Cyber Security of the Smart Grids

SUMMARY REPORT

Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids[1]

[1] http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2712

Table of contents

List of Contributors

This paper is produced by the European Commission using input and comments from the Expert Group on the Security and Resilience of Communications Networks and Information Systems for Smart Grids[2].

Program of Work:

Mr. Bram Reinders, Alliander

Mr. Bart Jacobs and Mr. Klaus Kursawe, Radboud University

Mr . Derk Fischer, PwC

Mr. Frank Hyldmar, Elster

Mr . Ilias Chantzos, Symantec

Mr . Monika Josi, Microsoft

Work packages team leaders:

Mr. Rajesh Nair, Swiss Grid

Mr. Eric Luiijf, TNO & CPNI.NL

Mr. Bernhard M. Haemmerli, Lucerne University

Mr. Zoltan Precsenyi, Symantec

Mr. Himanchu Khurana, Honeywell

Mr. David King, UK National Grid

Mr. Francois Ennesser, Gemalto

Mr. Felipe Alvarez –Cuevas, ENDESA

Mr. Auke Huistra, CPNI.NL

Mr. Klaus Kursawe, Radboud University

Work packages team members:

Mr. Simone Riccetti, IBM

Mr. Eric Van Aken, Alliander

Mr. Meir Shargal, CSC

[2] http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2712

Mr. Singh Nisheeth, Swiss Grid

Mr. Elyoenai Egozcue, S21SEC

Mr. Claudia Eckert, AISEC

Mr. Christoph Krauß, AISEC

Mr. Bernard Hourtane, EDF

Mr. Vangelis Ouzounis, ENISA

Mr. Rafal Lesczyna, ENISA

Mr. Konstantinos Moulinos, ENISA

Mr. Ralph Eckmaier, ESEC

Mr. Johan Rambi, Alliander

Mr. Sandro Bologna, AIIC

Mr. Hani Banayoti, ATOS

Dr. David Willacy, National Grid

Mr. Jeremy Wood, Deloitte

Mr. Joe Dauncey, Scottish and Southern Electricity

Mr. Jose Carlos Chico Garcia, IBERDROLA

Mr. Josep M. Selga, La Salle University

Mr. Michael John, ELSTER

Mr. Bart de Wijs, ABB

Mr. Jean Pierre Mennella, ALSTOM

Mr. Hans Honecker, BSI

Mr. Jarkko Saarimäki, FICORA

Mr. Igor Nai, GCSEC

Mr. Paul Theron; Thales Group

1. Introduction

01 In recent decades the application and use of Information and Communication Technologies (ICT) in our Critical Infrastructures, like drinking water systems, energy grids, financial and communication infrastructures has increased enormously. These systems have opened an unforeseen amount of opportunities. Infrastructures became highly efficient and flexible, which has been beneficiary for society. In particular in the energy infrastructures, flexibility is key to respond to the transition to intermittent sustainable power generation. Smart grids support the energy transition of the coming decades.

The growing dependency on ICT also means that new threats have to be met. Threats to ICT, intentional and unintentional are a fact and growing. The disruption or destruction of electricity grids would have a serious impact on economic and societal functions. In order to keep our infrastructures resilient we have to invest in secure and resilient architectures[3].

Smart Grids have been defined by the European Smart Grid Task Force[4] as electricity networks that can efficiently integrate the behaviour and actions of all users connected to it — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.

In Europe, the smart grid is conceived of as employing innovative products and services together with intelligent monitoring, control, communication, and self-healing[5] technologies in order to:

- Better facilitate the connection and operation of generators of all sizes and technologies;
- Allow consumers to play a part in optimising the operation of the system;

- Provide consumers with more information and options for choice of supply;
- Significantly reduce the environmental impact of the whole electricity supply system;
- Maintain or even improve the existing high levels of system reliability, quality and security of supply;
- Maintain and improve the existing services efficiently.

Smart Grids could be described as an upgraded electricity network to which two-way digital communication streams between supplier and consumer, intelligent metering, smart appliances, electric vehicles, and monitoring systems have been added.

The development of Smart Grids exemplifies the increasing reliance of European economy and society on ICT. ICT infrastructures have become the underpinning platform for other critical infrastructures without which some services (e.g. in electricity transmission and distribution) could come to an abrupt halt. To tackle this challenge the European Commission convened in 2010 a multi-stakeholders and multidisciplinary group of Experts[6] to discuss and work on relevant matters regarding the security and resilience of communication networks and information systems for Smart Grids. The Expert Group on the Security and Resilience of the Communications Networks and Information systems for Smart Grid had two main objectives[7]:

Objective 1

Identify European priority areas for which action should be undertaken to address the security and resilience of communication networks and information systems for Smart Grids. The Expert Group was also expected to define recommendations on how to progress on each priority area at European level.

Objective 2

Identify which elements of the smart grid should be addressed by the Expert Group (e.g. smart appliances, smart metering, smart distribution, smart (local) generation, smart transmission) and to what level. The use of an existing common concept model should be considered. The Expert Group will:

---

[3] Communication on Critical Information Infrastructures Protection COM(2011) 163
[4] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm
[5] The grid automatically isolates a possible fault, by opening the neighbor circuit breakers
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF (page 8)
[7] Terms of Reference in Annex I

- Identify key strategic and high level requirements to ensure the security and resilience of communication networks and information systems for Smart Grids.

- Identify a good practices guideline based on lessons learned and that develops how to secure and increase the resilience of the ICT lay down infrastructure of Smart Grids.
  Moreover, the guideline will provide proposals on the way forward to ensure that cyber security challenges of smart grids are approached from a multidisciplinary perspective encompassing a dialogue and synergies between ICT security experts and energy/smart grids experts.

- Propose mechanisms/messages to raise awareness of decision makers related to the security risk of ICT for Smart Grids, as well as possible measures to manage such risk.

To reach the objectives the Expert Group on the Security and Resilience of Communications Networks and Information Systems for Smart Grids [8] has develop a Program of Work (Annex II) since 2010 to 2012. The outcomes of the Program of Work (PoW) represent a first approximation to the solutions on the various problems identified by the panel. This should be considered as general guidelines and tools that come to cover the lack of a consistent knowledge base on cyber security issues related to Smart Grid. The approach is only a first step and need to be developed further.

1.1. Main Points

- Education (skilled personnel on cyber security in energy industry): Cyber security in European Smart Grids requires well-trained proactive decision-taking operators of collaborating Smart Grid stakeholders to operate the next generation Smart Grid infrastructure. Relevant stakeholders should work on generating the necessary expertise to design, build and maintain secure smart grid systems. To meet the increasing demand for ICT experts and ICT security experts with operational knowledge in electricity has become challenging and might require updating engineering and ICT education curricula.

- Risk Assessment: ICT and electricity security experts should work together to enhance the design of security in smart grids. It is advisable to carry out an overall risk assessment with the help of taxonomies of threats and countermeasures to identify the specific well-balanced and effective set of security measures to be adopted by relevant operators. It shall be noted that the cyber security risk of Smart Grids is continuously evolving and requires regular reassessment.

- Addressing cyber security of Smart Grids requires first the identification of dependencies between the ICT-infrastructures and Electricity Grids, and of all other relevant Smart Grid assets.

- Risk Management: Electricity Critical infrastructures converging with ICT-infrastructures require scenario-building that includes consideration of highly unlikely types of events. ICT security considerations need to be integrated within the wider risk management of the whole grid. ICT is therefore needed to carry out a risk analysis, and to define high level security requirements to enhance the security and resilience of ICT for Smart Grids. Security requirements based on security properties (confidentiality, integrity and availability) and along the dimensions of detection, response and recovery. Risk analysis would also consider use cases.

- Incident management, at National and European level, should be assigned to a governmental authority which will respond to incidents and manage crisis due to cyber-attacks on smart grid.

[8] http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2712

- (Public) Procurement: The need for establishing a common procurement language and/or standard for a base level of security in smart grid components and services in collaboration with private and public asset owners, vendors and regulators.

- Economic incentives to invest in cyber security of ICT for Smart Grids.

