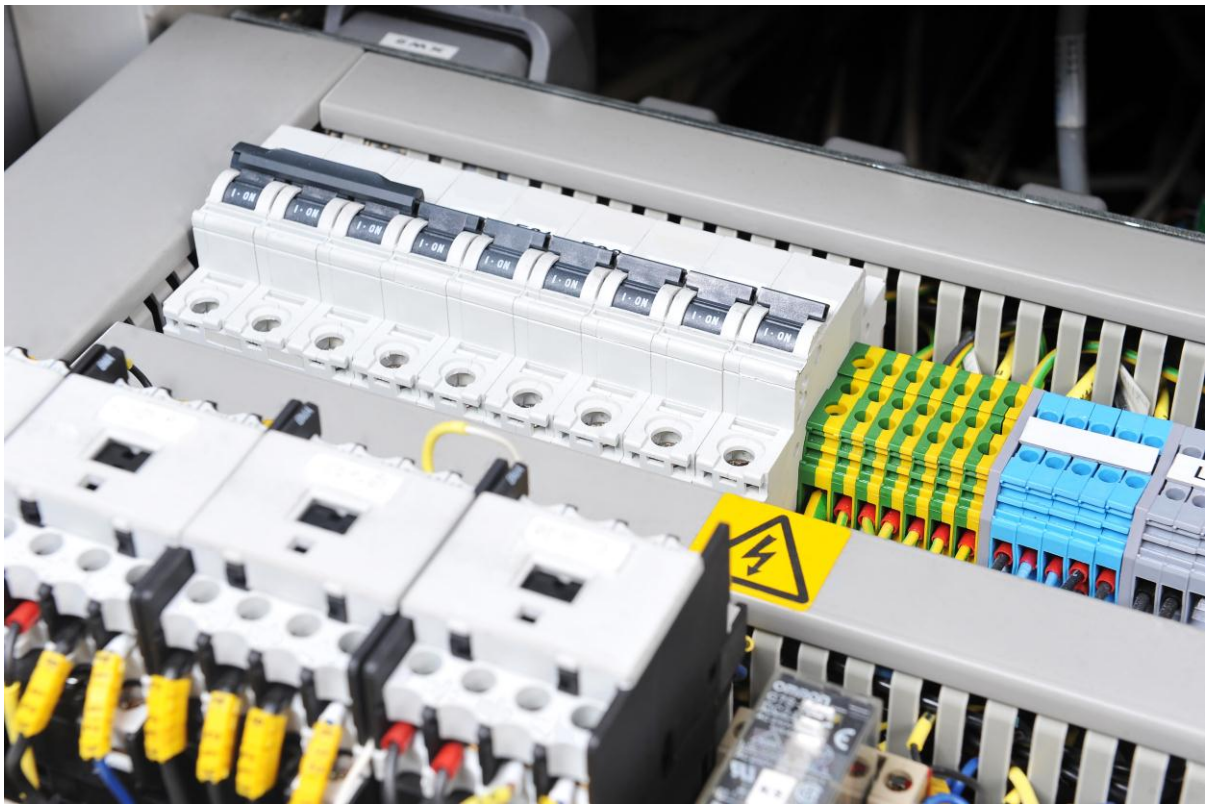
Smart Grid Security



Annex II. Security aspects of the smart grid

[Deliverable – 2012-04-25]

This document is Annex 2 (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.

Agreements or Acknowledgements

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

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

About ENISA

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

Contact details

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

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

For questions related to ''Smart Grid Security: Recommendations for Europe and Member States'', please use the following details:

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

Contents

List of Tables

1 Introduction

Information and Communication Technologies (ICT) are envisioned to be the underpinning platform of smart grids, which exemplifies the increasing dependency of European economy and society on Information and Communication Technologies. Thanks to ICT, the grid of the future will become smarter so as to improve reliability, security, and efficiency of the electric system through information exchange, distributed generation, storage sources, and the active participation of the end consumer. However, vulnerabilities of communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants. This was demonstrated for instance in 2009, when officials from the US public administration recognised that cyber spies from China and Russia had hacked into the US electricity grid and hidden software that could be used to disrupt power supplies (1). Smart grids give clear advantages and benefits to the whole society, but the dependency on computer networks and the Internet into future grids makes our society more vulnerable to malicious attacks with potentially devastating results. Additionally, it is largely acknowledged that the smart grid will also introduce privacy problems regarding the data protection of end-consumers information.

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

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

This annex provides a brief overview on the basic ICT security concepts affecting smart grids environments. The next section provides a review of real incidents or events affecting power grids which show that cyber security can have real consequences. Chapter 3 makes a review on risk factors and vulnerabilities that should be considered when protecting smart grids, including aspects such as technological vulnerabilities, human factors or physical security. Section 4 is devoted to the threats and attack scenarios that can take advantage of the vulnerabilities presented in section 3. Chapters 5 and 6 are directly related to the main challenges that security professionals will have to face when protecting smart grids. Finally,

chapters 7, 8, and 9 provide an overview on the policy context and the security standards that are being defined at the level of smart grid security. Besides, an outlook on the main security initiatives at the EU-level is presented. These are initiatives which are trying to overcome some of the main challenges that are presented in section 6.

2 The cyber security problem in the smart grid: Real Incidents.

The real cyber security incidents and related events that will be presented in this section show that the current grid is not secure. Besides, the grid is getting smarter thanks to massive deployment of ICT, and the number of actors will significantly increase (e.g. service providers, marketers, prosumers, etc.). This will introduce new risks, and therefore novel strategies should be defined to cope with them.

Attacks against the power grid can directly impact society's way of life. Public bodies and C-level staff of the utilities operating the distribution and transmission networks, as well as electricity marketers and generation organisations should be aware of this situation. Without them it would be unfeasible to put in place the necessary mechanisms to improve the security posture of their current networks and to include cyber security as a primary objective of the smart grids.

Some of the real cases presented in this section remind us that Process Control Systems (PCS) in general, and particularly power grid ICS infrastructures (e.g. SCADA systems), are starting to be seen appealing targets in cyber warfare (2). ENISA's study[2] on the protection of Industrial Control Systems (3) widely covers many relevant aspects that are directly applicable to smart grids. The reader is encouraged to use the associated reports as a complementary source of information to what is explained in this annex.

2.1 Considerations on security incidents

A cyber security incident to power grids could be defined as any adverse event that can impact the confidentiality, integrity or availability of the ICT systems supporting the different processes of the organisations involved in the well functioning of the power system, including all its domains (e.g. markets, operation of the distribution or transmission grid, customers, etc.). For instance, a successful penetration of the SCADA systems in a distribution substation could be used to directly impact substation automation processes and in turn any other process that might me critical for the operation of the distribution grid.

Incidents could impact power grids in many different ways. The consequences can range from relatively benign disruptions to deliberate acts of sabotage intended to cause harm, threatening lives of citizens and even national security. Besides, economic or administrative penalties to grid utilities should not be dismissed. This could be the result of not complying with Service Level Agreements (SLAs) or national laws and other regulations on civil responsibility and national security.

It should be stressed that, not only deliberate attacks should be considered. It has been widely demonstrated that a large portion of cyber incidents can have their root in accidental human errors. The reader is encouraged to read section 1.1.3 of the first annex of ENISA's study

[2] *The reports associated to this Study can be accessed directly at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems*

report on the protection of ICS (3). This section provides a detailed categorisation of possible incidents according to the level of intentionality.

The following is a list with a number of highly-visible examples of attacks that could be crafted against smart grids. This list is based on the work done by the team of WP1.2 of DG CONNECT's Ad-Hoc EG (4) as well as on the book "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems" (5):

- Delay, block, or alteration of the generation process of an electric generation facility, resulting in the alteration of the amount of energy produced.
- Delay, block, or alter information related to a process, thereby preventing a bulk energy provider from obtaining production metrics that are used in energy trading or other business operations.
- Fraudulent information about demand or supply causing automatic measures taken which try to deal with non-existing power flows. Result may be a blackout and/or high financial losses.
- Deliberate energy market manipulation by changing smart grid information about the power demand or supply in a stressed market.
- A physical and/or cyber attack on a (small set of) single-point-of-failure smart grid component(s).
- Technology Related Anger (TRA) of smart grids amplified by a very active (set of) individual(s), e.g. peoples sending tweets like 'Smart grid equipment radiation is deadly', while lacking a convincing mitigation strategy.
- Organised crime manipulating larger sets of consumer premises smart grid components or at the data concentrators, e.g. turning a large set of smart appliances off.
- The AMI being an entrance point to the smart grid network for hackers/criminals.
- Privacy-related information in Smart Grid components/(wireless) network links of smart grids that is used by criminals or hackers to create reputation loss of one or more stakeholders or even TRA and/or massive technology-related distrust by citizens.

2.2 Examples of real security incidents affecting power systems

Considering **power generation**, in March 2008 the Edwin I nuclear power plant in Georgia (USA), was forced to make an emergency shutdown for 48 h due to a software update. This software update was applied to the computer system in charge of monitoring chemical and diagnosis data of one of the plant's primary control systems. After applying the update, the computer was rebooted and this lead to a lack of monitoring information. Safety systems misinterpreted this and signalled that the water level in the cooling systems for the nuclear

fuel rods had dropped, which caused an automatic shutdown. There was no danger to the public, but the power company lost millions of dollars in revenue and had to incur the substantial expense of getting the plant back on-line.

In terms of the **distribution and transmission** domain, one of the most relevant incidents could be the attack suffered by the US electrical grid in 2009. Officials from the US public administration recognised that cyber spies from China and Russia had hacked into the US electricity grid and hidden software that could be used to disrupt power supplies (1). It was confirmed that attackers could use this software backdoors to cut electricity at will. In order to fully understand the real scope of such an attack, it is worth highlighting the words of a senior intelligent official about it. He said: "If we go to war with them, they will try to turn them (i.e. the software backdoors) on" (6) .

Concerning AMI, at the US Black Hat conference of 2009, Mike Davis, an IOActive security consultant, proved the weaknesses of the whole metering architecture and in particular of smart meters that were being deployed on those days. By means of a proof of concept he demonstrated that a cyber attack could be used to get remote control of about 15,000 out of 22,000 homes in a 24 hours time. To show that Mike Davis and his team created a simulator as well as a real piece of malicious software (i.e. a worm) capable of self-replicating and self-distributing across an area where all houses are equipped with the same brand of meter (7).

Unfortunately, the FBI recently discovered that smart meter installations are already facing real cyber attacks. In 2009 an electric utility in Puerto Rico asked them to help investigate widespread incidents of power thefts that it believed were related to its smart meter deployment. The FBI discovered that former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash. Presumably, they hacked into the meters using an optical serial port that allowed them to connect their computers locally and change the settings for recording power consumption. They just needed a software program that could be directly downloaded from the Internet.

