providers, while people are the one chosen by public bodies.

Experts participating in the study provided specific comments for each one of the three areas considered. They all agree that the three areas have to be addressed. What follows is a summary of these comments:

- **Processes:** all processes in the organisation have to be analysed and secured. An Information Security Management System (ISMS) 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.

- **People:** 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.
- **Technology:** components of the smart grid have 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.

Experts also listed several other important issues that do not only affect one of the previous categories but at least two, or even all of them at the same time. These are the following:

- 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.
- Following a holistic approach is the better way to secure the smart grid of the future. Different use cases need to be considered altogether since addressing specific ones in an isolated way will eventually result in risks not considered by anyone. Furthermore, securing individual components does not solve the problem of interdependency issues.
- Home Area Networks are directly dependent of 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.
- The more sophisticated technology is, the more threats you have to address.

10 Certifications and the role of National Certification Authorities

Experts participating in the study were asked whether national certification authorities could play a relevant role in what respects to the security of smart grids. Those respondents who answer positively were further enquired about what this role could be.

The following chart shows that a great majority of participants believe that these entities have an important role to play from now on.

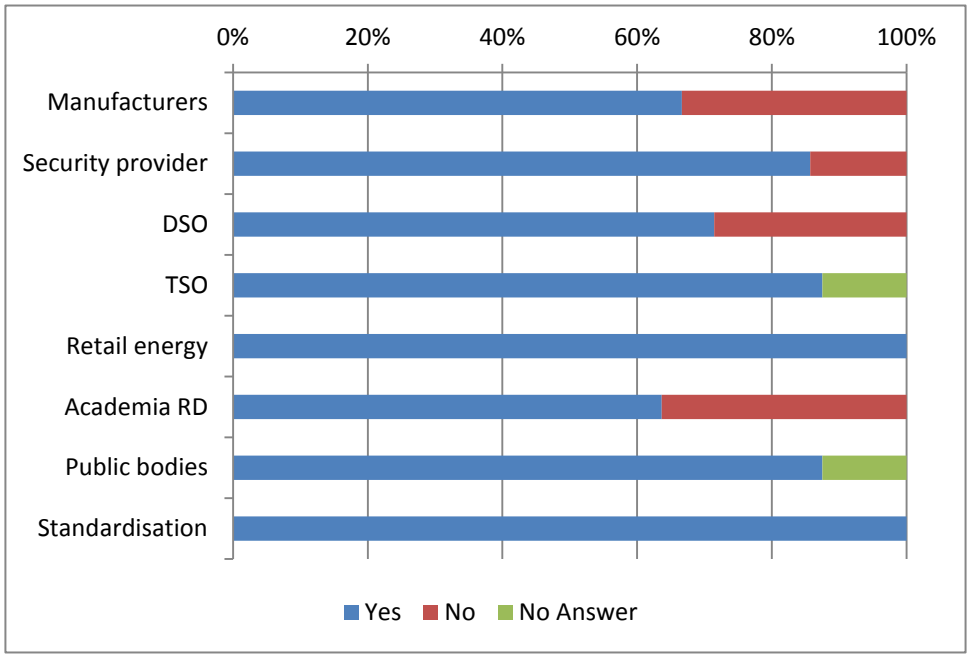

Figure 7 Percentage of experts considering security certifications important

To the question of what specific roles could National Certification Authorities (NCA) perform experts provided several answers. All of them have been summarised in the following lines:

- NCAs should guarantee that the critical components of the smart grid are secure enough by checking against predefined protection profiles. To this regard, experts envision that smart grid devices will require trust and authentication capabilities, and given the expected level and scale of deployment, they consider that there is no doubt that some certain interoperability should be required.
- In order to identify such components experts agreed that a risk-based approach should be followed, though some experts already pointed out to those components that might lead to a black-outs/brown-outs, including devices that handle keys, those that are involved in some critical transactions/operations, etc.