- Revision of the regulatory framework: cyber security regulations should be built on other existing security regulations for electricity sector. The smart grid brings with it a new set of technologies and threats, but cyber security should be an integrated part of the security process of an electric company. In this regard resilience is crucial as their objective is to keep their infrastructure running. Policy makers need to work with regulatory bodies to establish standards, security guidelines and compliance mechanisms. This approach will provide consistent guidance, a level playing field and incentives for compliance. However, tight and contra-productive regulation shall be avoided.

- Security standards: Cyber security in European Smart Grids requires an approach of security-by-design, and standardisation. An EU-wide harmonization of security standards is needed.

- Information sharing on security breaches and architecture is essential and presents a basic condition to protect Smart Grids. Information sharing within and between sectors and the government is important. Determining how to securey communicate vulnerabilities and attack vectors is key to vendors and end users.

- The smart meter is becoming a key node for managing information about the electricity system and final customers. However, Industrial Control Systems, and not the smart meters, draw today the primary cyber security focus.

- Trends towards greater automation and remote control need to be accompanied by policies that can guarantee integrity and authenticity of information[9]. Wireless communications channels will be used for short-distance communications as well as for long-distance communications. Availability, integrity and authenticity therefore need to be assured across the entire “value chain” of the control signal. Closer integration of large-scale operational systems with IP-based networks such as the Internet increases the openness of critical infrastructures. Operational systems that exchange data with IP-based networks need to be designed for security and resilience. The European Smart Energy Grid will only come to full growth when cyber security is a key factor in the full life-cycle of the Smart Grid appliances, devices and services.

- Where appropriate, the Smart Grid infrastructure shall be based on IP version 6 as IP version 4 is outdated and over time will become obsolete.

- The need for different levels of security measures. The architectural layers of the smart grid present different security requirements. There is a need to keep all architectural layers of the smart grid, be it electrical or ICT layers, as robust as resilient as possible.

- The need for a Roadmap and a set of Good practices for cyber security and resilience of the smart grids: For those already deploying a "smarter" grid it would be useful to have a baseline of essential recommendations and requirements to implement the cyber security measures since the earlier stages of the deployment of the smart grid. Furthermore, it will be needed guidelines and recommendations for the improvement of the cyber security of Industrial Automation and Control Systems (IACS) and Supervisory Control And Data Acquisition (SCADA) systems.

- CEOs awareness on cyber security: The need for raising awareness on cyber security issues among 'decision makers' in Electrical Power organisations/operators. The awareness on ICT security and

[9] ICT Applications for the Smart Grids, OECD

resilience challenges for the smart grids should reach the boardroom decisions levels of the energy organisations.

- Research & Development for security:
    - research in risk management, resilience and information security of chains of organisations responsible for the end-to-end supply of energy;
    - research in policy-based incentives to strengthen the end-to-end resilience of the supply of energy and to suppress misbehaviour by high system-based penalties;
    - research and development of architectural security concepts in smart grids, e.g. an N-1 approach equivalent for the ICT-enhanced power grid.

1.2. Program of Work (2010-2012)

1.2.1.Mission, vision and goals

The mission of the PoW was to contribute to a coherent and increased effort to improve the cyber security for smart grids. This should be covered by both the Technology and Organisation & Human aspects that are all essential for an integral security approach. Such an approach should lead to an overall growth in security maturity as distinguished for instance by frameworks of COBIT and ISO/IEC 27002:2005.[10] COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks, whereas ISO/IEC 27002:2005 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management.

1.2.2. Strategy

The main challenge come from the fact that such two different industries as Energy and ICT are converging to technologically but also in the provision of services while both industries are depending upon each other's services.

The strategy to accomplish a coherent and increased effort to improve the cyber security for smart grids is by aligning the PoW with current on-going work as executed by expert groups and associations within the European Union. In other words, instead of considering the PoW as a starting document for initiatives in the field of cyber security, it was considered as a coherent coverage of initiatives that have already started and that are to be started in order to improve the cyber security for smart grids.

1.2.3. Scope

The scope of the PoW is the security and resilience of ICT that impact on the performance of the physical electricity infrastructure.[11] The physical threats of security are only taken into account in case it has a direct relation with ICT. This would e.g. hold for opening the gate of a sub station by a cyber attack which would allow for a physical attack or for physically breaking into a central control room to get access to control systems network.

In this document, contains the main outcomes and conclusions of the development of the PoW, while the detailed information on the PoW and its deliverables can be found as Annex II, a separate document.

[10] See MM Lessing (2008) "Best practices show the way to Information Security Maturity" for Generic Security Maturity Models.
[11] i.e. the gas network is out of scope.

2. Executive Summary

Vision: "Be able to manage all cyber risk aspects and have true redundancy implemented before applying the Smart Grid technology"

2.1. Risk, threats and vulnerabilities

Accomplishing cyber security of Smart Grids requires a previous endeavour on analysing in depth and clarifying what are the key assets that need to be prioritised, what are the threats and vulnerabilities, and what could be the countermeasures that serve to reduce the resulting risk to a manageable, accepted level.

The Expert Group has **identified and categorised all relevant assets**, identify the magnitude of any impact that should be protected against, and then classifying the assets based on the protection needs. That means all critical energy assets within the Transmission, Distribution and Generation space which can:

1. Cause a International, Cross Border, National or Regional power outage or damage to infrastructure;
2. Cause a significant impact to Energy market participants;
3. Cause a significant impact on Operations and Maintenance of the energy grid;
4. Pose a significant risk to Personal Data of citizens (Privacy);
5. Cause significant safety issues for people.

The Smart grid architecture involved many cyber assets, where some have been part of the grid for a while and others are new "smarter" assets. To better distinguish the "smart" assets (i.e., Advanced Metering Infrastructure (AMI), Intelligent device control) from the "traditional" cyber assets (i.e., SCADA), the assets have split into two categories:

- Smart Cyber assets

A new Smart Asset category which includes new monitoring and control devices, communication infrastructures, etc., which add a whole new set of capabilities for the Grid Assets to utilise. The smart movement open the grid to vulnerabilities that already exist in the ICT world, now those vulnerabilities pose threat to the Smart Grid (and SCADA) communications and applications also.

This is a new category, which has influence mostly on all core component layers. They contribute in automation of processes and increased controllability of the grid. Consequently they increase the risk in the overall grid considerably due to the large numbers of the devices, and their collective impact. Their impact can be in any or multiple layers hence the security mechanisms need address other vectors as well.