2.3 Relevant incidents with proper name

In June 2010, the malicious software **Stuxnet** was detected. This piece of malware has the properties of a worm since it exploits several vulnerabilities in order to infect other systems and at the same time it is considered an ICS rootkit since it inadvertently modifies the way in which PLCs behave. This worm was conceived as a cyber weapon for sabotage. It focuses on Siemens specific software and hardware, modifying the logics of Siemens S7 PLC microcontrollers and hiding this from the supervisory software application/operators. Stuxnet is a very advanced piece of software: it exploits several zero-day vulnerabilities, it makes use of valid (stolen) digital certificates, and it masters Siemens WinCC SCADA application. Public press reported that security experts consider that only governmental services may have the capacity and resources to produce and release such a sophisticated attack tool. There is no official confirmation but security experts think that Stuxnet's target was the Iranian Natanz nuclear facility which is considered by many to be a key part of Iran's nuclear weapons program. Moreover, it was confirmed that since Stuxnet they have suffered numerous faults

with no straightforward explanation. The reader will find very detailed information in the Symantec Dossier (8).

Night Dragon was the name given to a number of targeted attacks. Their main objective was to compromise the industrial control system of several energy companies in the United States, including oil, gas and petrochemical companies. According to the report by the company McAfee (9), attacks are believed to have their origin in China. These attacks relied on a combination of several techniques, tools and vulnerabilities (i.e. spear-phishing, social engineering, Windows bugs and remote administration tools – RATs–). Although the attacks were not very sophisticated and did not exploit any zero-day vulnerability, the information obtained by attackers was very valuable for competitors. That information included financial documents, related to oil and gas field exploration and big negotiations, as well as operational details of production supervisory control and data acquisition systems.

Duqu is a computer worm that was discovered in September 2011 and which is believed to have been created by the same authors of Stuxnet, or at least that its authors had access to the source code of Stuxnet. However its purpose was totally different to that of Stuxnet. Duqu main objective was to collect information such as keystrokes and system information to prepare future attacks against industrial control systems. Duqu's executables have been found in a limited number of organisations, including those involved in the manufacturing of industrial control systems. Experts are still analyzing the code but they consider that Duqu may be used to enable a future Stuxnet-like attack or might already have been used as a basis for the Stuxnet attack.

3 Vulnerabilities and risk factors

As already mentioned, ICT are critical for the implementation of smart grids. ICT will play a vital role in the reliability and security of power systems and therefore, the protection of current and new ICT technologies must be addressed by the electricity sector. This is not only a task of grid operators but also of public bodies, standardisation organisations, academia, new service providers, and any other stakeholder.

Cyber security must be considered in all domains of the smart grid and at all phases of the system life cycle, from the design phase to decommission, through development, deployment, maintenance, etc. Besides, cyber security must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, or terrorists. As we already discussed in the previous section, inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters should also be considered (10).

Achieving a secure smart grid will not be an easy task. There are a series of vulnerabilities/weaknesses that must be identified and analyzed first and then try to get solved through risk management processes. However, there are a number of challenges, such as technological gaps, organizational problems or awareness issues that must be solved to achieve this objective. This section will provide an overview on the most relevant vulnerabilities and risk factors affecting the smart grids and in following chapters a detailed discussion on the greatest challenges for addressing them will be also provided.

3.1 General considerations

Cyber security vulnerabilities/weaknesses are conditions present in any cyber asset or organisational process at different levels, including its design, implementation, configuration, operation or management. Smart grids make heavy use of ICT and therefore attackers could exploit these vulnerabilities for a number of different purposes: penetrate DSO's corporate network; gain access to control software either in substations or central systems; manipulate smart meters to commit fraud, introduce malware to gain remote control, etc. Besides, smart grids offer cybercriminals with more entry points than today's grid. A two-way communication infrastructure will connect every house and building to the DSO, what notably widens the attack surface.

On the other hand, smart grids can be considered as a large system of systems. They span the whole electricity value chain, from generation to consumption. Many smart grid applications and features depend on each other and many times these applications and features are not under the control of the same actor. This is the case of Advanced Distribution Automation, which heavily depends on substation automation but also needs AMI data and Distributed Energy Resources information to perform correctly. Therefore smart grids can be seen as a system of heterogeneous interconnected systems (i.e. virtual power plants, transmission grid, distribution grids, etc.), each one with its own set of communication equipment and technologies, intelligent devices, automated control elements and algorithms, processing applications, connection points, specific procedures, different organisational approaches, etc.

This heterogeneity, diversity and complexity make highly difficult its protection and at the same time introduce new and complex (and likely vulnerable) interrelationships and dependencies which were not present in traditional power systems (11).

3.2 Cyber vulnerable ICT components of the smart grid

Vulnerabilities can be of different kind (e.g. management, organisational, etc.). This section provides a brief list of smart grid's ICT components that need to be considered as a source of vulnerabilities. It is a top-level categorization of utilities' infrastructure components that can have cyber-vulnerabilities (12). It is worth to highlight that in this report, Industrial Control System related technologies are being considered part of the whole set of ICT supporting the operations of the smart grids. The list is the following:

- **Operational systems:** generators, transformers, Supervisory Control & Data Acquisition (SCADA) Systems & Energy/Distribution Management Systems (EMS/DMS), programmable logic controllers (PLCs), substations, smart meters, and other intelligent electrical devices (IEDs).
- **Classic IT systems:** PCs, servers, mainframes, applications, databases, web sites, web services, etc, among which include the components of corporate infrastructure.
- **Communications networks and protocols:** Ethernet, Wifi, PRIME, DLMS/COSEM, Zigbee, 4G, DNP3, etc.
- **End points:** smart meters, EVs, smart phones and other mobile devices. Taking into account both physical and logical aspects.

For each particular case a vulnerability discovery and identification process must be conducted in order to identify all the vulnerabilities/weaknesses that affect the utility company. Annex I already covers most of the ICT applications and technologies which are envisioned to be enablers for the success of the smart grids and source of new vulnerabilities. We recommend the reader to have a quick look to this document so as to get a wide knowledge of all of them.

3.3 About technological vulnerabilities

The smart grids will bring a whole new range of applications and underlying technologies and communication protocols. However, those based on structured languages and web-based technologies (e.g. web applications and their supporting web services, application and http servers) are going to be a main player in smart grid implementations. For instance, these technologies will allow for remote control of the smart appliances and energy management systems located in Home Area Networks (HAN), either by the home proprietary or by the company providing energy-related services to the end consumer. Another example where web-based applications will play an important role is advanced metering applications. Such applications will make use of real-time access to energy rates and consumption information for demand-response functionalities and in a hope to achieve a more efficient use of the generated power. Even though other technologies – old and new ones – will coexist with web-

based applications, the latter is the spearhead of the new and perfectly exemplifies what could be the next generation of ICT-based vulnerabilities in power grids. As it has been demonstrated in other businesses, by implementing these technologies, utility companies will have to take much care to avoid implementing a single point of failure as well. Attacks that in the past would require exploits of multiple vulnerabilities to bypass multiple layers of control or the lack of interoperability among systems, may now be simplified to a single attack vector in smart grids.

Communications protocols used in smart grids are also an important source of vulnerabilities. Particularly, some of the wireless protocols to be used in smart grids (e.g. Zigbee, Wimax, Wifi, LTE, UMTS, GPRS, etc.) are already widely used in other businesses and therefore many of their vulnerabilities are well known by attackers, and automated tools are available easing their exploitation. In most cases, attackers targeting smart grids will attempt to attack wireless networks in order to cause a denial of service, get sensitive information, or bypass perimeter security controls so as to gain access to internal networks. Unfortunately, not only wireless protocols are affected by vulnerabilities. The use of certain application technologies, such as the aforementioned web-based technologies, also implies the use of certain application-level protocols. This is the case of XML over http for web service applications or of DLMS architecture for DLMS/COSEM-based applications. Many of these protocols have been designed with a lack of intrinsic security mechanisms. Moreover, some of the newest ones, which already include high-level security profiles, also include low level security profiles or not security at all. Securing many of these protocols require in many cases the implementation of highly complex encryption technologies requiring a good amount of computational power. Cost reduction pressures coming from utilities, together with a lack of security expertise and awareness in smart grid manufacturers and vendors, results in smart grid equipment lacking of the necessary security capabilities to guarantee the necessary security level on smart grid communications. Finally, the use of legacy SCADA protocols which were development without taking in count security requirements should not be dismissed. Besides, securing these protocols is not straightforward. We recommend the reader to check Annex I of ENISA's study on ICS protection (3) for more information on the security issues of ICS/SCADA protocols.

3.4 Human factors

Human factors include all those human aspects and conditions that an attacker could take advantage of to successfully achieve its malicious objectives. These human aspects and conditions are directly dependant on the security training employees receive and the awareness-raising actions being undertaken by organisations.

Social engineering attacks will test security awareness and training of the employees of smart grid operators, manufacturers, end consumers, etc. For instance, an attacker may try to impersonate an employee from the utility's contractor to ascertain confidential information such as authentication credentials, or to get additional privileges in certain equipment. Common examples of social engineering attacks also include the following:

- Impersonating an employee in front of the IT Help Desk to change his or her password

- Impersonating contractors to obtain potentially sensitive information or sabotage equipment.
- Leaving USB key drives containing malicious software at strategic locations so as to install a backdoor into the IT/smart grid infrastructure.
- Sending "phishing" e-mails targeting sensitive information such as customer information. Nowadays there are many social networks (i.e. professional networks) that make this task much easier (13).

3.5 Physical security

Utility companies can have thousands of miles of power lines that could be susceptible to physical attacks. This is especially true in smart grids where power will be generated by a combination of distributed energy resources based on renewable energy and conventional bulk energy plants. Besides, distribution networks will tend to be meshed networks so as to support intelligent power flow rerouting. Likewise smart meters will be installed in customers' homes and businesses. Therefore, fortifying smart grid's critical information infrastructure is sometimes a new and surely a daunting challenge due to the extensive network and large number of components that if is comprised of. For example, a utility can do little to prevent a motivated person from cutting down a transmission line or physically tampering a smart meter (14). Therefore, physical and cyber security will have to be managed in an integrated way.

3.6 Information sharing

The electricity industry does not have effective mechanisms in place for sharing and managing information on cyber security incidents. The electricity industry lacks an effective mechanism to disclose information about smart grid cyber security vulnerabilities, incidents, threats, lessons learned, and best practices. Furthermore, in some regions such as the US, the existing regulatory environment is somehow contributing to create a culture of compliance instead of a culture focused on achieving a comprehensive and effective cyber security. To this respect, and due to the immaturity of the industry with respect to cyber security, vendors and operators are implementing security controls using a variety of standards together with own proprietary mechanisms. This leads to poor interoperability, lack of true security and even in difficult security management.

3.7 Education and training

Furthermore, it is necessary to emphasize that consumers and utilities are not adequately informed about the benefits, costs, and risks associated with smart grid systems. This lack of awareness can result in a lack of the necessary investments, standardisation actions, regulatory and policy initiatives, etc. Therefore, education and training together with awareness raising initiatives should be fostered to create the necessary momentum for fostering the development and deployment of fully secure smart grids (15).