- To this regard, NCAs should not only target the products in place but also whole set-ups. For instance, control centres installations are normally turnkey projects under the control of the provider (e.g. manufacturer or integrator). Asking for a secure-certified SCADA software package is not enough. The whole set-up needs to be certified, including for instance the network communications and security gear as well as the software platform of the servers and other devices (i.e. operating systems, basic security setups, etc.)
- Most of the experts agreed that device/product certification (i.e. devices or complete set-ups) is not enough to guarantee that the smart grid is secure. A complementary certification assessing and certifying organizational aspects, processes, people, etc. is also necessary. This means that NCAs should not only target solutions providers (i.e. vendors, manufacturers) but also utilities and services providers and the way they operate their infrastructures and systems. For these two different categories, different certification approaches are needed and have to be considered simultaneously.
- Additionally, 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.

Most of the experts did not only provide their opinions on what should be the role of certification authorities, but also shared with us their concerns and points of view on how the abovementioned certification strategies should be implemented. However, in all cases the underlying basic principle is to not reinvent the wheel.

10.1 Strategy for implementing a device-oriented security certification

With the objective in mind of certifying 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. Finally, ISA 99 standard on security controls for embedded systems was also referenced several times.

Additionally, an expert explained that in some MS there are already bodies that give advice on which security level devices should be certified with. Such ongoing initiatives can be considered as an example for future work on this issue. For instance, this expert mentioned the case of the Technical Assurance Authority (CSG), a Government Authority, which is currently designing an accreditation process for smart metering devices in the UK.

Among the general reference frameworks, Common Criteria was by far the most referenced standard, and many interesting opinions regarding its applicability were provided. For instance, several experts belonging to the security tools and services provider stakeholder type, coincided in that Common Criteria (CC) is not specialised on control systems and other smart grid industrial elements, so it can be a reference but not the definitive guide when requiring secure devices to providers/manufacturers. Common Criteria needs to be really

focused on smart grid and smart metering equipment. According to these same experts, Common Criteria could be extended to include specific security profiles for the smart grid, similar to those related to the Smart Card Industry. In the context of the Smart Card industry there is already a common way to use Common Criteria which is basically an agreement of the involved industry (not directly related to the standard) on how to use the Common Criteria, which resulted in the development of a joint interpretation library.

On the other hand, there is a body of opinion which states that Common Criteria could be a high burden for manufacturers and integrators. According to the experts supporting it, Common Criteria requires too many details for a certain implementation of functionality. This means that if a manufacturer decides to change the functionality of a certain product/device it will need to also change the security profile, resulting in a need for readapting the whole certification process. Moreover, Common Criteria is complex and the technology for smart grid security is not yet mature enough to be included in this framework. Somehow supporting this idea, some representatives from DSOs, public bodies and security services providers declared that there is a need to be agile. They consider that we cannot simply wait to choose and develop the best standard for certifying products and setups. For this purpose they suggest that quick tests (e.g. white-box audits, code audit, etc.), not focused on certifying Common Criteria or other certifications, as those that could be conducted by organisations such as the ENCS, are very valuable and agile too, as it is done in the US inside the INL or Sandia Labs through the National SCADA Test Bed (NSTB) programme. Existing ICS cyber-security standards could be a good reference for such tests. To this respect, one of the experts also referred to WIB's requirements for vendors which is already an IEC/PS document (pre-accepted standard) with number 62443 and also part of the ISA framework (as ISA 62443).

10.2 Security governance certification strategy

As it became clear from the previous paragraphs, a security certification for electricity operators and other organisations related with providing value-added services is necessary. Security needs to be seen as a process that needs to continuously evolve and be monitored and tested. Therefore, experts suggested to have something similar to ISO 27K series of standards. Such a certification should take into account risk assessment and risk management no matter if the systems in place can be trusted (i.e. security-certified systems) or not (e.g. legacy systems). Moreover, such certification should check the proper implementation of integral ISMS. 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.

For this purpose, several experts referred us to ISA 99, NIST 7628 Guidelines for Smart Grids Cyber security, and of course the aforementioned ISO 27K as a more general framework. It is interesting to highlight that, according to an expert from a national public body, NIST guidelines cannot be directly applicable since it has been demonstrated that smart grids in the US are not directly comparable to those in Europe. If ISO 27K were the chosen security

framework standard it should be adapted to the smart grid field, as it happened with the telecommunications sector that has its own annex.