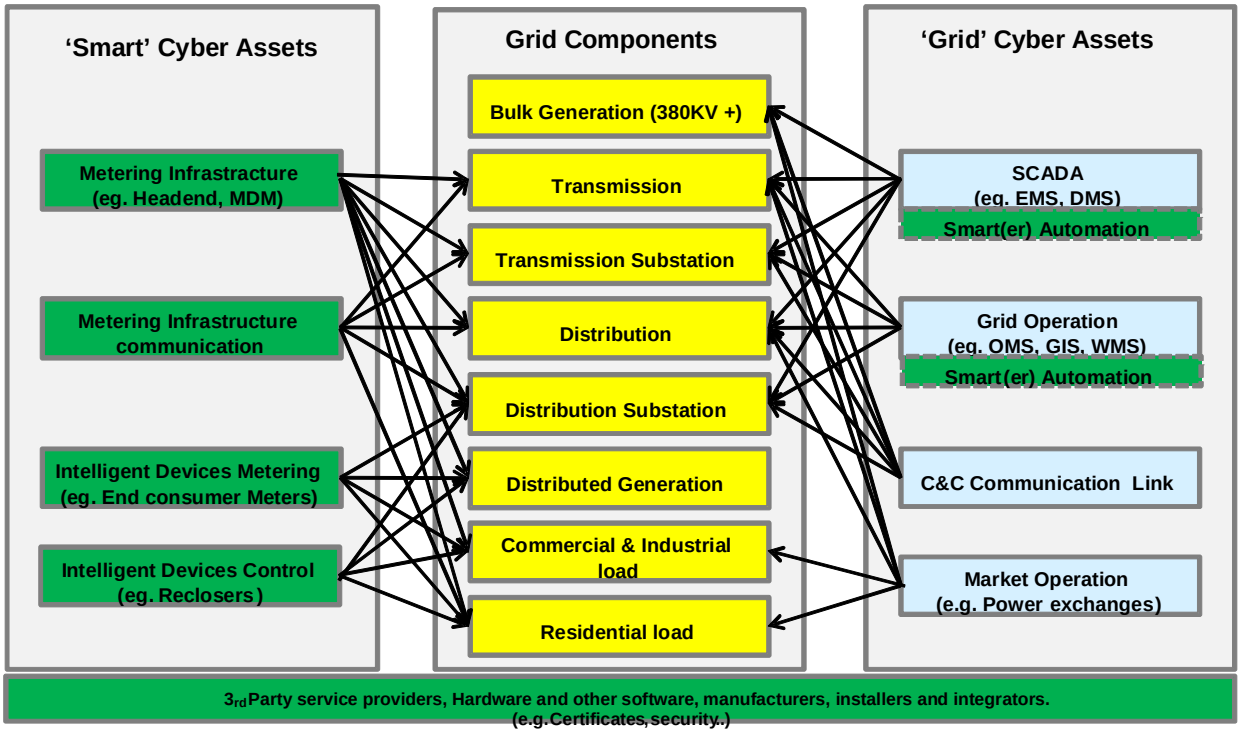
- Grid Cyber assets

Grid Assets historically developed along with the core components and exist in a very mature fashion in today's infrastructure. The traditional grid assets are now being upgraded with the capability to address the needs of the smart Assets and the new Distributed Generation aspects of the core components. Additional functionalities in the Grid Assets which help automate, improve control capabilities and increase the efficiency of grid operations or the energy markets are now being implemented due to smart grids.

The span of control of the Grid assets is also considerably high. This means that their impact is also similar to those of the Smart Assets, but the numbers of assets are very few. These then form the high value targets that have a different protection need.

Based on this, the Expert Group suggests to classify the relevant smart grid assets into the three major classifications: **Smart cyber assets**, **Grid components** and **Grid Cyber assets**. The criticality of the types of asset are defined and a minimum measurable impact is also defined.

The risk management processes are expected to be dovetailed into this defined classification and the defined impact thresholds.



This baseline categorisation allows the development of a comprehensive and all hazards **threat taxonomy**, analysing and weighting of these threats makes it easier to determine how measures can be taken in order to mitigate the overall risk of Smart Grid operations across service-chains of multiple organisations which may even be competitors.

The objective is to address all actors involved in providing a reliable energy service with a taxonomy of threats that need to be considered when developing and deploying Smart Grid infrastructures in the European Union. We identified an extensive set of stakeholder and actors involved in securing the smart grid. The current ENTSo-E, EFECT/ebIX **Harmonised Electricity Market Role Model** lacks some of these stakeholders and **need to be extended** with manufacturers and system integrators of smart grid equipment (smart appliances, electric vehicles; DSO and TSO level smart equipment), financial service providers (buying or selling electric vehicle power), 3rd party information services (e.g. certificate issuers), and governance (regulators, standardisation organisations).

Referencing this complex set of stakeholders, the threat identification step encompasses both the information and the infrastructure dimensions of Smart Grids and comprises (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.

As European Smart Grids in the end comprise up to hundreds or thousands energy suppliers, power transmission operators and distributors, millions of customers/prosumers, and millions of smart appliances,

electric vehicles, etcetera's, which *together* operate in the end the energy value-chains, also the (1) deliberate and (2) common mode failure threats to the multi-stakeholder value-chains need to be recognised. An example of (1) is the Western U.S. Energy Crisis of 2000 and 2001 where competing companies created a power demand supply gap with brownouts as a result. Therefore, Europe has to govern the total Smart Grid chain threats. The following threat challenges stand out:

Threat challenge 1: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain that governs power supply.

Threat challenge 2: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain that governs power demand.

Threat challenge 3: The subset of ICT-related threats dealing with the manipulation and disruption of the inter-organisational Smart Grid information chain balances power demand and supply at the various power grid levels.

Threat challenge 4: Earlier Smart Grid investments by a stakeholder could be of no or limited value due to the appearance of disruptive technology.

Threat challenge 5: Bulk generation, power transmission and distribution companies are used to slowly changing technology and long economic depreciation cycles, thirty to forty years are not uncommon. On the other hand, ICT has short technology aging cycles. The move to smart energy grids will require the aforementioned organisations to change their investment and depreciation cycles as well as incurring costs for continual ICT updates.

Threat challenge 6: The subset of ICT-related threats which may disrupt components that are deployed in massive rollouts, e.g. smart meters, smart appliances, electric vehicles. Crisis management of Smart Grid stakeholders need to be prepared for fast update cycles at hundred thousands to millions of customer and prosumer sites and/or pieces of equipment after the appearance of a vulnerability. When not mitigated in time, a vulnerability in such a component may cause criminals, activists or even terrorists to take control over (parts of) the ICT-side of the Smart Grid.

Threat challenge 7: Earlier Smart Grid investments could be of no or limited value due to adverse laws and ruling by EU, Member States or Regulators (e.g., export license control, privacy-related ruling not supported by hardware).

The identified sets of threats to the Smart Grid show that there is a manifold of opportunities to deliberately affect the functioning of Smart Grids. 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.

Scenarios and so-called 'use cases' may help to find and rank attack avenues that relate the function elements above in relation to the (potential) impact. However, any risk mitigation need to be balanced with the risk factors stemming from the all hazard threats.

Some highly-visible examples of attacks to Smart Grids from the threats and actors identified above:

- 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.
- 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.

- 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.

This previous thorough analysis on the key critical assets in the Smart Grids and the threats landscape also serve as an appropriate baseline to develop a **set of countermeasures** to improve and reach the resilience and reliability of energy grids.

Countermeasures against new emerging risk are required to ensure that the Smart Grid operates well and in particular the security of supply is ensured. This includes all ICT components which directly deal with energy for monitoring and control, i.e., SCADA systems including AMI, etc. The security of these systems is of paramount importance since successful attacks may directly influence the security of supply. Likewise, the security of ICT components of the Smart Grid which are not dealing directly with energy must be ensured. For example, the ICT for the energy market must also be secured by applying appropriate countermeasures against attacks. Countermeasures depend upon several prerequisites:

1. A clear policy should be in place in which way the Smart Grid system is used and which purposes it has to cover.

2. The architecture of the Smart Grid system should be defined, as well as the according security requirement specification. Within the architecture appropriate countermeasures, i.e., security mechanisms are implemented. It should be noted that it is not sufficient to simply add security mechanisms to the individual components; i.e., a holistic security architecture considering the whole system is required.

3. For a given system, a risk assessment must be performed to set priorities of the countermeasures under consideration of the security requirement specification – if available. From the countermeasure priorities a security implementations plan should be elaborated.

Another view on Smart Grid security is the perspective of high impact and low frequency (HILF) risk: The European high voltage grid should not break apart. Direct costs are extremely high and indirect costs are even not really to calculate because of the magnitude. Therefore, adding resilience to a secure infrastructure with the target to have an availability of nearly 100% is the right way to go. The level of the resilience against the HILF risk is finally a political decision depending on:

- the general views during a given time period: how society perceive the risk and is willing to live with it[12],
- the willingness to agree on service level, or degraded service levels, and
- the ability to invest into security.

Recommendations on Countermeasures

- Self-assessment methodology for Smart Grid cyber security

Cyber security is – for a few electrical grid domains - a completely new and often not sufficiently covered topic in EU. Other electrical grid domains have paid attention and are more developed. A well-defined self-assessment guide for the ICT security experts in SCADA and Smart Grid enables each Smart Grid stakeholder to identify potential risk and to assess vulnerabilities. The results can be used as health check to define countermeasures and to reapprove security specifications. Also in long term it would be desirable that the stakeholder would agree on minimum standards.

[12] E.g., the Fukushima incident turned in Europe the risk perception of nuclear power in some nations.

- Promote application and adaption to Smart Grid of well-established ICT Security good practices

Information security and ICT-security is a well elaborated field in research and in practical solutions. This is especially true for corporate information systems. For Industrial Automation and Control Systems (IACS) there are the real time and 24/7 operation requirements, which need extra measures. Until recently IACS were not internetworked with the Internet and interconnected widely. For maintenance, efficiency, and monitoring purposes, IACS are connected to the corporate networks which often have several interconnections – either open declared or hidden – to public networks.