3.8 Summary

Smartening the grid implies making extensive use of ICT technology. At the same time, smart grids are complex systems where multiple actors are involved, many more than those traditionally related to power grids. In the following lines we provide a summary on the most relevant facts that can be derived from previous sections:

- Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors.
- Interconnected networks can introduce common vulnerabilities, such as communication protocol vulnerabilities or IT vulnerabilities.
- Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks.
- Increased number of entry points and paths are available for potential adversaries to exploit.
- Interconnected systems can increase the amount of private information exposed and increase the risk when data is aggregated.
- Increased use of new technologies can introduce new vulnerabilities.
- Smart grids will expand the amount of collected data that can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.
- Awareness of the companies' employers is important to prevent the success of social engineering attacks, as for instance avoiding the introduction of malware in the smart grid systems.
- Raising awareness of consumers and utilities about the benefits, costs and risk associated with smart grid is necessary.
- Regulations should focus on pointing – by means of promoting best practices or policy actions – the way ahead so as to guide vendors and utility companies in considering security from a holistic point of view.

4 Threats in smart grids

Threats can be defined as “possible actions that can be taken against a system” (16). These actions may aim to cause harm in the form of death, injury, destruction, disclosure of private information, interruption of operations, or denial of services. It is quite usual to find partial descriptions of threats affecting critical infrastructures such as smart grids. They are normally based on specific characteristics, such as the threat agent behind it, the degree of intentionality, the way in which the threat agent is organised, etc. In this section we will compile an overview of the current threats that could affect the smart grid from a set of various documents where this topic is addressed. Before, we present a brief overview on the different ways in which threats can be classified.

4.1 Threat classification

Depending if threats are accidental or deliberate the following classification can be made:

- **Accidental/Inadvertent threats:** Security threats to assets can result from inadvertent events. In fact, often more actual damage can result from safety breakdowns, equipment failures, carelessness, and natural disasters than from deliberate attacks. CIs are accustomed to worrying about equipment failures and safety-related carelessness. However, someone unfamiliar with proper procedure and policy still causes an accidental risk. At the same time, it is also likely that an organization does not know all the risks and may uncover them by accident as it operates complex industrial automation and control systems. Fortunately what is changing is the importance of protecting Information which is becoming an increasingly important aspect of safe, reliable, and efficient process operations.
- **Deliberate threats:** it is important to highlight that the reactions to successful deliberate attacks can have tremendous legal, social, and financial consequences that could far exceed the physical damage.

Accidental/inadvertent threats may be further divided into:

- **Safety failures:** “Safety has always been a primary concern for CIs. [...] Meticulous procedures have been developed and refined over and over again to improve safety. Although these procedures are the most important component of a safety programme, monitoring of the status of key equipment and the logging/alarming of compliance to the safety procedures through electronic means can enhance safety to a significant degree, and can benefit other purposes as well” (17). For instance, electronic monitoring of safety measures inside electric power substations can also help to prevent some deliberate attacks, such as vandalism and theft.

- **Equipment failures:** These are the most common and expected threats to the reliable operation of the power system. Significant work has been undertaken over the years: redundant components and networks, equipment status monitoring, etc.
- **Carelessness:** Often carelessness is due to complacency ("no one has ever harmed any equipment in a substation yet") or laziness ("why bother to lock this door for the few moments I am going into the other area") or irritation ("these security measures are impacting my ability to do my job"). Examples of carelessness threats include: permitting tailgating into a substation; not locking doors; inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards; applying updates, corrections and other changes to operating systems and control applications without a previous test in a controlled environment; etc.
- **Natural disasters:** storms, hurricanes, and earthquakes, can lead to widespread power system failures, safety breaches, and opportunities for theft, vandalism, and terrorism.

There are many other ways in which threats can be classified. For instance threats can be characterised based on how threat agents are related to the target company/system (i.e. outsider and insider), or depending on how the threat agents organise themselves and the resources and support they have (e.g. lone/small groups, criminal groups, terrorists, etc.), or even based on the attacking techniques (e.g. physical attack, malware, theft, etc.). A more detailed classification can be found in Annex I of the ENISA's study on ICS protection (3).

4.2 Threats affecting smart grids

Characterizing cyber security threats to smart grids is a difficult task since there is relatively little statistical data on security breaches. Smart Grid is a new concept. As a result there is very little practical experience on cyber attacks affecting these infrastructures. Besides, ICS and industrial cyber security is also a quite new topic and security experts are still learning the topic, developing hacking tools and finding new vulnerabilities at an exponential rate. On the other hand, physical security and safety is much more stable and well-known by the actors involved in the smart grid deployment. For instance, there is lot of statistical data about natural disasters, such as hurricanes or earthquakes, which makes it much easier for experts to characterise these threats from a risk point of view. Alternatively, natural disasters are random events while cyber threats depend on persons (i.e. attackers), their motivations, capabilities, interests, etc. Besides, all these factors change over time. Therefore, managing risks deriving from cyber security threats is a real challenge that needs to be solved. In order to succeed in such task it is important to firstly identify potential threats, at all levels, from natural disasters to very technical aspects. When identifying threats, it should be not only consider those targeting primarily infrastructure operations, but also those targeting the end consumer (i.e. privacy aspects) as well as national security related factors (i.e. government personnel; other national facilities, assets, and interests identified by national intelligence, etc.) (18).

Bearing in mind the above considerations, the following table shows a possible classification of threats. As the reader will notice, not only security threats have been included but a wider scope has been considered for shake of completeness.

Threat classification	
Type	**Threat**
Technical	Malware
	Non optimised processes
	Weak innovation
	Manipulation of device's internal electronics
	Physical manipulation of devices' subcomponents
	Removable component replacement
	Manipulation of home devices
	Unauthorised firmware replacement
	Compromised firmware update
	Escalation of privileges
	Sensible information interception
	Alteration of information in transit
	Traffic injection
	Sensible information theft
	Credentials discovery
	Partial denial of service
	General denial of service
	Breakdown
	Propaganda
	Disclosure of information
	Disinformation
Corporate Image and Information management	Low quality information for decision making
	Damage to Brand Image/reputation
	Rumour
	Bad patenting policies and procedures
	Weak knowledge of regulations
	Lack of comprehensive insurance coverage
	Unfavourable contractual agreements
Legal, social aspects and human ethics	Non compliance with national and international regulations
	Strike
	Sabotage

	Retention
	Faked sickness
	Incompetence
	Bribery
	Dishonest behaviour
	Employee unreliability
	Error
	Illicit action
	Panic
	Epidemics
	Penuries
Organizational	Weak relations between management staff
	Weak internal controls
	Not respected management
	Procedures are not followed
	Illness
	Badly controlled outsourcing
	Low morals
	Labour accidents
International Relations/Politics	War
	Terrorism
	Regional conflict
	Organised crime
	Kidnapping
	Government corruption
	Mass psychoses
	Group anarchy
	Riots
Marketing/Economical/Financial	Volatile market
	Product/service boycott
	Unsuccessful merger/acquisition
	Bad product/service performance
	Non adapted product
	Unsatisfied client
	Bad strategic decisions
	Client dependence
	High competition
	Interrupted production
	Negative Return on Investment (ROI)

	Debt
	Low capital
	Demands of shareholders
	Untrustworthy financial sources
	Slowdown in economic growth
	Fraud
	Insufficient resources
Environment	Natural catastrophe
	Pollution
	Nuclear catastrophe
	Biological disaster
	Chemical disaster
	Radio-electric incident

Table 1 Threats affecting smart grids

5 Managing risks in smart grids

Power grids infrastructures are essential to enable and support knowledge and innovation based economies. This is why EU Member States so heavily depend on the reliability of the power systems. The changes that smart grids will bring into today's power grids will probably make the whole system less reliable in the first term, as many more stakeholders participate in the network, demand increases, and the necessary ICT is implemented. For these reasons, it is of high importance to systematically analyse and manage the new risks associated with the smart grids. In order to achieve it, risk assessment/management methodologies and strategies are of paramount importance. In the following lines a brief overview on some of the ongoing initiatives addressing this topic is provided. Besides, this section also compiles a number of considerations that are relevant when dealing with the risks deriving from ICT that affect smart grids.

5.1 Risk assessment methodologies for smart grids

Cyber risks management could be defined as the program and supporting processes used to manage cyber-security risks to an organization's operations. In order to effectively perform risk management, an entity must have a thorough understanding of their people, processes, and technology, as well as on how they enable achieving the objectives defined in the business strategy. Each organization needs to identify its most critical assets, assess the risks, and establish and implement a risk management strategy. Furthermore, the management of risks should be a continuous process that should include risks reassessments so as to ensure that new threats are considered, all vulnerabilities are being adequately managed and countermeasures are being effectively implemented.

In order to provide smart grid organisations with a reference on how to implement risks management programmes within smart grid related organisations (e.g. public bodies, TSOs, DSOs, ...), some guidelines and documents have been published or are currently under development. For instance, US DoE's "Electricity Sector Cybersecurity Risk Management Process" (19) guideline presents a model which is meant to "take this routine process and formalize it to ensure that risks are identified appropriately and responded to in a way that best carries out the mission of the organization". At the EU level, the DG INFSO's ad-hoc EG on the cyber security aspects of the smart grids is also addressing this topic. Specifically, one of the four areas of work deals exclusively with risks, threats and vulnerabilities affecting smart grids. Likewise, the UK government has conducted a risk assessment for the smart metering implementation programme. The results of this assessment are classified as restricted information and cannot be published in this document. The risk assessment was defined using steps 1 to 3 of HMG Information Assurance Standard No.1 (IS1) methodology, a security standard applied to government computer systems in the UK.

One of the first and most important steps in any risk assessment is the identification and categorization of the most relevant assets. DG INFSO's ad-hoc EG suggests[3] defining different impact scenarios/magnitudes against which smart grids should be protected, and then classify assets based on the level of criticality with respect to these scenarios. They recommend including all critical energy assets within the transmission, distribution and generation domains. They propose the following asset classification:

- Those assets that could cause an international cross border, national or regional power outage or damage to infrastructures.
- Those that could cause a significant impact to energy market participants,
- Those that could cause a significant impact on operations and maintenance processes of the energy grid
- Those that pose a significant risk to personal data of citizens (i.e. privacy)
- Those that might cause significant safety issues for people

Additionally, the DG INFSO ad-hoc EG also reflects on the different types of cyber assets. According to them, the Smart Grid architecture involves many cyber assets, where some have been part of the grid for a while (i.e. SCADA, RTUs, etc.) and others are new "smarter" assets (i.e. AMI, IEDs, smart meters, etc.). Regarding the latter, it is explained that they "contribute to the automation of processes and increased controllability of the grid. Consequently they increase the overall risk considerably due to the large numbers of devices, and their collective impact. Their impact can be in any or multiple layers hence the security mechanisms need address other vectors as well". On the other hand, when describing "traditional" cyber assets, they explain that the number of this type of assets is much lower than "smarter" cyber assets. However, the potential impact of each one of these assets could be much higher, comparable to the impact that a large number of "smarter" assets could have (e.g. collection of smart meters). Therefore, these assets then form the high value targets that have a different protection need.