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.

11 Considerations about how to measure cyber security in smart grids

During the study several issues regarding measuring cyber security were discussed. In the following lines we will explain the main coincidences and discrepancies among all of them regarding this topic.

11.1 A reference framework for measuring security objectives

One of the issues experts were enquired about was on how could be verified if security controls are effective. In general terms 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.

However, 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 make comparisons among different companies. According to the experts, such a framework should consider:

- Including a minimum set of standards and guidelines, such as: 1) a reference common 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. Those standards and guidelines should be developed by counting on with all stakeholders[3].
- Defining certifications schemes for product/devices and utilities operating the grid. A certification authority organised preferably as a Public-Private Partnership (PPP), counting with specific test beds as well as an expert group of auditors would extend certificates to products, setups and organisations. Guaranteeing the independency of such an entity is necessary according to experts, since the market is deregulated and is very commercial.
- Articulating regulatory mechanisms asking for mandatory product/device and organisational security governance certifications (in the terms described in section 10), as well as risk assessments (in the terms described in section 4). Requirements should be more stringent for systemic organisations. The results of such evaluations should be

[3] *One expresses his concern because some non-standard security requirements are pushed by companies for economic reasons.*

communicated to the National Security/Regulatory Authorities, which in turn should report to a European body. In case of incompliance there should be regulatory pressures like monetary fines/fee/penalties.

- An expert belonging to a DSO suggested updating the European Directive 2008 114/EC, Council Directive on the Identification and Designation of the European CIs to also include the DSOs and not only TSOs. This update would provide a legal basis that would support the abovementioned mandatory evaluations for DSOs.
- The results of these evaluations should be of public knowledge, available to everybody and in particular to the consumer, so that they can react to the security posture of the utility organization. One way of doing this while not revealing confidential information is as simple as that an authorised organisation gives a "green tic" approving their security strategy.
- Some experts suggested that this framework should be articulated and managed by the European Commission in coordination with DG Energy.
- Finally, such a framework should establish the basis for allowing DSO's, TSO's and maybe also other stakeholders share internal best practices.

It is interesting to highlight that there are discordant opinions about such a framework. For instance, one expert considers that methodologies, tools and regulatory mechanisms should be defined very carefully to avoid situations as those of the NERC-CIP in the US or in other national initiatives on CIP across the EU. This expert stated that a framework asking for security assessments (i.e. certifications and risk analysis) can even be counterproductive. This can happen if operators do not continue investing in security once they achieve the security control objectives defined in coordination with the competent authority. Operators will only comply with a minimum level of security, which does not necessarily guarantee that they are really secure. In such situations control objectives are defined by the risk analysis being carried out by the operators themselves. As a result operators define their own priorities, which in turn can result in each one addressing those aspects that are less problematic.

11.2 Measuring security during the lifecycle of product development

Experts were enquired whether development process evaluation is more or less important than security functionalities verification. More than a half of the answers stated that they are equally important, and that it is not possible to choose one over the other, as they have different purposes and objectives/methods.

In any case a high number of respondents consider that, if one has to be chosen, it should be the development process evaluation. The main reason for this answer is efficiency. According to the respondents this type of measures can avoid redesigns which would have costly consequences in a large life-cycle domain, such as is the case of Industrial environments as the smart grid. Just a few of them (especially among DSOs and TSOs) consider that verification is more important than a development process evaluation.

Some experts consider that choosing between one or another might depend on the number or importance of the devices to be deployed. According to them, the most important ones

(i.e. control or massively deployed devices) have to be evaluated during the development process and at several intermediate critical points. This same thesis was supported by manufacturers which additionally stated that such evaluation must be agile.

12 Managing cyber attacks

Experts were asked about the best options to detect, isolate and mitigate an incident in a Pan-European attack scenario. As it will be seen in the following lines, experts did not only refer to large-scale incidents but to cyber security incidents in its broadest sense. All contributions are considered highly valuable. Therefore, in the following lines we will present the conclusions on how to deal with cyber security incidents in general.

During the interviews and also in the answers to the questionnaire, some experts pointed out that 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 generation to consumption, and at all levels, from infrastructures to services and operations.