- Stimulate Inter-Organisation Actions

In general, standardisation is the mean to cooperate between organisations and cross borders. Today many standards are elaborated, but merging of existing standa4rds and adaption for international co-operation is still a need.

- Public-Private Partnership: Stimulate Industrial-Control-System specific exchange of information, knowledge and expertise at the national and international levels.

- Exercises: Regular and specific exercises for IACS incidents and combined IACS cyber incident must be planned, executed, and evaluated. Especially the following should be considered:

  -Combination of different organisational culture.
  -Combination of profile culture energy- electrical and Telco / ICT engineering.
  - Exercise should scope all situations including the ability to cold start all systems, knowing, that this could take years until the scope is properly covered.

- Provide a European wide (plus connected neighbourhood countries including links to Africa and Asia) and accepted vocabulary to enable and stimulate exchange. This vocabulary (probably in English) should have translation in each local language and must cover the variety of manufacturer and vendor specific terms.

- Smart meter of renewable producers or prosumers: Up to recently smart meters were just needed for billing and accounting. Adding more functionality to smart meters could enable better asset security and interfaces to a large scale energy management system. The ultimate goal of these additional functionalities is the improvement of the energy quality in terms of availability management, but also in prediction of energy prosumers and controlling variation in voltage magnitude, harmonic content in the waveforms for AC power.

- Secure maintenance and repair: Distributed System Operators (DSO) have been adding to the pure one directionally oriented power distribution system the option for prosumers and independent power producers to feed renewable energy into the DSO network. Switching off the DSO network requires today the down-stream switching off and switching off all renewables. Although existing network operation standards ensure the safety of the field agents working on the network, additional smart meter functionality or smart connector could allow central switching off capability. The trade-off between the ICT-security risk and the safety risk must be elaborated in separate discussions and studies.

- Apply security improvement management systems

Security is nearly always not perfect, because there is no source to finance all over perfect security, neither would it be economically viable. Usually risk assessment shows up to which degree protection is needed. Experts assume, that in some cases, e.g., in the core of the European grid, approaching perfect security is a real need. For SCADA this means to provide compartment security (highest level secure zone) with ideally no public network access (air gap principle of shielded networks). From the Stuxnet case, all experts learned that an ultimate air gap does not work in real environments.

The security level of given SCADA systems should be monitored, observed and continuously improved. Security improvement systems are:

- Incident and near incident monitoring and handling: Incident and near incidents are always a living proof of vulnerabilities. With an appropriate handling and monitoring systems improvement over time the security of a given system – even the system is always changing – will result, at a high level. The security management cycle should encompass at least three separate levels of SCADA: a) system elements, b) procedures, and c) system/architecture.

  Additionally it is very important to have well-educated and sufficient digital forensic capacity, such that incidents and near incidents can be investigated in-depth and according lessons can be identified. For the more technical hands on part, an Industrial-Control-System specific CERT should be discussed.

- European and national reporting entity[13]: SCADA and SCADA-Cyber incidents should be European wide reported to a suitable entity to stimulate the learning curve between Member States and inter-company. This reporting should be comparable to the airlines industry incident reporting system of the FAA.

- Provide sufficient reaction capacity: Security – especially SCADA cyber security is never perfect. Therefore post incident measures must be in place up front. This includes contingency planning but also to be prepared for a complete "plan B". The reaction capacity should start at intra-company level, extended by support contracts of collaborators, manufacturers, service companies, and in serious cases gradually enlarged up to international public-private partnership (PPP) level.

- Regular penetration tests for critical systems / networks: Penetration tests and security audits – preferably in a risk based repetition interval - are the means to assess the real security and remaining vulnerabilities up to the skill level of the specialised penetration testing / audit team. In practice, most of the environments will be penetrated or will show potential for optimization in case of audit which triggers as a follow up learning process.

- Penetration testing on individual devices that will be connected to the critical network on should be encouraged and could be done as a part of product certification.

- Elaborate and plan financing: Security level and available funding for security measures is a strongly coupled and interdependent pair. Ideally, a security requirement specification is given and the according measures will result. However, in practice, responsible agencies and boards try to circumvent this discussion, knowing that clear decisions could result in not controllable costs. Therefore, good practices have to be fostered by the community such that the pressure on European and Member State regulators and owners will result in the demand to comply with good practice and standards such that reasonable funds for preventive and after incident reactive security are available. Standards and good practice are means to leverage security concerns of organisational members to a non-personal compliance issue.

- Approaching the Highest Security Control Network (HSCN)

As already stated in the introduction, the high impact control devices in Smart Grids (aggregated overall impact 2 GW[14] and higher) require ultimate security[15] because there is no tolerance against system failure. The concept is: the ultimate critical assets are interconnected by the ultimate Highest Security Control Network (HSCN). Against the background of 100 known bottle necks on highest voltage transmission lines the need for HSCN is underlined. Reflecting this fact, a highest security control network – ideally completely separated from the internet is postulated. For clarity, there is a consideration that meters with contactors could be considered

[13] Incident reporting and administration is part of the improvement process and may complement collaborative early warning system, as partly available by today, but not sufficiently covering the specific SACDA security needs.

[14] To create the right expectation for the readers, in praxis this would mean, that many device collections with an impact of more than 100 MW already would be connected to HSCN. See WP1.1 of Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids

[15] No system failure means to apply fail save technology, redundancy, self-healing and similar technologies to reach n-1, n-2 or n-3 levels of security. (n-3: three components may fail without degrading normal operation)

requiring this network. However, to spread the HSCN to all metering endpoints would make the perimeter of the network impossible to control, and therefore meters with disconnect functions should rely on individual signatures for each meter to validate that disconnect-related commands must be sent to individual meters.

The **H**ighest **S**ecurity **C**ontrol **N**etwork HSCN concept must be built having in mind – neither direct nor indirect – connection to the public network which includes Internet, ISDN, and wireless networks.

Being aware that "no connection" is a theoretical principle and has to be replaced by the fewest amount and only known and well-defined connection: Today's Trammission System Operator (TSO) and bulk generators need to exchange current load, current demand, expected load, expected demand, and RESERVE status directly from their SCADA environment. A low number of exceptions which has to be handled by protocol verification secure transitions and all additional security increasing options must be considered. Even with these exceptions the protection of such a network is far more secure than any open link to the public network. The exceptions could be handled using the principle of utmost limited numbers of ports and commands related to ports: Therefore, the transition security to and from the HSCN will be verifiable with according software and therefore being aligned with today's best known security practise.

HSCN needs to be discussed and specified in a separate project. However, HSCN could serve several applications:

- In a country or in a limited size area, HSCN could be used as real time network with max reaction of 4msec: With this specification HSCN could be used for intertripping or protecting relaying.
- Communication of risk level and estimation global risk situation by communication between the stakeholders: TSO / DSO / bulk generation / Distributed Energy Resources (DER).
- To combine energy market information and SCADA in a secure way to achieve better resilience.

HSCN separation from the Internet: Even this SCADA network may use Internet Protocol, considering IPv6 if feasible, the Highest Security Control Network HSCN is for nearly all protocols completely separated from the commercial Internet. In specific cases even a VPN data stream may be put in commercial network and coupled out at the destination in an ultimate secure way.

As a consequence, the usual vulnerabilities of public networks will be eliminated or at least reduced to the lowest possible number. HSCN could work in a similar way as SWIFT does for the financial world. In many core regions SWIFT has 100% availability: even the architecture is designed for providing continuous service with no interruption. However, the stakeholder of the sector will decide on the business model having in mind the SWIFT case.

Specific requirements, such as propagation delay, other key properties, and feasibility have to be elaborated in a separate study. Also the expert debate setting the policies including the very strictly handling of exceptions is in scope of such a study.

Being well aware, that HSCN is essential shift of all paradigm of today, the argumentation for this network is consistent and compelling.