Another major point in any risk assessment methodology is the identification and evaluation of threats. It is essential to effectively analyse and characterise the threats (i.e. identify threat agents, their resources, motivation, vulnerabilities, etc.) so as to have a clear picture of the probability and impact on the different critical assets. This process also helps determine which measures to take in order to mitigate the overall risks. This has already been introduced in the previous chapter and will not be detailed here. However, it is interesting to provide some significant aspects highlighted in the different guidelines out there or under definition. For instance, the US Guidelines on the cyber risk management process for the electric sector (19) considers the following threats agents/sources: i) people (malicious violation of policies by current/former employees and third-party personnel); ii) processes (missing or deficient procedures); technology (component failure through design, implementation, and/or maintenance); external disasters (natural or man-made); and systemic, recurring cyber

[3] *The work of DG INFSO's ad-hoc EG is still under development. The information presented in this section referring to this EG cannot be considered official.*

security incidents. On the other hand, DG INFSO's ad-hoc EG suggests that the threat classification step should encompass both the information and the infrastructure dimensions of smart grids and comprise: (1) threats to the confidentiality, availability and integrity of data in the system, (2) threats to the resilience, security and proper use of the infrastructure as a whole, (3) threats to the environment of Smart Grid operations, and (4) inter-organisational related threats. This EG also provides a complete taxonomy of threats against the smart grid and specifically warns about the fact that there exist multiple opportunities to deliberately affect the functioning of smart grids. They specifically suggest that "risk analysis should consider the likelihood of **specific actor** types having the opportunity to exploit vulnerabilities of Smart Grids by effectuating a certain threat to a certain (set of) deployed Smart Grid component(s) or asset(s) using a certain motivation and the availability of means".

The process of information security management and in particular of risk management includes assigning priority to risks, establishing a budget for the measures to be implemented, and finally implementing and maintaining the selected risk reduction measures (i.e. safeguards). To this respect, it is important to previously identify the current security mechanisms and evaluate their effectiveness. Considering and choosing the appropriate measure requires a cost/benefit analysis approach. It is interesting to understand the cyber security challenges of smart grids in order to define and implement the appropriated safeguards. Some of these safeguards could include high level actions beyond the scope of a single organization (e.g. promote the application and adaption of well-established ICT security good practices; stimulate inter-organisation actions). As usual, other safeguards should be considered by Top Management to addressed risks specific to an organisation (i.e. establish an information security policy, considering physical and environmental security controls, etc.). However in this case, the specificities of industrial control and automation systems should be taken into account to establish the appropriate technical and compensatory controls so as to assure that security does not affect their operation.

5.2 The CIA Triad

Security requirements for the information infrastructure of the smart grid are similar to typical corporate information systems. However, when it comes to managing the risks, strategies and priorities are significantly different and heavily depend on the domain we are focusing on (20). From an operational perspective, there are two major classes: 1) when we focus on grid automation and supporting ICS (e.g. SCADA, RTU, PLC, IED, etc.); 2) when we focus on value-added service provided to end consumers and supporting infrastructures (e.g. smart meters, energy management systems, etc.). The latter is a domain very much similar to traditional ICT businesses, something that will be explained more in detail in the following lines.

Managing ICT security is normally based on three fundamental dimensions, which are Confidentiality, Integrity and Availability, and which is commonly known as the CIA triad. These dimensions are used to define risk management priorities, classify information, characterise security requirements, and so on.

In the following lines we will explain these three dimensions and their importance on smart grids:

- **Integrity** focuses in identifying and preventing data to be modified without authorization. In smart grids it would include aspects such as: have control commands and power control readings been modified during their transmission through a communication infrastructure, or during their storage in a historical data base? If they have been modified, has this been done by an authorised entity? Integrity is equally important either it concerns to grid automation systems or data or if we consider value-added services for end consumers at their homes or businesses.
- **Availability** focuses in identifying and assuring data and services that need to be available for a specific purpose at a very precise time. When talking about smart grids, availability is a key aspect in real-time systems, such as the SCADA servers of DSOs' and TSOs' control centres. Availability is critical for systems supporting grid automation, while is less important in smart metering applications.
- **Confidentiality** is the security dimension which analyses whether some specific data should be protected from being accessed by unauthorised parties. It is the least critical dimension when considering grid automation systems and information but a very important one for end consumers. Confidentiality is intrinsically linked to privacy aspects. Therefore, when we think about confidentiality in the smart grid we should consider privacy of consumers, power market information, etc.

There are also two other interrelated security dimensions that may be considered relevant concerning smart grid security. These are **authentication** and **non-repudiation.** The first has already been considered implicitly when describing the CIA triad and deals with making sure that someone or something really is who or what it claims to be. On the other hand, non-repudiation deals with proving that an action has been made by the entity really responsible for that action, or even that a data signal or command has been provided or issued by the actual source. Both dimensions are equally important either in grid automation or end consumer added-value energy services.

The following figure provides an overview of the priority order of the CIA triad depending on which domains of the smart grid we are focusing on. When dealing with grid operation and automation, the priority order is Availability, Integrity and Confidentiality (A,I,C), while when focusing on general purpose ICT processes or smart metering, confidentiality is at the top (C, I, A).

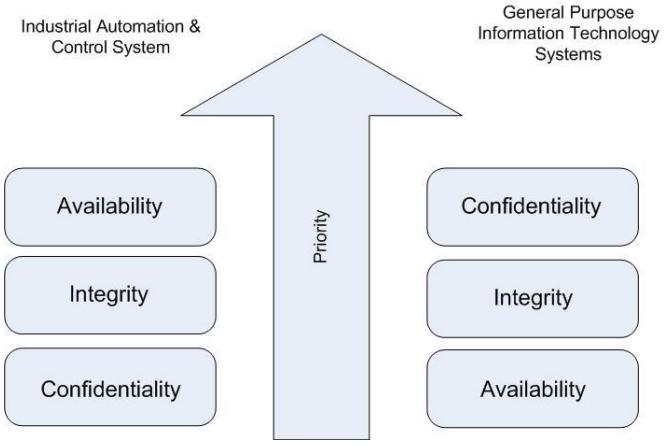


Figure 1 ICT security goals in smart grids

In traditional IT systems information confidentiality and integrity are the main concern. For ICS systems in charge of grid automation human and equipment safety, environmental impacts and the process itself (i.e. power blackouts) are the main concerns. For this reason availability and integrity are the priorities for grid automation.

On the contrary, smart metering security priorities resemble traditional ICT environment. Meter readings are starting to be considered as personal data since they provide knowledge about personal habits (e.g. if someone is on vacations or what movie is their watching). As a result, in what concerns to value-added energy services for end consumers, a CIA approach is preferred over an AIC one (21) (22).

6 Smart grid security challenges

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

I the following lines a description on the greatest smart grid security challenges is presented. Some of them have already been introduced in the previous sections while others are new but equally relevant. The order in which they are presented is not related to the level of importance.

- **Data and information security requirements:** ICT will become the central nervous system of the new smart grids. Data and information flows will flood all domains. In the operational aspects of the grid (i.e. generation, transmission and distribution automation) data integrity and availability will be of paramount importance. Likewise, when dealing with end-consumer related data, such as consumption data or even personal data at the billing systems, confidentiality will need to be guaranteed during transit and storage. Moreover, in some cases the smart grid application will determine which security dimension is more important for a same piece of data. For instance, in demand-response applications, consumption readings coming from smart meters could be used in an aggregated manner for power flows rerouting and grid optimization. In such a case, availability and integrity is absolutely necessary to guarantee that the supervisory control system takes the appropriate decisions.

  Data protection requirements for each smart grid domain and application will have to be clearly defined so that manufacturers, operators and other actors participating in the smart grid development and implementation can establish the necessary security controls as well as develop the appropriate technologies to protect smart grids' data. Data flow encryption, tunnelling, authentication and no repudiation, digital certificates and also other topics such as security in the supply chain, firmware validation or patch management should be addressed.

- **Large numbers of "smart" devices:** The smart grid will result in the deployment of a huge number of electronic and information processing devices configuring a huge mesh. Smart meters and devices and the AMI communication infrastructure in general is probably the most significant example. However, substation automation in the distribution domain together with the smartening of transformer centres will also bring in a huge number of IED and related ICT technologies. Not only deploying but also designing and maintaining a scalable and reliable solution will be a great challenge for grid operators which are not used to it and do not have the necessary systems or even internal processes. Besides, this solution/infrastructure has to be secure considering all the interconnections in place, processes (e.g. firmware updates,

management actions, etc.), or even the devices themselves. This will add a lot of complexity to the issue. Probably, system or software as a service, cloud computing, and security in depth strategies should be considered, especially in the situation of small or medium size operators.

- **Physical security and grid perimeter:** Special attention will need to be paid to physical security aspects in smart grids. The interconnection at the ICT level of households, buildings and industry with DSO and DER information networks will significantly extend the grid security perimeter. For instance, smart meters will not be under direct control of the DSO or retail providers since they will be installed inside the consumer houses, buildings or business. For this reason, they are at risk of being tampered – as it has occurred in the past with electromechanical meters – and suffer a firmware hack or replacement (i.e. "flashing") so as to commit fraud or to get an entry point to the AMI network from where to craft malicious attacks or to propagate malware against other meters, smart grid applications (e.g. demand-response) or even to the back-end systems. On the other hand, due to the increasing automation of the distribution grid, transformer centres and distribution substations are becoming more appealing for cyber attackers. Transformer centres are in many cases not well protected against physical attacks and provide a point of presence of the DSO's ICT infrastructure. Most transformer centres are physically located inside a locked building or locker/closet. Unfortunately, many contactors do have a copy of the key providing access to such installations and the lockers are not sufficiently robust. Anybody with physical access – authorised or unauthorised – to these installations is able to get access to the communication network of the DSO.

- **Legacy and (in)secure communication protocols:** Many of the communication protocols currently in use for the control and automation of power generation, transmission and distribution were never designed with security in mind. Many of these protocols were initially conceived as serial protocols with no built-in message authentication. For this reason devices will accept connections from any device trying to communicate with them mindless they are authorized or not. Besides, none of these protocols use encryption or message integrity mechanisms and as a result communications are exposed to eavesdropping and session hijacking and manipulation. Even though these vulnerabilities have been around for years, new factors have augmented the real risk. Many ICS vendors have begun to open up their proprietary protocols and publish their protocol specifications to enable third-party manufacturers to build compatible accessories. Organizations are also transitioning from proprietary systems to common networking protocols such as TCP/IP (i.e. Modbus/TCP, IEC 104, etc.) or new standard open protocols such as OPC to reduce costs and improve performance. Likewise, standard legacy communication protocols such as IEC 101 can now be found in its TCP/IP encapsulated version, but still with no security mechanism in place. Operators will need to be able to deal with these

shortcomings in the next years, defining novel strategies such as making use of compensatory measures such as protocol tunneling.

On the other hand a totally new set of communication protocols is emerging so as to cope with new applications in smart grids. This is the case of AMI-related protocols such as PRIME, Meters&More, DLMS/COSEM, etc. Fortunately, these protocols are being designed with security principles in mind, including cryptography for end-to-end authentication and encryption. Nevertheless, to successfully implement the highest security, cryptographic material (i.e. keys, certificates, etc.) needs to be managed efficiently and effectively. As it has been already stated before the number of smart devices in smart grids will be really high and therefore, managing cryptographic material will be a complex and tough task.