Moreover, some experts also consider that depending on the cyber attack it is of high importance 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.

12.1 Experience in dealing with power-grid related incidents

There are several experts who referred to past experiences on pan-European incidents, such as the Italian blackout deriving from problems at the Swiss and French power grids, to support the idea that domino effects cannot be managed at the national level. According to them there is a need to have a pan-European entity to coordinate these transnational structures.

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) and that there exist already mechanisms in place, at the organisational and coordination level and also at the technical level that should be considered. According to these experts DSOs and TSOs are good already in restoring the power service since they've been doing it for the last 100 years. To this regard, an expert from a public body explained that there is already a cooperation model among TSOs in Europe with a crisis management strategy and two central points from where they monitor – and also act on – the TSOs' networks in Europe and where TSO operators can work together in case of an emergency.

12.2 Detecting cyber security incidents

Representatives from a DSO, a public body and security tools and services provider 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. As an example of this, an expert mentioned the IRRIS FP7 IP project, which role is to create an alarming system among different operators/energy providers.

One of the experts highlighted the importance of identifying where an incident originates so as to detect the cause and decide how to deal with it. This expert mentions the challenge of dealing with incidents affecting devices of private households (e.g. The TV is hacked) or related with the Internet in added-value services, as well as on defining what behaviours should be reported to DSOs and TSOs, etc.

With respect to the technical details of how DSOs and TSOs should do incident monitoring, experts suggested the following ideas:

- It would be necessary to implement managed security monitoring, either decentralised monitoring where sensors are distributed along the network or centralised monitoring where data is forwarded to a central point of collection and analysis. It is suggested that such a central point could be a SOC (Security Operations Centre).
- Signature-based software will be needed so that sensors can send alerts to these central systems (e.g. SOCs). These central systems should be intelligent to understand and correlate all information (new signatures, threats, etc.)
- It would be very important that these systems are intelligent enough to distinguish if an electrical incident, such as a blackout, has its root cause in a cyber security event or in any other kind of event (e.g. burned transformer)
- Monitoring centres like this could be organised as PPPs and could also include research activities (i.e. write new signatures, study new threats, etc.) and could be a valuable source of information to improve the resiliency of the grid architecture based on real experience.
- There should be a regulation obliging these organisations to report on incidents to a national or supranational entity.

12.3 A European-wide coordination

As it has already been introduced, several experts share a common view on the need for a pan-European entity which coordinates transnational structures (i.e. European power grid) when managing a large scale cyber security incidents. Experts provided their opinion on what should be the desirable characteristics of such an entity:

- It should have a global overview on what is going on in the European Smart Grid, and provide feedback to those organisations affected.
- Such an organisation should be in charge of escalating alarms and acting upon them, by taking the lead to deal with cyber security incidents that affect the stability of the grid.
- Final decisions (e.g. isolating a TSO) are considered a political issue involving several countries for which this entity can only provide advice.
- It should understand the interdependencies along the value-chain, as for example among DSOs, with TSOs, retailers, etc.
- It could be sponsored by the energy organisations, public bodies or even the EU.

Additionally, an expert from a public body reminded that in the case of a power blackout there will be many other critical infrastructures involved. As a result, the coordination in case of large incidents should be led by those agencies dealing with Critical Infrastructure Protection (CIP) at the national and European levels. They will advice the normal crisis management structures on how to better deal with the consequences of cyber incidents.

Regarding decision taking, an expert from academia considers that operators should be involved but should not take any decision in order to avoid conflicts of interest among them (e.g. trying to impose the knowledge base of one operator as the standard one).

Several experts provided their own suggestions on which organisations could have a role in such coordination activities. The list includes ENISA, ENTSO (European Network of TSOs), ACER (Agency for the Cooperation of Energy Regulators) – which is part of the EC and coordinates TSO's responsibilities.

Later in this section, it would be also explained the role that CERTs[4] could play in such scenarios.

12.4 Other relevant aspects

It is a common perception among experts that, at the National level, DSOs and suppliers should also be involved when dealing with cyber security incidents (that might not be important enough to have a European-wide impact). At the local level (e.g. related with smart meters) a local management is needed and DSO's and suppliers will have to be the final responsible for that.