Finally, given the thorough fully analysis of key assets, threats and countermeasures, it has been also identified by the Expert Group the need of a tool for market operators that will support them with guidance and recommendations for selecting and implementing an appropriate risk assessment methodology and giving guidance for selecting appropriate information security controls deployable within the Smart Grid infrastructures within the European Union.

A **high-level security risk assessment methodology for relevant assets** will allow to identified clear objectives of risk analysis, enumeration of levels at which relevant operators should conduct risk analysis, process for prioritising risks, and phases and stages for risk mitigation, and therefore to aid in taking complete and effective measures against the risk encountered.

The risk assessment methodology catered for a continuous improvement rather than seeing security as an absolute. The typical stages of an in-depth security approach (prevent, detect, defend and recover) could be used as a model. Moreover, the traditional landscape (SCADA/DCS) of where we find control systems and meters is evolving also to other devices which call for an end to end security perspective.

To complement the high level threat analysis and risk assessment other technologies are in scope, such as reputation and intrusion detection techniques, that can allow to pick up abnormal data flows and traffic patterns even in otherwise secured systems.

The risk assessment approach proposed by the Expert Group is derived from the UK Government's Technical Risk Assessment Methodology which is widely applied in UK government organisations. The methodology has a number of characteristics which make it suitable for application in the domain of smart energy systems:

Tailored for assessing Information and Communication Technology (ICT) systems

Smart energy systems operate as an ICT layer on top of the physical energy grid. The proposed methodology specifically focuses on ICT systems, which shows in both the methodology's assessment steps and the explanatory text and examples.

Aligned with risk management standards such as ISO/IEC 27001 and ISO 31000

As example, the HMG IS1 standard considers the risk assessment a 'snapshot' investigation of risks. A structural approach to securing ICT systems such as the Smart Grid demands that the risk assessment results fit into a security/risk management system. The HMG IS1 standard has been designed to fit into the frameworks provided by the ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2011 and ISO 31000:2009 standards.

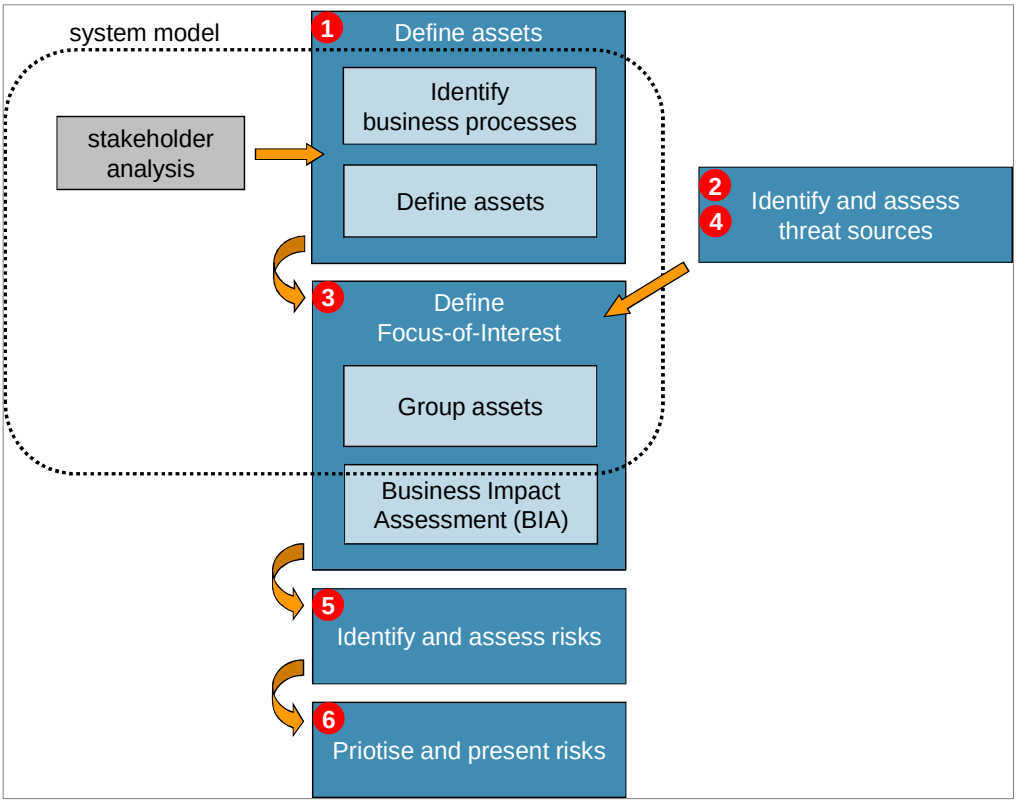
Supports design-time, iterative risk assessment

Smart energy systems development is still in an early stage. This allows taking a 'security-by-design' approach, using risk assessment results in the designing process. The HMG IS1, a national standard, acknowledges that in the early design stage only a rudimentary conception of the system, its environment and relevant risks is possible. It therefore propagates an iterative approach, refining the risk assessment as the system design takes shape.

Provides a structured transparent approach

The HMG IS1 standard uses a highly structured approach, providing transparency about how risk ratings are derived. Transparency is a key requirement in the multi-stakeholder context of smart energy systems where consumers and politicians want to form their own opinion about the level of privacy and security level, and the rationale behind it.

The proposed risk assessment method follows six defined steps. These steps allow the analyst to understand the system under consideration, define applicable threats and determine risks to the system with associated risk levels. The six steps are described, as well as some guidelines for how they may be applied in the context of smart energy systems.



2.2. Requirements and Technology

Information relating to the Smart Grid design will reside on disparate networks with various owners, it is critical to properly secure the security policies, procedures, and protocols that will be used during the planning and design phases of the project. This means reducing the risk of data loss or intrusion while, at the same time, allowing access for the relevant stakeholders who will be involved in the initiation and later phases.

Agreed security requirements for the Smart Grid information relating to both the initiation and design must include:

- Stakeholder agreed policies for protecting the information both in transit and storage.
- Security incident handling policies and procedures agreed and in place.
- Non-Disclosure agreements in place.

The following high-level requirements are relevant at the initiation stage:

- Agreement by every member of the working group to adhere to a defined security strategy, policies and standards in areas that may affect more than one stakeholder;

- Creation of an agreed certification body for Smart Grid assets;
- Development of a thematic network of smart grid experts to share intelligence in a formal structured way;
- Agreement and definition of common Business Continuity Management (BCM) practices across the working group, to enable a secure and maintainable grid design to be developed;
- Creation of a holistic approach to security by ensuring that physical and cyber-security strategies are aligned.

High Level Security Requirements and Measures

For operational systems to mitigate the risk appropriately, it is necessary to ensure that security is engineered into the deployed solutions. Therefore the security requirements need to cover not only those things that are relevant in an operational system, but that the process of planning and development provides appropriate levels of assurance that compromised solutions are not deployed.

The scope of a **Information Security Policy** needs to cover the full scope of each organisation that implements or supports Smart Grid element, recognising that Smart Grid security is dependent on effective interactions across organisational boundaries. The scope should include both ICT and operational technology (e.g., SCADA, development and test environments). Information security policies based on ISO/IEC 27001:2005 tend to focus on information systems and assets. The deployment of smart grid requires that the stated mitigating controls extend also to operational systems and assets, and that additional controls are deployed.

To support effective **organisation of information** security, design should be an integral component of the organisational security management system. Role definitions should seek to harmonise and integrate skills sets for securing operational security and information security systems. The use of **external parties** to develop solutions should be subject to independent verification and audit.

Operational and informational assets should be clearly identified. **Asset management** scope that is traditionally covered by ISO/IEC 27001:2005 should be extended to include operational assets. Classification methods that are used for informational assets should also extend to cover operational assets. Both sensitivity and criticality should be considered.

Risk associated with **human resources security** needs to identified and managed throughout the employment lifecycle. The risk associated with engaging third parties within the development lifecycle needs to be appropriately mitigated (e.g., through background checks). Many organisations are dependent on third party development services. Without adequate controls, the security of organisations and the services that they provide are exposed at the development and all subsequent phases of the lifecycle.

Development environments should offer appropriate **physical and environmental security** controls to protect the confidentiality of intellectual property, integrity of designs and their implementation, as well as the integrity of the development processes and procedures. Consideration should be given to the security of on-site facilities where development and deployment is undertaken.