- **Large number of stakeholders and synergies with other utilities:** The smart grid infrastructure is complex, and by its very definition it needs of a large number of varied stakeholders to collaborate together so as to provide the physical and logical structure for a working solution. Traditionally, the power system was comprised of a small number of actors (i.e. bulk generators, TSOs, and DSOs). However, due to the deregulation of the electricity service first, followed by the redefinition of the power system concept by means of the smart grid, we have come to a situation where a large number of stakeholders are now dedicated to energy delivery and related added-value services. There are different types of stakeholders, but what is more important, there are many more actors involved: end-consumers, small power producers, energy retailers, advanced energy service providers, EV related businesses, etc. The difficulty lies in rapidly coordinating the activities of such a varied group of stakeholders, each one with its own organisational processes, business priorities, information communication requirements, reference regulatory standards and best practices, etc. to provide a reliable, secure, and high-quality power delivery service.

  On the other hand, the concept of advanced metering will not only affect the power sector. It is envisioned that in the upcoming years other utilities such as gas/heating and water will make use of smart meters to remotely read and process consumption data. Synergies are possible and necessary since from a business point of view it would not make much sense to deploy as many AMIs as utility services reach a business or home. For instance, a single AMI could be used for reading any smart meter type (e.g. gas, heating, water, electricity). Data would then be delivered to the back-office systems of the AMI operator (e.g. DSO, energy retailer, gas distributor, etc). Therefore, it seems necessary to develop a flexible, interoperable and well communicated infrastructure that can support all information sharing needed between different utilities. However, this will result in an even more complex system of systems, where not only all the new power grid stakeholders but also other utilities actors will need to be considered when securing the smart grid.

- **Lack of definition of the smart grid concept and of its security requirements:** A large number of technologies and very novel concepts are emerging with the smart grids. They are appearing all at once even though the final picture of what smart grids are is not well defined yet. As a result, security requirements are still to be defined, taking into consideration the different domains involved and their importance for national security or citizens' personal data privacy. It is therefore necessary to create a reference architecture setting down the basic aspects of the smart grids. Besides, the definition of risk assessment methodologies as well as of security best practices and standards addressing system interoperability and considering security as a fundamental aspect is also necessary.

- **Lack of awareness among smart grid stakeholders:** Many of the previous challenges cannot be solved without a real commitment from manufacturers and grid operators and other stakeholders. Actually, one of the main challenges in the field of critical infrastructures is to make C-level staff aware of the cyber security problems that they will face in the short and long terms. This is especially true in the case of smart grids, where ICT will play a key role. Therefore, awareness raising initiatives are necessary. Asking for compliance with specific security standards, conducting risks analyses, making penetration tests, and promoting professional events or actively involving CSIRTs/CERTs are some examples of possible initiatives that could help to this aim.

- **Security in the supply chain:** One of the hot security topics discussed when addressing CI security is how vulnerable current supply chains are. Actually, the risk that the supply chain for electronic components or ICT technologies, including microchips, embedded software, SCADA and control applications, operating systems, etc. could be infiltrated at some stage by hostile agents is very real. These hostile agents could alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry. Moreover, backdoors and logic bombs and other malicious software could be included as part of the firmware of many IED, controllers, or smart meters. As a result enemy states, or terrorists, or any other threat could make use of a backdoor to get remote control of the affected information systems or alternatively take advantage of preinstalled logic bombs that could cause terrible harm.

  The security of the supply chain is of paramount importance for smart grids protection. This is especially true for those applications and components that could be relevant for national security. The design, fabrication, assembly, and distribution of the electronic components and applications will have to be controlled and appropriately regulated. It is important to have in mind the economical dimension of the problem and establish security objectives that are economically viable. The key to solving the problem of malicious firmware is to make the entire global supply chain more secure.

- **Promote the exchange of information on risks, vulnerabilities and threats:** As already mentioned in previous sections, information exchange among smart grid stakeholders

could be a powerful tool to quickly share best practices and solutions on information security management, including security incidents and the strategies used to deal with them, common security flaws and vulnerabilities and remedial actions taken, priority actions to be followed to secure ICS, etc. It is essential to firstly establish a network of contacts at different levels, and then make the necessary arrangements to generate trust and facilitate information exchange. In these initial phases, public bodies such as the national centres for the protection of critical infrastructures could play a very important role.

- **International cooperation:** Even though there might be some differences among the priority targets/objectives of the smart grids around the world, it is also true that there are many points in common. Therefore, it could be highly beneficial for European countries to share their experience and points (i.e. security priorities, requirements, methodologies, etc.) of view with other regions in the World, such as the US, Japan, Australia, Canada, India, etc. Besides, international collaboration would be also necessary to help Europe be one of the World's leaders in the definition and development of security standards affecting the grid of the future. International organisations such as IEEE, IEC, ISO or ITU and their standards and technical documents are the basic reference for manufacturers when developing their systems and applications.

- **Security management process in utilities:** System vendors will play a very relevant role in securing the smart grids. If products are built-in without security functionality or not considering security requirements during the development cycle, the protection of the power grid would be a very difficult task. However, the security of the power grids does not only depend on having secure products. It is a continuous process that will highly rely in power utilities such as DSOs and TSOs. Grid operators must assess the security of their existing systems, especially of ICS and new infrastructural deployments. Furthermore, they have to evaluate and plan new investments to improve the security posture, define security policies and establish procedures, train employees, and last but not least, establish an information security management framework that ensures that all these objectives get done and continuously improved.

7 The European security policy context and related initiatives

In this section we will provide an overview of the current European policy context highlighting the most interesting related initiatives on the context of Critical Infrastructures and CIIP protection. Moreover, a detailed description and analysis of the security aspects in the European policies on smart grids is also presented.

As already explained in the previous chapters, the smart grid concept includes multiple domains, ranging from the distributed power generation to the advanced metering infrastructure, including markets, retailers, transmission systems, distribution infrastructures, and so on. Some of these domains are under the umbrella of Critical Infrastructure Protection (CIP) and Critical Information Infrastructures Protection (CIIP) policies. Therefore it is essential to review these contexts. Moreover, one of the chief objectives of the smart grid in the EU is to "maintain or even improve the existing high levels of system reliability, quality and security of supply". Therefore, security aspects are also a key topic in any policy action specifically targeting the smart grid.

This document mostly focuses on information and network security aspects of the smart grid. Any other related aspect, such as physical security or safety, might also be considered, but only as they are related to information and network security.

Finally, a more exhaustive list and descriptions on the different initiatives in smart grid security (i.e. public agencies, standardization organisms, public-private associations, industry associations, security programmes, etc.) are presented in Annex V.

7.1 Smart grid specific policies and regulations addressing security

In November 2010, the Commission adopted the Communication "Energy 2020 – A strategy for competitive, sustainable and secure energy" (23) (24), COM(2010) 639. This Communication recognises that the existing strategy is currently unlikely to achieve all the 2020 targets, and it is wholly inadequate to the longer term challenges. Furthermore, it considers that "the urgent task for the EU is to agree the tools which will make the necessary shift possible and thus ensure that Europe can emerge from recession on a more competitive, secure and sustainable path". It recognises that information and communication technologies have an important role to play in improving the efficiency of major emitting sectors, by enabling a structural shift to less resource-intensive products and services, by helping achieve energy savings in buildings and electricity networks as well as by turning transport systems into a more efficient and less energy consuming infrastructure. To this regard it refers specifically to the actions set out in the Digital Agenda for Europe at COM(2010) 245 (25). Furthermore, the Communication considers the smart grids and smart metering as enabling technologies for the necessary shift. This Communication also considers Energy security (and safety) in the sense of continuing developing systems for safe nuclear power, the transport of radioactive substances, as well as the management of nuclear waste, or to introduce stringent measures for offshore oil and gas extraction, as well as for new energy technologies like hydrogen safety, safety of CO_2 transportation network and storage, etc. However, ICT –related

security is not considered explicitly, and therefore the only consideration to this regard is the aforementioned reference to DAE.

One year later, the Commission also adopted a Communication on "Energy infrastructure priorities for 2020 and beyond – A Blueprint for an integrated European energy network", COM(2010) 677 (26). This Communication outlines a Blueprint which aims to provide the EU with a vision of what is needed for making European networks efficient. The EC proposes short term and longer term priorities to make energy infrastructure suitable for the 21st century. One of these priorities is the roll-out of smart grid technologies in order to support i) a competitive retail market, ii) a well-functioning energy services market which gives real choices for energy savings and efficiency, iii) the integration of renewable and distributed generation, as well as iv) to accommodate new types of demand, such as from electric vehicles. Furthermore, the Communication states that the timely establishment of technical standards and adequate data protection will be key to this process, proposing intensifying the focus on smart grid technologies under the SET-Plan. The Communication also refers to the Task Force on smart grids established by the Commission in November 2009 which has the mandate of advising the Commission on the EU level policy and regulatory actions and to coordinate the first steps towards the implementation of smart grids, including aspects on data safety and data protection. For more info on this initiative see section 8.1.

In April 2011, COM(2011) 202 on smart grids, "Smart Grids: from innovation to deployment" (27), the Commission identifies challenges on smart grid deployment and proposes to focus, among others, on developing technical standards, ensuring data protection, and providing continued support to innovation for technology and systems. Regarding to privacy context, the European Commission has conformed a group of high-level stakeholders to assess the network and information security and resilience of smart grids as well as to support related international cooperation.

With respect to the development of common European smart grid standards, the Commission issued a mandate (M441 (28)) to the European Standardisation Organisations (ESOs) CEN, CENELEC and ETSI to establish European standards for the interoperability of smart utility meters (electricity, gas, water and heat), addressing interoperability and communication protocols and their security aspects. The scope of the mandate has been further refined with intermediate findings of the Smart Grid Task Force, and the first deliverables are expected by the end of 2012. Likewise, in March 2011, the Commission issued another mandate to ESOs on Smart Grids, M490 (29), where they are requested to develop a framework to enable (ESOs) to perform continuous standard enhancement and development in the field of smart grids, while maintaining transverse consistency and promote continuous innovation. This has to be done by the end of 2012. Building, Industry, Appliances and Home automation are out of the scope of this mandate; however, their interfaces with the smart grid and related services have to be treated under this mandate. The expected framework will consist of i) a technical reference architecture of the smart grid, ii) a set of consistent standards which will support the information exchange (communication protocols and data models) and the integration of all users into the electric system operation, and iii) sustainable standardization

processes and collaborative tools considering security and privacy as high level system constraints. This framework will build on the Smart Grid Task Force reports as well as the material already delivered through other mandates, such as M441.

According to addressing data privacy and security issues, one of the main topics identified by the Commission in COM(2011) 202, it is acknowledged that, for the acceptance of the smart grid by consumers, it is essential to develop a legal and regulatory regimes that respect data privacy and facilitating consumer access to and control over their energy data processed by third parties. Directive 95/46/EC (30) on the protection of personal data constitutes the core legislation governing the processing of personal data. It is technology-neutral and applies to any sector, and therefore affects some smart grid aspects. The key aspect here is the definition of personal and non-personal data. When the processed data are technical and not relate to an identified or identifiable natural person, companies could process them without needing to seek prior consent from grid users. To this regard, the Smart Grid Task Force has agreed that a "privacy by design" approach is needed. As a result, the standards being developed by the ESOs will integrate this concept. In addition to privacy issues, the Commission launched a multi-stakeholder group for high-level discussions which will focus on cyber security and resilience challenges of the infrastructure supporting the smart grids. This is presented on COM(2011) 202 as an action on data privacy and security in smart grids. The group is called "Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grid" and is further described in section 8.3.