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. In any case, other experts who are not against a centrally coordinating entity also share the same points of view regarding the importance of improving communication and knowledge sharing in crisis management.

Additionally, several experts agreed that in case of a cyber incident impacting the electricity delivery service, first the DSO/TSO should concentrate in restoring the energy service, and then deal with the cyber security incident itself. It is envisioned that with the smart grid services and systems will be much more automated and therefore updated procedures will need to be defined to be able to restore the electricity service. Moreover, if one portion of the whole grid is attacked there should not be a cascading effect. To this regard it is important that utilities know about each others' architectures if coordination is done in a distributed manner. If coordination activities were conducted by a central coordinating entity, this organisation should be the one managing such information.

---

[4] *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.*

12.5 The role of CERTs

The experts participating in the study were asked about the necessity of creating of a unified ICS/Smart Grid CERT to manage security incidents. The results of this poll are shown in the following chart:

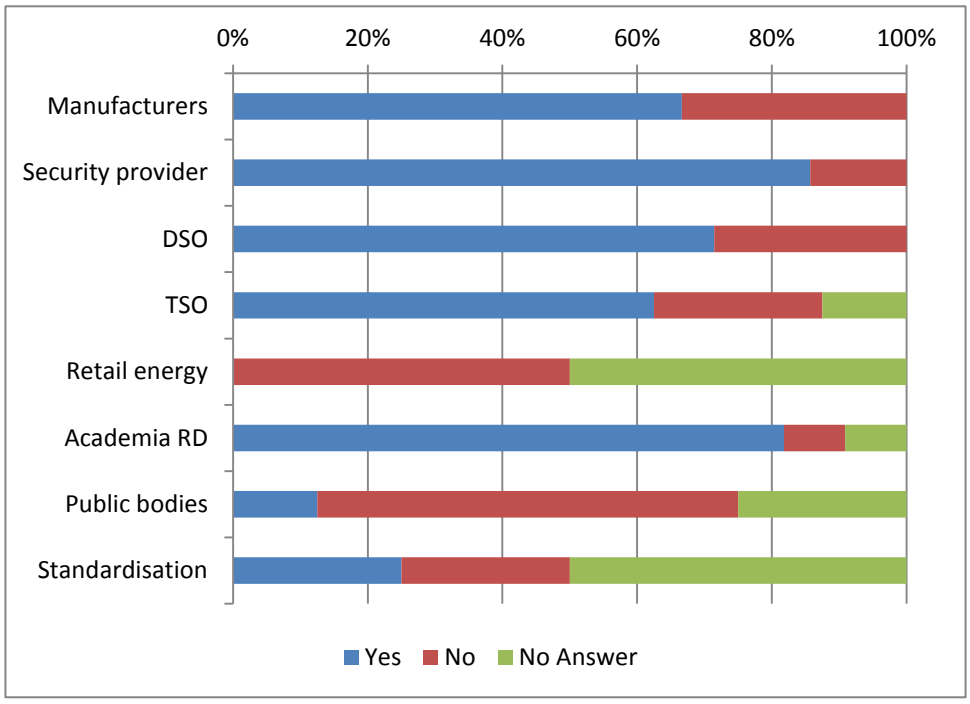

Figure 8 Perception of the necessity for an ICS/Smart Grid CERT

As seen can be seen from the figure, a slight majority of experts (57%) believe that this would be a good idea. But, there is also a significant part of them (29%) that is against such a CERT, while the other 14% do not express their opinion. As a result, the creation of a unified ICS/Smart Grid CERT would probably find some resistance.

Security Providers and Academia seem to be more convinced with the idea, with a wide majority of experts (over 80%) supporting it. Manufacturers, DSOs and TSOs are less convinced by it – between 62 and 72% of the experts support it. Finally, public and standardisation bodies are mostly against such an idea and in many cases did not answer at all.

The experts were further enquired on some details, such as the scope and benefits of a CERT dealing with smart grid cyber security issues.