Development of **communications and operations management** systems and processes should be subject to the same controls as for informational systems. Where development processes and environment are themselves reliant on communications and operations management systems (e.g., for off-shore scenarios), these should be subject to risk assessment and controls implemented to protect the development environment and the assets that reside within it. Consideration should also be given to international regulation concerning possible limitations of deploying cryptographic technology.

Development environments should be restricted to those authorised to access them through effective **access control** processes. Controls to separate development from production / operational environments should be deployed with no development taking place on production environments. This is to ensure that these environments are not exposed to risks to continuity of service.

A process should be implemented for **information systems acquisition, development and maintenance**. Its scope should cover both informational and operational systems. The acquisition of third party products and services should be risk assessed with at least the same degree of rigour as for those developed internally. A known source of risk to the integrity of control systems is through attacks on the up-stream supply chain.

Intelligence that is derived from analysis of incidents handled by **information security incident management** processes should be factored into the design and development of new systems. This is to ensure that incidents reporting and management is supported by the new systems (e.g., through capture and logging of relevant information).

Development environments should be subjected to effective **business continuity management** processes. Consideration should be given to the continuity of provision of third party software and services, covering the operational risks of suppliers as well as the market risks that may affect the suppliers' ability to fulfil its contractual obligations.

Considerations regarding **compliance** in the development lifecycle include but are not limited to privacy requirements, NERC-CIP (for the US), cryptographic rules. The organisation may have obligations to its customers through regulation to demonstrate the effectiveness of its controls (e.g., SOX, SAS 70).

On overall terms, the following general high level security measures can be recommended for the robustness and resilience of Smart Grid ICT infrastructures:

- All architectural layers of the smart grid, taken independently (power layer, communication layer, information layer...), should be as robust and resilient as possible. Each layer shall validate the correctness of its input data before using it.

- Power devices should be able to overrule ICT-issued commands whenever they are seen as not electrically appropriate (i.e. they may compromise electric safety), even when the addressed asset is owned by a prosumer (e.g., Distributed Energy Resource (DER)).

- The smart grid ICT infrastructure should be able to switch to independent back-up power in case of outage of their main power source.

- The information architecture for communication and processing should be distributed, to minimise the risk that attacks on a critical node could lead to global compromising.

- Smart Grid ICT infrastructures should be deployed with sufficient redundancy to provide the intended level of availability, also taking into account the shorter lifetime of ICT equipment compared to power elements. Ideally, deployment should be planned so that redundancy is ensured between equipment with different expected lifespan, to limit the risk of redundant equipment failing simultaneously. Redundancy between equipment in different geographic locations should be preferred to limit the risk of disruptions, and required for critical elements (this requires that all the information required for operation is available in all places to enable service take over).

- The large amount of information acquired from sensors and processes within the smart grid ICT infrastructure should be exploited for predictive rather than reactive maintenance of ICT equipment as well as power elements.

- The amount of traffic exchanged on the smart grid ICT infrastructure should be minimised, by promoting local processing of the information within a node and communicating only the minimum required information to other nodes.

- The communication links of the smart grid ICT infrastructures should be dimensioned to withstand surges in traffic that may occur even as a result of emergency situations. Extensibility and flexibility should be promoted to facilitate adaptation to evolving traffic conditions.

- It should be possible to isolate affected ICT components, where such precaution is necessary to prevent extension of damages to other elements (e.g., cascading effects).

Regarding the involvement of Distributed Energy Resource and Storage within the grid, grid resilience will benefit from requiring the support of islanding, especially forced islanding imposed by grid outages. The main impact for supporting islanding will be more on power equipment than on ICT infrastructures. However possible disruptions of the grid ICT backbone in emergency situations should not prevent fall-back to islanding mode, and may even be used as a trigger for switching into islanding mode.

Standards for DER and Storage integration in transmission and distribution systems that properly address the power disturbance they may generate when switched on and off (avoiding possible cascading effects on triggering conditions) will be essential to ensure smart grid stability and resilience. This requires proper standards for modelling such resources.

It is clear that an extensive set of security measures needs to be applied to ensure the security and resilience of smart grid ICT infrastructures, be it at the technical level (for products and services) or at the organisational level (for involved organisations and processes). But in the end, Smart Grids are very complex systems which involve a large number of actors, some of which may be subject to different requirements and regulatory frameworks (e.g., energy distribution companies and telecommunication operators). Assuming that each actor masters its own domain, we can hope that proper security and resilience will be implemented sustainably, but for this to happen, the biggest challenges of the smart grid environment still need to be overcome:

- Actors of different domain (e.g. utilities and telecommunication companies) need to be able to cooperate, despite their differences in culture, business practice and professional languages.
- But most of all, despite the complexity of the ecosystem, the legal and regulatory framework must clearly establish the responsibilities of all actors, be it in terms of reliability or security incidents, so that each involved stakeholder is aware of its potential liability in case of incidents and takes due diligence to address the risk in its own domain. Special focus should be given to privacy issues and commercialization of micro-generation in order to reach the engagement of the prosumer / European Citizen.

Incorporate data security measures to Smart Grid communication protocols and infrastructures

Smart grids mean different things for different domains, different stakeholders, and different areas in the world. The Expert Group has systematically analysed and described how to implement new protocols, security measures or counter-measures by using current and widely adopted international standards. The Expert Group worked from a generic perspective trying to cope with different definitions and scenarios related with smart grids.

Smart grids will require suitable ICT-based systems with the appropriate levels of reliability, bandwidth and protection within the grids.

Regarding the total grid system reliability, there has to be a clear separation between ICT within the grid, which are necessary for normal power grid operations, and the ICT used within the peripheral innovative business which are not critical to the power grid operations. Maybe there must be gateways between those ICT domains to achieve a secure system. In any case, the power grid and ICT system controlling its operation are critical infrastructure that should be protected. It could be targeted by potentially powerful attackers, such as foreign countries or activists. This makes security and resilience challenges more difficult but also more important to achieve.

Cyber Security requirements already exist for specific applications and domains. They differ in granularity and scope, ranking from process oriented to technical standards. Some standards address the operator, while others contain very detailed implementation requirements. The subsequent bullets list relevant documents:

- IEC 62351-1 to 6, *Power systems management and associated information exchange - Data and communications security*.
- NERC CIP-002 and CIP-003 to CIP-009.
- IEEE 1686-2007, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*, Institute of Electrical and Electronics Engineers.
- ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*
- ANSI/ISA-99, *Security for Industrial Automation and Control Systems*
- NIST Special Publication 800-82

But not all protocols have a "security" extension. As an example, IEEE 1588 has no security mechanism at all while being crucial for protection applications. In addition to domain- and application-specific standards, common and application-spanning aspects need to be addressed. This is especially true for the requirements covering the aspects of end-to-end security. Technical requirements will not be sufficient to address the complexity of the Smart Grid, especially towards growth and change. Operational aspects such as policies and training as well an on-going cycle of risk assessments needs to be developed and introduced.

- A specification of a dedicated set of security controls (e.g. perimeter security, access control) to protect the Smart Grid needs to be comprehensively developed. As an example, a specification of granular access controls for the discrete boundaries derived from compartmentalization needs to be determined.
- A compartmentalization of Smart Grid applications (domains) based on clear network segmentation and functional zones needs to be developed.
- A specification comprising identity establishment (based on trust levels) and identity management in the Smart Grid as a large network connecting a high number of entities and end points needs to be developed. It should cover the aspect of credential management (distribution, validation, revocation) as an essential part.
- Moreover, existing standards must be reviewed, adapted and enhanced to support general and ubiquitous security across wired and wireless connections.
- IEC 62443 should confirm the standards architecture and the implementation methods, harmonize the constitution of standards with ISA and other organisations, speed up the standardisation process, and be compatible with the contents of the Smart Grid. The goal is to realise the unification and standardisation of any industrial control systems.
- Security of the legacy components in the Smart Grid was not fully considered in the initial design, thus the security performance was poor and difficult to upgrade. Standardisation of the physical protection and network protection should be enhanced for the legacy.