7.2 Policies on CIP

Due in part to the terrorist attacks in Madrid, in March 2004, against the suburban railway service, the European Council of June 2004 asked the Commission for the preparation of an overall strategy on critical infrastructure protection.

In October 2004, the European Commission (EC) adopted the Communication on "Prevention, preparedness and response to Terrorist Attacks", COM(2004) 698 (31), provided a non-exhaustive list of the different policy areas where the Commission was currently contributing towards the implementation of the Union's Plan of Action on Combating Terrorism. This list included: external cooperation, integrating European and national systems, authorities' communication with the public, linking-up with the law enforcement community, the security research priority, the role of the private sector, and explosives.

In the same date, and accompanying three other simultaneous Communications, the Communication from the EC on "Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702" (32), proposes the creation of a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical infrastructure Warning Information Network (CIWIN) as additional measures to strengthen the EU's Critical Infrastructure Protection (CIP) capabilities. This Communication also provides the definition of a Critical Infrastructure and enumerates an exemplary list of generic CI's. It also provides initial discussion on the criteria for determining what CI's are. Critical infrastructures were defined as "*those physical and information technology facilities, networks, services and assets which, if disrupted or*

destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States".

In December 2004, the European Council provided their conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" in which they endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP).

In November 2005 the EC presented the Green Paper on "A European Programme for Critical Infrastructure Protection, COM(2005) 576 (33)", a follow-up publication which addressed the definition of European Critical Infrastructures (ECI's) and National Critical Infrastructures (NCI's). This Green Paper compiled the main results of two seminars and other participative work in which Member States and industry associations participated. As a result, this document outlined policy options on how the Commission could establish EPCIP, including also specific ones for the CIWIN.

The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection.

The EC responded to this request setting out the principles, processes and instruments proposed to implement EPCIP, by adopting in December 2006 the COM(2006) 786 (34) "on a European Programme for Critical Infrastructure Protection". In this Communication, the purpose (i.e. objective and types of threats addressed) of EPCIP was fixed, recognising the threat from terrorism as a priority even though the protection of critical infrastructure would be based on an all-hazards approach. This Communication also defined the main guiding principles of EPCIP and identified the necessity for creating an EU framework concerning the protection of critical infrastructures. This framework was defined in this Communication and included:

- A procedure for the identification and designation of ECI's
- Measures to facilitate the implementation of EPCIP: an action plan, CIWIN, CIP expert groups at the EU level, CIP information sharing process, and the identification and analysis of interdependencies.
- Support for member states concerning NCI's.
- Contingency planning
- An external dimension, enhancing cooperation beyond the EU.
- Financial measures under the umbrella of the EU programme on "Prevention, Preparedness, and Consequence Management of Terrorism and other Security Related Risks".

During that same year and in the context of its i2010 Program, the Commission also adopted the Communication COM(2006) 251 (35), "A strategy for a Secure Information Society – Dialogue, partnership and empowerment". Its intention was to revitalize the EC's strategy set

out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach". It reviewed the current state of threats to the security of the Information Society and determined what additional steps should be taken. This Communication proposes a "Dynamic and integrated approach that involves the stakeholders based on dialogue, partnership and empowerment". These policy initiatives complemented the activity being planned to achieve the goals of the Commission's Green Paper on the EPCIP. It was the early stages of today's Pan European PPP for Resilience.

In COM(2008) 676 (36) of October 2008, the Commission presented a proposal for a Council Decision on CIWIN. In this Communication CIWIN was defined as an electronic forum for the CIP related to information exchange, as well as a rapid alert system that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure. The CIWIN pilot phase was launched in the first half of 2010.

Also in December 2008, the Council Directive 2008/114 was issued (37). This Directive defined the procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure. This Directive considers that all those infrastructures and facilities for generation and transmission of electricity (in respect of supply electricity) are candidates for being identified as European Critical Infrastructures.

7.3 Policies on CIIP

In March 2009, the Commission adopted COM(2009) 149 (38) on Critical Information Infrastructure Protection. This Communication was named "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". It recognizes that ICT infrastructures are the underpinning platform of other CI's. In fact, Critical Information Infrastructures (CII's) are defined as "ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures". The Communication defines a plan of immediate actions to strengthen the security and resilience of CII's based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for EC infrastructures in the field of ICT. None of these activities were targeting Industrial Control Systems in general or the electric sector (e.g. smart grid) specifically. The Communication also highlights that activities under this plan will be conducted under and in parallel to the EPCIP.

Finally, in March 2011, a new Communication from the Commission on Critical Information Infrastructure Protection, COM(2011) 163 (39), was adopted. This Communication on the "Achievements and next steps: towards global cyber-security", recognizes that new threats have emerged, mentioning Stuxnet as an example of a disruption-purpose threat. Threats with destruction purposes, with a direct mention to ICT in Critical Infrastructures such as the smart grids and water systems were also considered. The Communication goes over the achievements of the plan presented on COM(2009) 149 (38), and proposes activities for the future. These activities are classified under the following categories: promote principles for the resilience and stability of the Internet, build strategic international partnerships, and

develop trust in the cloud. As already happened with COM(2009) 149 (38), none of these activities were targeting smart grid components specifically.

8 The most relevant EU-wide smart grid security-related Initiatives

This section provides an overview of the most relevant and active initiatives at the EU level addressing the challenges of smart grid cyber security. It is not comprehensive and we refer the reader to Annex V in order to find an exhaustive catalogue of all the initiatives being carried out at the EU level and also at the level of Member States. Besides, annex IV of ENISA's report on ICS protection (3) also includes a very detailed outlook on ICS security European initiatives.

8.1 Smart Grid Task Force

To facilitate and support the process of a European Union-wide smart grid implementation, the European Commission decided to set up a Task Force on Smart Grids. The Task Force Smart Grids was designed to provide a joint regulatory, technological and commercial vision on smart grids taking into account accumulated experiences worldwide and the technological challenges to be faced mainly during next decade/s, so as to coordinate the first steps towards the implementation of smart grids under the provision of the Third Energy Package.

The Task Force aims to jointly agree among the regulatory authorities, regulated companies and end users on key issues such as the estimated cost/benefits, the associated risks and the incentives needed. The ultimate goal of the initial work programme of the task force is to identify and produce a set of regulatory recommendations to ensure European Union -wide consistent, cost-effective, efficient and fair implementation of smart grids, while achieving the expected smart grids' services and benefits for the network users. The planned efforts of this Work Programme are focussed on:

- **Functionalities of smart grid and smart meters:** The key deliverable is to provide an agreement among all actors involved on a set of minimum functionalities for smart grids and smart meters.
- **Regulatory recommendations for data safety, data handling and data protection:** The key deliverable is to identify the appropriate regulatory scenario and recommendations for data handling, safety and consumer protection.
- **Roles and responsibilities of actors involved in the smart grids deployment:** The key deliverable is the development of recommendations on the roles and responsibilities of all involved actors in the implementation of the smart grids as well as the definition of criteria and recommendations for funding of smart grid deployment.

In the beginning the Smart Grid Task Force comprised three Expert Groups (EG) to which a fourth one was added afterwards. These EGs are the following:

- **Expert Group 1:** Functionalities of smart grids and smart meters.
- **Expert Group 2:** Regulatory recommendations for data safety, data handling and data protection.

- **Expert Group 3:** Roles and Responsibilities of Actors involved in the smart grids Deployment.
- **Expert Group 4:** Smart grid aspects related to Gas.

The EG2 is involved directly in smart grid security. This group aims to:

- Identify the benefits and concerns of customers with regard to smart grids.
- Provide an overview of European legislation on data protection, privacy and its enforcement.
- Recommend whether further protective measures should be put in place.
- Identify possible risks in the handling of data, safety and data protection.
- Identify ownership of data and access rights.
- Identify responsible parties for data protection and enforcement mechanisms.
- Develop a framework in which way data can be used.
- Provide recommendations on the Communication of Smart Grid benefits to consumers, citizens and politicians.

The EG2 issued in February 2011 a report titled 'Regulatory recommendations for data safety, data handling and data protection' (40) which focuses on identifying the appropriate regulatory scenario and recommendations for data handling, security and data protection.

8.2 CEN/CENELEC/ETSI JWG and SG-CG

The Smart Grids Task Force highlighted the importance of new standards for a successful deployment of smart grids together with a need for change and improvement of the existing standards. In addition, this group of experts identified the risk of too many standardization bodies providing an inconsistent set of standards. As a result, the Expert Group 1 of the EC Smart Grid Task Force concluded there was a need for a joint CEN/CENELEC/ETSI group on standards for smart grids, to deal more intensively with establishing detailed recommendations to selected standardization bodies. For this reason the CEN/CENELEC/ETSI Joint Working Group (JWG) on standards for the smart grid was established. It worked between June 2010 and March 2011 on the production of a report addressing standards for smart grids. This document was called 'final report of CEN/CENELEC/ETSI JWG on standards for smart grids'.

In M/490 the European Commission requested ESOs to develop a framework to enable ESOs to perform continuous standard enhancement and development in the field of smart grids, while maintaining transverse consistency and promote continuous innovation. The focal point addressing the ESO's response to M/490 is the CEN/CENELEC/ETSI Smart Grids Coordination Group (SG-CG) which was built around the membership of the previous JWG. Besides, M/490 requires the work to build on already existing material delivered through other mandates such

as the M/441 and M/468. The SG-CG is the main and visible body of a larger structure which includes four Working Groups (WG) coordinated by the SG-CG. These working groups are:

- Reference architecture WG.
- First set of standards WG.
- Sustainable processes WG.
- Security WG (also referred sometimes as Smart Grid Information Security Working Group - SGIS WG).

In addition to other standardisation aspects (e.g. reference architecture, communication interfaces, generation, transmission, distribution, smart metering, etc.) the CEN/CELEC/ETSI JWG final report on standards for smart grids includes a number of recommendations for smart grid standardisation on the field of information security.

On the other hand, the SGIS WG of the SG-CG is defining a number of essential security requirements for smart grids based on confidentiality, integrity, availability, reliability/resiliency, privacy and interoperability criteria. Moreover, this WG is working on the establishment of different security levels to classify the infrastructures that the smart grid will comprise. Besides, it is also revising international standards on smart grid security, identifying gaps and differences in current European regulations and standards. Finally, the working group is also defining a set of tools and methodologies to help classifying assets, assessing risks and filling the aforementioned gaps and other requirements.

8.3 DG CONNECT's Ad-Hoc EG on Smart Grid Security

The European Commission created the Ad-hoc Expert Group to better understand the views and objectives of the private and public sectors on the ICT security and resilience challenges for the smart grids as well as to identify and discuss about the related policies at EU level.

COM(2011) 163(22) on Critical Information Infrastructure Protection as well as COM(2011) 202 (23) on Smart Grids were presented are the two main pillars backing up this initiative. Specifically, COM (2011) 202 declares that the Commission should continue bringing together the energy and ICT communities within an expert group to assess the network and information security and resilience of smart grids.