Regarding the benefits of such an organization, the advantages described are the following:

- A unified point for information exchange which centralises and distributes information/reports, helps sharing experiences and knowledge, etc. This is considered useful for general security assessment, improving response times and R&D activities.

- A reference for valuable information such as threat advisory, good practices distribution. Furthermore, recommending on how to respond to cyber attacks can also be part of these duties.
- A central point for cyber security monitoring at the pan-European level on a 24x7 regime. This characteristic is considered a great added value, especially among DSOs, TSOs, and academia.
- An organisation for leading activities focusing in awareness rising.
- A reference organisation aiding organisations to deal with cyber security certifications.

Many experts agreed that such CERTs could play a role but should not be the central piece. According to them, CERTs cannot be familiarised with the details of electricity systems, their operation, and existing interrelationships across the value chain. Therefore it is important to particularly involve TSOs but also DSOs, DER, etc. However, these experts consider that there is room for ICS-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. Additionally, 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. If there is a highly organized cyber attack against Europe it will not only target smart grids but also other critical infrastructures. Therefore such a CERT should have this broader view, recommending on how to respond to such a cyber attack.

In any case, regarding the scope of such CERTs, a high number of respondents declared that an appropriate answer to this issue needs more discussion and should involved existent CERTs.

13 Research topics

Experts were interviewed on the most relevant research topics addressing cyber security in the smart grid. There were multiple and very interesting answers that we have grouped into several categories. These topics are listed in the following lines:

- **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.)
- **Architecture:** 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.
- **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, security governance, use-case modelling, threat analysis, development of security mechanisms against distributed denial of service attacks and other attacks.
- **Trust and assurance:** security metrics to measure the maturity level of security controls for each domain of the smart grid; hardware-based one-way communications.
- **Security in dependable systems:** with subtopics such as the definition of common procedures and interfaces, the overcome of hardware constraints limiting log management, encryption, or application/network filtering capabilities.
- **Privacy and security by design:** protection against zero-day vulnerabilities; optimization of very specific cryptographic protocols to reduce processing load without reducing the security level.

Other topics mentioned by the experts included: supply chain protection; usability, legal and economic issues; and smart grid and the cloud.

It is interesting to highlight that according to a DSO representative, grid operators should be responsible for investing in cyber security research activities, a role that should not be delegated to public bodies. They need to lead the research by putting the bulk of the money on research activities in this field. Public bodies could then incentivize such research programmes.

14 Bibliography

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

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

3. **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. COM(2011) 202 final.* 2011.

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

5. **Zhang, Zhen.** *Smart Grid in America and Europe: Similar Desires, Different Approaches (Part 1). .* 2011.

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

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

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

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

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

11. *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.

12. **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.

13. **National Institute of Standards and Technology (NIST).** *NIST SP 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* 2010.

14. **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.

15. **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.

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

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

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

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

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

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

22. **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.

23. **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.

24. **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.

25. **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.

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

27. —. Recloser. [Online] [Cited: 12 26, 2011.] http://en.wikipedia.org/wiki/Recloser.

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

29. **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.

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

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

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

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

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

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

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

37. **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 .

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

39. **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.

40. **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.

41. **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.

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

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

44. **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.

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

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

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

48. **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.

49. **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.

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

51. —. *NISTIR 7628: Guidelines for Smart Grid Cyber Security.* Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

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

53. **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.

54. **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.

55. **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.

56. **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.

57. **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.

58. **Mo, Yilin, 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.

59. **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.

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

61. **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.

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

63. **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. Energy 2020: A strategy for competitive, sustainable and secure energy. COM(2010) 639 final.* 2010.

64. —. *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.

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

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

67. **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.

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

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

70. —. *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.* 2005.

71. —. *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.* 2006.

72. —. *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.

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

74. **Commission of the European communities.** *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.

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

76. —. *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.

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

78. **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.

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

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

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

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

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

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

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

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

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

88. **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.

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

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

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

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

93. **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.

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

95. **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.

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

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

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

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

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

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

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

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

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

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

106. **National Institute of Standards and Technology (NIST).** *NIST SP 800-53: Information Security.* National Institute of Standards and Technology. 2009.