As described, there are almost standards enough to provide a strong security level for the future smart grid systems. Security should be considered as a fundamental part of those systems, implementing the required mechanisms from the beginning at all levels in order to weak and discourage possible attacks by using security in depth techniques.

Complementary to the recommendations from the critical infrastructure protection (CIP) view, it could be convenient to take into account a few known syndromes to avoid directly related with utility companies while analysing the challenges and recommendations for ICT security an resilience:

- The first one is related with the traditional nature of these companies. The assets of the utilities lasts for long time, this is the main reason they are extremely traditional. Since the energy grids undergo heavy changes we should avoid the syndrome "**BTTWWADI**" (**B**ecause **T**hat's **T**he **W**ay **W**e have **A**lways **D**one **I**t"). However this is already changing and will keep changing, in most cases beyond the point of no return.

- Another common syndrome is related with the size of our systems. Our information systems are so huge that we are used to split our system into smaller and disconnected ones. This behaviour should

change too. In order to deal with smart grids, integration while distribution is a must. So "**Silo Mentality**" should be avoided too. Vertical and disjoined approaches should be replaced by horizontal and integrated ones. On the other hand, we might need to stick to the common approach (in grid architecture and operation) to limit repercussions of failures and attacks as good as possible to the already affected part of the grid.

- Finally, utilities in the past have commonly relied on proprietary security solutions, sometimes called "**Security by Obscurity**". Instead, the use of standardised security mechanisms and protocols should be promoted while using reliable and well-supervised (third party supplied) ICT-services (Consider DigiNotar disaster).

The conclusion might be to reconsider the traditional approaches, evaluating necessities that led to them, and then include these necessities into the requirements regarding the on-going development of the energy supply systems into smart(er) grids.

Example: Keeping energy delivery up and running as good as possible can easily be identified as one of the main drivers for above mentioned approaches, but there are definitely more like the need for economical feasible solutions and others, that also need to be considered.

Procurement recommendation and standards for the Smart Grids

The Expert Group identified the need for establishing a common procurement language and/or standard for a base level of security in smart grid components and services in collaboration with private and public asset owners, vendors and regulators.

Procurement for components (like control systems) in the smart grids is even more important since a lot of these components are not easy to replace or to update, once they are installed. They have typical life cycles between 15 and 30 years. Therefore, security should be built in from the beginning and not thought of at the end.

Procurement of third party services for Smart Grids, such as maintenance of (sets of) smart grid components and of integrated parts of the smart grid, requires a common base level in Europe on minimal security requirements with respect to these services, (ICT) tools to be used, personnel as well as the protection of the physical environment of smart grid component(s), e.g. protection against theft and unauthorised access.

Currently, utilities are left hoping that the Smart Grid system components they are deploying are adequately addressing current and emerging cyber security threats, with little more than faith in the security claims their vendors provide as initial evidence. Utilities are then forced to dedicate significant resources to test the security claims their vendors make, and many utilities simply do not have the resources to expend on such testing (regardless of the size of the utility). This is a similar challenge that other critical infrastructure sectors face and have faced. The plan security workgroup of the WIB[16], The International Instrument Users' Association created a set of baseline security requirements for vendors, driven by the security needs of end users. This workgroup was lead by Royal Dutch Shell, one of the largest energy companies[17] in the world. Shell has mandated third party certification against the WIB security requirements for all of their vendors that operate in the Process Control Domain.

Following this line, Southern Company, a big utility in North America, followed suit by mandating the same for their vendors. It worked together with Wurldtech, the first company to create a certification program for the WIB requirements. This certification program is known as Achilles Practices Certification[18] (APC). The first Advanced Metering Infrastructure (AMI) vendor, under the mandate from Southern Company, to achieve APC certification was SENSUS[19].

The WIB 2.0 requirements, which were developed to address Electric Industry security requirements lacking in version WIB 1.0, are well-aligned with the NISTIR 7628 requirements. This led to the submission of the WIB

[16] www.wib.nl
[17] https://www.pfcenergy.com/~/media/Files/Public%20Files/PFC%20Energy%2050/Final_PFC_Energy_50_2012.pdf
[18] http://www.wurldtech.com/achilles-certification/achilles-certified-practices/program-summary.aspx
[19] http://www.sensus.com

2.0 requirements to IEC as part of the IEC 62443 series of cyber security standards for industrial automation control systems (IACS), and was approved as a project within IEC in the summer of 2011. IEC 62443-2-4 is about security requirements for vendor of IACS; smart grid devices being a sub-case.

It will still take some years before the IEC62443 series are finished and adopted. It is important to bridge the gap and already agree on a standardised set of cyber security requirements throughout the Smart Grid industry. This team will give advice to the European smart grid community how to bridge this period and how to establish a baseline set of security requirements that everyone in the smart grid industry can adopt.

2.3. Information and knowledge sharing

The Working Group identified the need for systematic information and knowledge sharing among the stakeholders. Although trusted information sharing platforms are common in other sectors i.e telecommunications, this is not the case with the Smart Grids. Only a few initiatives, with limited publicity among the stakeholders, are in place at the moment. Therefore, the following measures are recommended:

- The establishment of trusted information sharing platforms aiming at addressing the security of the Smart Grids at strategic level. By information sharing we mean the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice. A common name for this kind of platforms is Network Security Information Exchange (NSIE). We envisage the SG-NSIE as a form of strategic partnership among public and private stakeholders involved in the provision of Smart Grid services. Its scope would be limited to addressing the security of Smart Grids in both the public and private domains. The partnership will work at a tactical and strategic level by exchanging information on security incidents, vulnerabilities, threats and solutions in a trusted environment to ensure that barriers to sharing are minimised.

  The most popular structure to facilitate this sharing is a trusted platform where private sector infrastructure owners or operators can meet face-to-face at regular intervals and hold informal, un-attributable discussions. Frequently (but not exclusively), such groups are moderated or facilitated by a public sector agent. These may be within Public-Private-Partnerships (PPPs) or other more formal or informal mechanisms (e.g. established by regulatory authorities or collectively by industry). ENISA has already published a good practice on how to establish and maintain such kind of trusted information sharing platforms[20]. The partnership might be a new one or be hosted by an already existing one i.e the EP3R.

  The focus of this exchange is mostly to address malicious cyber attacks, but also natural disasters or physical attacks. The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information which is not available from any other source or cannot be easily found elsewhere. Incentives and barriers for trusted information sharing must also be taken into account[21].

- In addition to the trusted information sharing platforms which work at a strategic and tactical level, Member States have to consider initiatives aiming at building national Smart Grid Computer Emergency Capabilities (SG-CERC). This capability will aim at supporting and provide assistance to the affected entities in cases of security incidents related with the smart grid and might be developed from scratch or incorporated into already existing computer emergency capabilities (e.g. CERTs). The main differences between CERTs and NSIEs are that the former have an operational role on an incident or crisis, they tend to disseminate more information than they receive (on the contrary NSIEs are peer to peer networks where

[20] Good Practice Guide: Network Security Information Exchanges, ENISA, 2009, available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

[21] *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*, ENISA, 2010, available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

the information is exchanged) and usually only middle management or every day operation staff is involved in the process. Taking into account the lack of previous experiences in the field of smart grid response capabilities, the EC in cooperation with ENISA might address the issue by providing advice and recommendations to the Member States.

- Security related incident reporting must be institutionalized in a similar to the telecommunications sector (article 13a of the new telecommunications package) manner. The incidents might be reported to the national regulatory authorities or to other authorised entities with experience in handling this kind of sensitive information. To respond to this requirement, the Member states must develop information sharing and response capabilities similar to those described above.

- Apart from their well-known benefits (i.e increased level of readiness, increased cooperation, improvement in continuing planning etc) exercises might facilitate the transfer knowledge among the involved parties. Therefore, smart grid security relevant exercises must be planned, executed and then evaluated at regular intervals. The scope of these exercises should start from the corporate (intra-organizational) and then continue to national, regional and European level. Furthermore, the scope should not be limited only to the boundaries of the Smart Grids and ICS but also scenarios which involve interactions and interdependencies with other sectors (i.e telecommunications, ICT) must be tested and executed.