The two main objectives of the Expert Group are:

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

Based on the aforementioned two main objectives, a 'Programme of Work' (41) was defined with the mission of contributing to a coherent and increased effort to improve the cyber security of the smart grids and which focuses on the security and resilience of communication and information systems that are critical for the performance of the physical electricity infrastructure. This programme of work includes four main areas, divided into twelve work packages. The areas and WPs are the following:

I. **Area 1. Risks, threats and vulnerabilities**
    a. WP 1.1 Identify and categorize all relevant smart grid assets
    b. WP 1.2 Develop an attach/threat taxonomy for relevant assets
    c. WP 1.3 Develop a countermeasure taxonomy for relevant assets
    d. WP 1.4 Develop a high-level security risk assessment methodology for relevant assets
II. **Area 2. Requirements and technology**
    a. WP 2.1 Security requirements
    b. WP 2.2 Extend smart grid requirements to include effective security measures
    c. WP 2.3 Research smart grid communication protocols and infrastructures to incorporate data security measures
    d. WP 2.4 (Public) procurement
III. **Area 3. Information and knowledge sharing**
    a. WP 3.1 Develop a cross-border alliance between Member States (MS) and relevant competent bodies
IV. **Area 4. Awareness, education and training**
    a. WP 4.1 High level conference for strategic leaders
    b. WP 4.2 Propose initiatives to increase stakeholder awareness on data security
V. **WP 4.3 Skilled personnel on cyber security in energy industry**

8.4 FP6 and FP7 research and development programmes

The Research Framework Programme (FP) is the EU's main instrument for research funding in Europe. The FP is proposed by the European Commission and adopted by the Council and the European Parliament following a co-decision procedure. Framework Programmes normally cover a period of five years (with the exception of FP7 which lasts for seven years), the last year of one FP and the first year of the following FP overlapping.

FP6 ran from 2003 to 2007, and the Information Society Technologies (IST) efforts within it aimed at contributing directly to creating European policies for the information society. Among the strategic objectives of IST FP6 were (42): A global dependability and security

framework; semantics-based knowledge systems; networked business and government; e-Safety for road and air transport; e-Health; cognitive systems; embedded systems; improving risk management; and e-Inclusion.

FP7 started in 2007 and runs until 2013, lasting for seven years. FP7 includes thematic domains of interest that are continued after the end of FP6 and includes two new areas, space and security.

There are some projects under the scope of the FP7 which are related to smart grid security. The following sets out a number of them:

- **ELVIRE** (43): It is an Information and Communication Technologies (ICT) research project. Its purpose is to develop an effective system which is able to neutralize the driver's 'range anxiety'. In order to ease and optimize energy management of Electric Vehicles (EV) and to cope with the sparse distribution of electrical supply points during the ramp-up phase, innovative Information and Communications Technologies and service concepts are being developed. The participants of this project are working on procedures to secure data transmission between vehicles and external services, sending the information in real time.
- **AFTER** (44)**:** This project addresses vulnerability evaluation and contingency planning of the energy grids and energy plants, considering also the ICT systems used in protection and control. It aims to develop a methodology and a tool for vulnerability analysis and risk assessment of interconnected electrical power systems considering their interdependencies. Moreover, it also aims at developing develop algorithms and tools supporting contingency planning in a two-fold approach: preventing or limiting system disruption, by means of physical security techniques and defence plans; and re-establishing the system after a major disruption, by means of restoration plans.
- **Open Meter** (45): The main objective of the OPEN meter project is to specify a comprehensive set of open and public standards for Advanced Metering Infrastructure (AMI) supporting multi commodities (Electricity, Gas, Water and Heat), based on the agreement of the most relevant stakeholders in the area. The general requirements include aspects such as security, interoperability, robustness, scalability, maintenance, performance and management. Part of its work focuses on the identification and specification of security requirements and on the determination of security clauses. The project includes specific tasks devoted to cyber security in smart grid environments. Besides, a series of deliverables providing an overview on the steps to be implemented to achieve a secure smart grid.
- **Internet of Energy** (46) (47)**:** The objective of this project is to develop hardware, software and middleware for seamless, secure connectivity and interoperability achieved by connecting the Internet with the energy grids. The project will evaluate and develop the needed ICT for the efficient implementation in future smart grid structures, including security capabilities.

- **DLC+VIT4IP:** this project will develop, verify and test a high-speed narrow-band power line communications infrastructure using the Internet Protocol (IP) which is capable of supporting existing and extending new and multiple communication applications. These shall include the existing power distribution network for novel services in smart electricity distribution networks such as demand side management, control of distributed generation and customer integration. This projects develops, among other things, reference designs and embedded systems architectures for the high efficiency and secure smart network systems addressing requirements on compatibility, networking, security, robustness, diagnosis, maintenance, integrated resource management and self-organization.

8.5 The EU-US Working Group on Cyber-Security and Cybercrime

The EU-US Working Group (EU-US WG) on Cyber-security and Cybercrime was established in the context of the EU-US summit of 20th of November 2010 held in Lisbon. Its main objective is to tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend. The EU-US WG addresses a number of specific priority areas and was planned to report progress within a year time after its establishment. The efforts include:

- Expanding incident management response capabilities jointly and globally, through a cooperation programme culminating in a joint EU-US cyber-incident exercise by 2012.
- A broad commitment to engage the private sector, sharing of good practices on collaboration with industry, and pursuing specific engagement on key issue areas such as fighting botnets, securing industrial control systems and smart grid (such as water treatment and power generation), and enhancing the resilience and stability of the Internet.
- A programme of immediate joint awareness raising activities, sharing messages and models across the Atlantic, as well as a roadmap towards synchronised annual awareness efforts and a conference on child protection online in Silicon Valley by end 2011.
- Continuing EU/US cooperation to remove child pornography from the Internet, including through work with domain-name registrars and registries.
- Advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties.

With respect to ICS and smart grid security the proposed tasks include the stock taking and comparative analysis of existing initiatives, pilots, good practices and methods addressing ICT risks, privacy and security. The input from the EU side includes:

- Activities at national level (NL, DE, UK, SE…) as well as at European level (Euro-SCSIE, possibly via Member States experts in the WG and during the stock taking of the ENISA studies on ICS and smart grids security)

- Ongoing ENISA studies on Industrial control systems and Interdependencies of ICT sector to energy

- Activities of the Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids, composed of European public and private stakeholders and coordinated by DG CONNECT.

The input from the US side includes:

- Experiences in international public-private coordination to mature acceptance of voluntary security standards.

- Specific methodology and mechanisms to engage with the private sector to achieve cooperation and mutual engagement in public-private control system security coordination.

- The deliverables expected from this cooperation include:

- Strategy for EU and US engagement on the control system/smart grid priority area;

- Plan of Action for EU and US public private engagement on cyber security of industrial control systems and smart grids; this will also draw on an analysis of existing coordination bodies for security of industrial control systems and highlighting best practices for voluntary participation developed within them.

8.6 ENCS

The ENCS aims to be the partner for organisations working on the security and protection of critical digital infrastructures, to help them to make accurate risk assessments and to take the appropriate measures to safeguard these infrastructures and guaranteeing the continuity and smooth running of the systems. ENCS is the evolution of a previous initiative called CyberTEC.

ENCS is an independent European public-private collaboration. Its founding members are Alliander (Dutch DSO), City of The Hague, CPNI.NL, KEMA, KPN (Biggest Dutch Telecom provider), Radboud University Nijmegen and TNO. The idea of ENCS is that it contributes to the resilience of CI by connecting people and organizations, being an information and knowledge sharing catalyst and educating people to the highest management levels. The ENCS will not only focus on the technical, but also on physical and personnel security.

The ENCS focuses primarily on the protection of smart grids and critical infrastructures' Process Control Domains, which still present substantial cyber security issues and challenges.

To address them, the ENCS connects existing organisations. The ENCS is planned to constantly scan the international arena for relevant developments, innovating and creating new initiatives to enable others. Besides the public-private network of experts and organizations, the ENCS will focus on four main areas:

- Research & Development
- Test Bed
- Information & Knowledge Sharing
- Education & Training

All four focus areas are interconnected, providing collaborative input and optimal synergy. The ENCS will start primarily on the protection of smart grids and CI's Process Control Domains. These still present substantial cyber security issues and challenges. To address them, the ENCS will connect existing organisations as the European Commission, ENISA, Joint Research Centre and national public and private initiatives across Europe and beyond – collaboration with the **DHS Control Systems' Security Program** and **Idaho National Labs** are prime examples.

9 Security standards, guidelines and regulatory documents for smart grids

Fortunately, there are many documents – standards, guidelines and regulatory documents – focusing on the electric sector and its several domains (e.g. generation, transmission, distribution, markets, end-consumer services, etc.). If we have a look to the documents compiled in Annex IV it will become evident that the electricity sector has been very active in addressing the cyber security risks. It is interesting to see that many of these documents are in a final state, and at the same time many others are currently under development or revision, mainly those addressing smart grid new cyber security aspects.

In this section we will provide an overview of the most relevant documents targeting smart grids and their security. For a comprehensive catalogue we refer the reader to Annex IV.

At the EU level, and in response to **Mandate M490**, ESO CEN, CENELEC and ETSI are working in a set of documents that are expected to be published during 2012. The scope of this mandate includes the development of a set of consistent standards within a common European framework that integrates a variety of digital computing and communication technologies and electrical architectures, and associated processes and services. Among them, it should be highlighted a specific standard on the security aspects of smart grids and a reference architecture. This will make possible to achieve interoperability among systems and will enable and facilitate the implementation in Europe of the envisioned smart grid services and functionalities.

On the other hand, the **Dutch Netbeheer Nederland** Privacy and Security Working Group has developed a best practice guideline entitled "Privacy and Security of the Advanced Metering Infrastructure," in which it is defined the framework that will serve as the foundation for Securing the Advanced Metering Infrastructure. This framework can be used by individual grid operators to implement security requirements and measures.

If we refer to the US, the NIST (National Institute of Standards and Technology) has developed a series of documents, **NISTIR 7628**, which have been called “Guidelines for Smart Grid Cyber Security”, which includes three different volumes. The first volume addresses the Smart Grid architecture as well as the cyber security strategy, as well as a set of requirements needed to implement appropriate security measures. The second volume focuses on privacy issues and on how to secure smart grids to protect the data transmitted for the grid operation. Finally, the third volume concentrates among other things on potential vulnerabilities, on concrete security problems of the smart grids that currently don’t have specific solutions, and on the a list of R&D topics related to smart grid security.

10 Bibliography

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

2. **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.

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

4. **EG, DG INFSO Ad-Hoc.** *WP 1.2. Threat Analysis.* 2012.

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

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

7. **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.

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

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

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

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

12. **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.

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

14. **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.

15. **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.

16. **American National Standard (ANSI).** *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.

17. **International Electrotechnical Commission (IEC).** *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.

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

19. **Department of Energy (DoE).** *Electricity Sector Cybersecurity Risk Management Process Guideline.* 2011.

20. **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.

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

22. **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.

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

24. **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.

25. —. *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.

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

27. —. *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.

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

29. **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.

30. **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.

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

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

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

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

35. —. *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.

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

37. **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.

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

39. —. *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.

40. **Task Force Smart Grids. Expert group 2.** *Regulatory recommendations for data safety, data handling and data protection.* s.l. : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf, 2011.