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

108. **Institute of Electrical and Electronics Engineers (IEEE).** IEEE Power & Energy Society. [Online] http://www.ieee-pes.org.

109. **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.

110. —. *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.

111. —. *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.

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

113. —. *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.

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

115. —. *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.

116. —. *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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

131. **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.

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

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

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

135. **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.

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

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

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

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

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

141. **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.

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

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

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

145. **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.

146. **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.

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

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

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

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

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

152. **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.

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

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

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

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

157. **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.

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

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

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

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

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

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

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

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

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

167. **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.

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

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

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

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

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

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

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

175. **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.

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

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

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

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

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

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

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

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

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

185. —. *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.

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

187. **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.

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

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

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

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

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

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

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

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

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

197. **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.

198. —. *Cyber storm III Final Report.* Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division. 2011.

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

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

201. **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.

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

203. **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.

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

205. **North American Electric Reliability Corporation (NERC).** *Categorizing Cyber Systems. An Approach Based on BES Reliability Functions. Cyber Security Standards Drafting Team for Project 2008-06 Cyber Security Order 706.* 2009.

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

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

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

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

210. —. *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.

211. —. *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.

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

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

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

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

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

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

218. **Institute of Electrical and Electronics Engineers (IEEE).** *WGC1 - Application of Computer-Based Systems.* http://standards.ieee.org/develop/wg/WGC1.html.

219. —. *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

220. —. *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

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

222. **Norwegian Oil Industry Association (OLF).** *OLF Guideline No. 104: Information Security Baseline Requirements for Process.* Norwegian Oil Industry Association. 2006.

223. **International Federation of Automatic Control (IFAC).** TC 3.1. Computers for Control — IFAC TC Websites. [Online] http://tc.ifac-control.org/3/1.

224. —. TC 6.3. Power Plants and Power Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/6/3.

225. —. 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.

226. **International Federation for Information Processing (IFIP).** IFIP TC 8 International Workshop on Information Systems Security Research. [Online] http://ifip.byu.edu.

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

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

229. —. Control Systems Security Publications Library. [Online] http://energy.gov/oe/control-systems-security-publications-library.

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

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

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

233. **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.

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

235. **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.

236. **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: A Digital Agenda for Europe. COM(2010)245 final.* 2010.

15 Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
BAN	Building Area Networks
BPL	Broadband over power line
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIA	Confidentially, Integrity and Availability
CO2	Carbon dioxide
COTS	Commercial of the Self
DG ENER	Directorate-General for Energy
DLMS/COSEM	Device Language Message specification/COmpanion Specification for Energy Metering
DLR	Dynamic Line Ratings
DMS	Distribution Management System
DSM	Demand Side Management
DSO	Distribution System Operators
EACI	European Association for Creativity and Innovation
EC	the European Commission
ENISA	European Network and Information Security Agency
ENTSO	European Network of Transmission System Operators for Electricity
ETP	Executive Training Programme
ETSI	European Telecommunications Standards Institute
EU	European Union
FAN	Field Area Network
FTP	File Transfer Protocol
GHG	Greenhouse Gas
GPRS	General Packet Radio Service
HAN	networks (Home Area Network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IAC	Integrity, Availability, Confidentiality
IAN	Industrial Area Networks
ICS	Industrial Control Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPS/IDS	Intrusion Protection/Detection System
IP-Sec	Internet Protocol secure
ISM	Information Security Management

ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
LAN	Local Area Network
MAN	Metropolitan Area Network
MID	Measuring Instruments Directive
MPLS	Multiprotocol Label Switching
NAN	Neighbourhood Area Network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OMS	Outage Management System
OWASP	Open Web Application Security Project
PLC	power line communications
R&D	Research and Development
RF	radio frequency
RTU	remote terminal units
SCADA	Supervisory Control and Data Acquisition
SFTP	Secure File Transfer Protocol
SG	Smart grid
SIEM	Security information and event management
SMART	standardization (S), monitoring (M) accounting (A) rethink (R) transformation (T)
SSH	Secure Shell
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunications Network
TSO	Transmission System Operators
UK	United Kingdom
USA/US	United States of America
VPN	Virtual Private Network
WAN	Wide Area Networks

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