41. **DG-INFSO Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids.** *Programme of Work.* s.l. : https://resilience.enisa.europa.eu/security-and-resilience-of-communication-networks-and-information-systems-for-smart-grids/program-of-work/draft-final-version-pow/at_download/file, 2011.

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

43. *Elvire.* [Online] 2011. http://www.elvire.eu/.

44. **CORDIS Services.** *AFTER.* [Online] 2011. http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_LANG=EN&PJ_RCN=12231422.

45. **The OPEN meter Consortium.** *Open Meter.* [Online] 2009. http://www.openmeter.com/.

46. **Aretmis.** *Internet of Energy.* [Online] 2011. http://www.artemis-ioe.eu/.

47. **O.Vermesan, R.Zafalon, K.Kriegel, R.Mock, R.John, M.Ottella, P.Perlo.** Internet Of Energy pag:33. *Advance Microsystems for Automotive Applications 2011.* [Online] http://books.google.es/books?id=Qt7HDlzmrhsC&pg=PA33&lpg=PA33&dq=Internet+of+Energy+%E2%80%93+Connecting+Energy+Anywhere+Anytime&source=bl&ots=KlFXHWQYEA&sig=YDjZYgFqAevFtfWL6tuFqJxIKOo&hl=es&sa=X&ei=arVdT6mDIuem0AW9v9zWDQ&ved=0CIUBEOgBMAY#v=onepage&q=Int.

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

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

50. **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 .

51. **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.

52. **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.

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

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

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

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

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

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

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

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

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

62. **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.

63. **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.

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

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

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

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

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

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

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

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

72. *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.

73. **Amin, S. Massoud.** *Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control.* s.l. :

http://central.tli.umn.edu/CDC_Semi_plenary_Smart%20Grids_Massoud%20Amin_final.pdf, 2011.

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

75. **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.

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

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

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

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

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

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

82. **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.

83. **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.

84. **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.

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

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

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

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

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

90. **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.

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

92. **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.

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

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

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

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

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

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

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

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

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

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

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

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

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

106. **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.

107. —. *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.

108. —. *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.

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

110. —. *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.

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

112. —. *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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

127. **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.

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

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

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

131. **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.

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

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

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

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

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

137. **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.

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

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

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

141. **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.

142. **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.

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

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

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

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

147. **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.

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

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

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

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

152. **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.

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

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

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

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

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

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

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

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

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

162. **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.

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

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

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

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

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

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

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

170. **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.

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

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

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

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

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

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

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

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

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

180. —. *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.

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

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

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

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

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

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

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

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

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

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

191. **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.

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

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

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

195. **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.

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

197. **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.

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

199. **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.

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

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

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

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

204. —. *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.

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

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

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

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

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

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

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

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

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

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

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

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

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

218. —. 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.

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

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

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

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

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

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

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

226. **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.

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

228. **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.

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

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

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

232. **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.

233. **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.

234. **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.

235. **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.

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

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

238. **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.

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

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

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

242. **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.

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

244. **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.

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

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

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

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

249. **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.

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

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

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

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

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

255. **International Electrotechnical Commission (IEC).** *IEC 62443: Security for Industrial Process Measurement and Control: Network and System Security.* 2010.

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

257. —. *ISO/IEC 15408: Information technology. Security techniques. Evaluation criteria for IT security.* 2009-2011.

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

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

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

261. **National Institute of Standards and Technology (NIST).** *Field Device Protection Profile for SCADA Systems in Medium Robustness Environments.* 2006.

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

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

264. —. *DLMS/COSEM: Conformance Testing Process.* 2010.

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

266. **IEC.** *IEC TS 62351-5: Power systems management and associated information exchange – Data and.*

267. **International Electrotechnical Commission (IEC).** *IEC 60870-5: Telecontrol equipment and system.* 2007.

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

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

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

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

272. **American National Standard (ANSI).** *ANSI C12.19: American National Standard for Utility Industry End Device Data Tables.* 2008.

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

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

275. **Commission of the European communities.** *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. COM(2011) 163.* 2011.

276. **Zwan, Erwin van der.** *Security of Industrial Control Systems, What to Look For.* 2010.

277. **CIGRÉ.** *The Impact of Implementing Cyber Security Requirements using IEC 61850.* s.l. : CIGRE Publication 427, 2010.

278. **European Technology Platform SmartGrids.** *Strategic research agenda for Europe's electricity networks of the future.* s.l. : http://www.smartgrids.eu/documents/sra/sra_finalversion.pdf, 2007.

279. **Commission of the European communities.** *Commission staff working document definition, expected services, functionalities and benefits of smart grids SEC(2011)463.* 2011.

280. En. [Online]

281. **ESMIG.** *External Activities, ESMIG.* [Online] http://www.esmig.eu/about-us/smart-meter-coordination-group-sm-cg-new.

282. **Taylor, Dr. Gary.** DEVELOPING NOVEL ICT BASED SOLUTIONS FOR SMART DISTRIBUTION NETWORK OPERATION. [Online] http://dea.brunel.ac.uk/hiperdno/files/UPEC%202010%20HiPerDNO%20Project%20Presentation.pdf.

283. **SGTF.** Smart Grid Task Force. [Online] http://www.nerc.com/filez/sgtf.html.

284. **SGWG.** Smart Grid Working Groups. [Online] 2011. http://www.nerc.com/filez/sgwg.html.

285. **ENTSOE.** *WG European operational standards.* [Online] https://www.entsoe.eu/system-operations/working-groups/wg-european-operational-standards/.

286. —. *ENTSOE Working Group System Protection.* [Online] https://www.entsoe.eu/system-operations/working-groups/wg-critical-system-protection/.

287. —. *WG Electronic Highway.* [Online] https://www.entsoe.eu/system-operations/working-groups/wg-electronic-highway/.

288. **Netbeheer Nederland.** *Privacy and Security Advance Metering Infraestructure. Apendix A.* s.l. : http://www.energiened.nl/_upload/bestellingen/publicaties/356_320006%20-%20PS%20M%20StakeholderAnalysis.pdf, 2010.

289. **DECC.** *Smarter Grids: The Opportunity.* s.l. : http://www.decc.gov.uk/assets/decc/what%20we%20do/uk%20energy%20supply/futureelectricitynetworks/1_20091203163757_e_@@_smartergridsopportunity.pdf, 2009.

290. **ASAP-SG.** *Advanced Security Acceleration Project for the Smart Grid.* [Online] 2011. http://www.smartgridipedia.org/index.php/ASAP-SG.

291. **Cyber Security Working Group.** *Cyber Security Working Group.* [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

292. **Smart Grid Architecture Committee.** *Smart Grid Architecture Committee.* [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SmartGridArchitectureCommittee.

293. **NIST SGIP.** *Priority Action Plans.* [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PriorityActionPlans.

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

295. **NIST SGIP.** *Domain Expert Working Groups.* [Online] 2011. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/DEWGs.

296. **NIST -SGIP.** *SGIP Catalog of Standards.* [Online] 2012. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCatalogOfStandards.

297. **NEMA.** *National Electrical Manufacturers Association. Position Statement on Cyber Security.* s.l. : www.nema.org/gov/energy/smartgrid/upload/Cyber_Security_Position_Statement.pdf.

298. **EPRI.** EPRI Progress Report. [Online] http://www.smartgrid.epri.com/doc/IntelliGrid%20Newsletter%20Template_June%20053111.pdf.

299. **Institute of Electrical and Electronics Engineers (IEEE).** *IEEE-PES Smart Grid Forum.* [Online] tp://www.ieee-pes.org/smart-grid-forum.

300. **National Institute of Standards and Technology (NIST).** *NIST Smart Grid Federal Advisory Commitee.* [Online] 2010. http://www.nist.gov/smartgrid/committee.cfm.

301. **VGB.** *VGB-R.175 IT-Sicherheit für Erzeugungsanlagen .* s.l. : http://www.vgb.org/shop/r175.html, 2006.

302. **Institute of Electrical and Electronics Engineers (IEEE).** *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* s.l. : http://standards.ieee.org/develop/wg/WGC6.html, 2010.

303. —. *WGC1 - Application of Computer-Based Systems.* s.l. : http://standards.ieee.org/develop/wg/WGC1.html, 2007.

304. —. *E7.1402 - Physical Security of Electric Power Substations.* s.l. : http://standards.ieee.org/develop/wg/E7_1402.html, 2000.

305. **CEN/CENELEC/ETSI.** *CEN/CLC/ETSI/TR 50572. Functional reference architecture for communications in smart metering systems.* s.l. : ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf, 2011.

306. **EUROELECTRIC.** 10 Steps to Smart Grid. [Online] 2010. http://www.eurelectric.org/10StepsTosmartGrids/.

307. **DIN.** *Electromobility.* [Online] 2011. http://www.naautomobil.din.de/cmd?contextid=naautomobil&bcrumblevel=1&subcommitteeid=118124005&projid=149029465&level=tpl-proj-detailansicht&committeeid=54738955&languageid=en.

308. **National Electrical Manufacturers Association (NEMA).** *Position Statement on Cyber Security.* s.l. : http://www.nema.org/gov/energy/smartgrid/upload/Cyber_Security_Position_Statement.pdf .

309. **Department of Energy (DoE).** *Electricity Sector Cybersecurity Risk Management Process Guideline.* 2011.

11 Abbreviations

AMI	Advanced Metering Infrastructure
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentially, Integrity and Availability
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
CO2	Carbon dioxide
CSIRT	Computer Security Incident Response Team
DAE	Digital Agenda for Europe
DER	Distributed Energy Resource
DG CONNECT	Directorate General for Communications Networks, Content and Technology
DHS	Department of Homeland Security
DLMS/COSEM	Device Language Message specification/COmpanion Specification for Energy Metering
DMS	Distribution Management System
DNP3	Distributed Network Protocol version 3
DoS	Denial of Service
DSO	Distribution System Operator
EC	the European Commission
ECI	European Critical Infrastructure
EG	Expert Group
EMS	Energy Management System
ENCS	European Network for Cyber Security
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
EU	European Union
Euro-SCSIE	European SCADA and Control Systems Information Exchange
EV	Electric Vehicle
FBI	Federal Bureau of Intelligence
FP	Framework Programme
GPRS	General Packet Radio Service
HAN	Home Area Network
HTTP	Hypertext Transfer Protocol
HW	Hardware
IAC	Integrity, Availability, Confidentiality

IAN	Industrial Area Networks
ICS	Industrial Control Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IST	Information Society Technologies
IT	Information technology
JHA	Justice and Home Affairs
JWG	Joint Working Group
LTE	Long Term Evolution
NCA	National Critical Infrastructure
NIST	National Institute of Standards and Technology
OPC	Ole for Process Control
PCS	Process Control System
PLC	power line communications
PRIME	PoweRline Intelligent Metering Evolution
R&D	Research and Development
RAT	Remote Administration Tool
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Smart grid
SGCG	Smart Grid Coordination Group
SGIS	Smart Grid Information Security
SLA	Service Level Agreement
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TRA	Technology Related Anger
TSO	Transmission System Operator
UMTS	Universal Mobile Telecommunications System
USA/US	United States of America
USB	Universal Serial Bus
WG	Working Group
Wimax	Worldwide Interoperability for Microwave Access
WP	Work Package
XML	eXtensible Markup Language

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