2.4. Awareness, Education & Training

Particularly relevant for the Expert Group is to identify and explore key policy issues related to raising awareness on (data) security of all the stakeholders involved in designing, manufacturing, system integration and operating and using the European Smart Grids. Securing the (data) in smart grids is not only the responsibility of the asset owners and the critical infrastructure operators. It is a combined effort of these two sets of actors with suppliers (system vendors and integrators, component suppliers, 3rd parties delivering services, IT and Telecom providers), research and knowledge institutes (research institutes, universities, education & training, standardisation bodies), industry (branch associations, industry organisations), government at the strategic policy-level (departments at policy level; regulators) and at the tactical/operational level (police, intelligence services and CERTs) and consumers/prosumers.

Awareness of the cyber and other risk factors related to the application of Smart Grids, the possible business impact and the possible impact on specific clients and society as a whole is the starting point for taking the right actions. A right level of awareness at all organisational levels combined with a sound knowledge of possible controls and measures to mitigate the risk will give these organisations the opportunity to make the right risk assessments and take appropriate actions.

Stakeholders should be aware of the risk factors that the Smart Grids face. Unfortunately, Smart Grids priorities regarding security are not easily defined. Looking at them from an "industrial and operational" perspective (e.g. considering for example the ICS environment), an AIC (availability, integrity and confidentiality) perspective is normally followed. In higher contexts the priorities are obviously reverted (i.e. CIA). The identification of the right trade-off between these priorities is part of the risk assessment and mitigation challenge. What matter, however, is the fact that attention should be paid to all these domains: Confidentiality, Integrity and Availability (including performance and timeliness) as well as data privacy (combination of organisation, integrity and confidentiality) and non-repudiation (e.g., electronic contracts). So the scope is broader than only data security, since data security is only one of the security aspects (though important) while implementing the smart grids in Europe. Stakeholders should be aware of the cyber security risk for the smart grids.

They also need to know their responsibility to contribute to achieving the primary protection goals of the Smart Grids like keeping up energy supply with a very high reliability and protecting consumer data to the necessary very high degree – taking into account the aforementioned risks. In order to raise this awareness, initiatives should be proposed to motivate stakeholders to take appropriate security measures to mitigate both the overall risk and risk in their own (business) scope.

Awareness is the key factor to secure the smart grids. There is a clear need to raise consciousness that cyber security is a critical component in our daily life and business. We need to learn from everyday practice to

identify the blind spots, educate and train stakeholders, exchange information on good practices and information gaps. Awareness about cyber security in Smart Grids is needed at all stakeholders and from their C-level officers down to the youngest maintenance engineer, since there is not one organisation that can fix the security challenges for the smart grids on their own. The asset owners and critical infrastructure operators of course have a very important role, since they are responsible for implementing and operating the smart grids, but it does not stop there. The Smart Grid risk factors are not limited to single organisations. Smart Grids bring multi-organisational risk components which overarch the whole energy supply and demand chains and include manufacturers of components, system integrators, 3rd party service organisations, regulators, research and development, and so on.

Particular attention has to be paid to the necessity to meet the primary protection goals for the emerging Smart Grids – at any point of time in the continuous further development towards their final implementation. Main goals are:

- Keeping up the energy supply with the necessary – i.e. very high – overall availability, even under condition of general crises (natural and pandemic disasters, failures or impairment of other critical infrastructures) and ICT-crises.

- Keeping the data security on the necessary level (e.g. very high integrity for grid control data, very high privacy for consumer metering data).

All stakeholders should take into account the vital need for a very high availability of the supply of energy. This is mandatory in the design, implementation and operation phase of all parts of energy infrastructures that contribute to the delivery of energy, or can endanger it. Since it will not be possible to quickly rebuild energy infrastructures under changing threats, this primary protection goal requires choosing solutions that anticipate or keep the vulnerability and susceptibility to changing threats to a minimum. Also awareness has to be built regarding the fact, that the degree of resilience and robustness already built-in in the functional view/general layer and energy-physical layers of the Smart Grids heavily influence the security and resilience necessary in the ICT-layers.

Next to the broad awareness raising activities regarding ICT security in general and the specific need for continuous robustness and resilience of Smart Grids, specific attention has to be paid to data security. A substantial part of the security that will have to be built into smart grids, especially in the smart metering segment of the value chain, is geared towards ensuring consumer data confidentiality and integrity, i.e. the basic requirements of data security. When building the inventory of implications and challenges of potential security requirements, it is important to bear in mind that the more privacy-relevant a particular data is, the higher levels of security it requires. In turn, to be able to provide the appropriate level of security, it has to be clearly known and understood exactly which data are privacy-relevant (you need to know what you are protecting in order to be able to protect it appropriately).

It is important to align the awareness raising activities with existing ones by, e.g., Smart Grids Taskforce, DG ENER's Mandate 490 on Smart Grids, ENISA with its stock-taking research on Smart Grids and ICS, the workgroup on ICS and Smart Grids within ERNCIP, the EU-US Working Group on Cyber Security and Cyber Crime: Expert Sub Group on PPP and ICS & Smart Grids, the European Network for Cyber Security (ENCS), national initiatives like, e.g., the National Roadmap for Secure Process Control Systems in the Netherlands, and similar ones in de US. The private sector is also very active at this moment in organising seminars on the topic of smart grid (data) security. At the same time it is important to bring the awareness not only to stakeholders but also on the standardization body's discussion tables, to ensure that the due attention to these topics will be paid in the delivery of the coming new international standards on the security of Energy Smart Grids.

In order to raise the awareness at all levels, initiatives should be proposed to motivate stakeholders to take action on security and privacy measures. This can be done through:

- Building and maintaining national and linked pan-European and global social network that brings experts together and cooperates in securing the smart grids.
- Facilitating the storage, dissemination and exchange of information and knowledge between public and private sector entities in Europe and around the globe.

    - Sharing of incidents, threats, vulnerabilities, good practices and policies across borders through conferences, workshops and an interactive information sharing platform.
    - Special targets are the C-level people in the private and the public sectors. This target group is dealt with in WP 4.1
    - Creating a general inventory of key implications/challenges with regard to data & privacy security in smart grids that potential security requirements would have. This issue should be dealt with in the other Sub-groups.
    - Involving standardisation bodies (ISA, ISO, IEC, ETSI etc.) in the definition of guidelines for the definition of permanent Information Sharing groups within Smart Grids interested entities as one of the requirements for improving their security. This is also a topic to be dealt with by other Sub-groups.

- Improving security capabilities (people, products, organisations) while ensuring compliance with industry accepted standards.
- Leveraging the skills and experience of global experts in collaborative and cooperative projects.
- Education & Training
    - Education & Training facilities in Europe for all organisation levels (up to and including the C-level)

In particular, Education & Training (E&T) is fundamental to counteract cyber security threats on the smart grids. Stakeholders will have to be educated and trained throughout the life cycle of new security solutions for Smart Grids. The E&T programmes will have to help stakeholders to think in different, innovative ways and experience new approaches. The focus of these E&T programmes should be on:

- Enhancing (and updating) awareness;
- Providing insight and perspective into real-case scenarios;
- Developing, experimenting and experiencing new (cyber security) concepts.

In particular, senior management training (C-level) is key since this audience is mostly responsible for the proper functioning of the critical infrastructures they manage. This specifically includes meeting the primary protection goals like the necessary high overall reliability of energy supply and ensuring the necessary privacy of end consumer data. Senior managers will be helped to understand the challenges they face and take responsibility. They will learn to take the most effective and appropriate actions within their own organisations. Courses will be developed in collaboration with relevant partners (like universities and private organisations in Europe and INL in the US). The E&T curriculum should consist of the following products:

- C-level training course
    - Unique course for the education of top management (C-level).
    - Gives overview regarding primary protection goals and discussion of the necessary contribution of the stakeholder.
    - Gives insight into cyber threats, vulnerabilities, risk factors and the disruptive effects of cyber attacks at strategic level.
    - Give insight that the degree of resilience and robustness already built-in in the functional view/general layer and energy-physical layers of the Smart Grids heavily influence the security and resilience necessary in the ICT-layers.
    - Handles policy and executive dilemmas and will provide insight into the current perspectives for policy makers (at C-level).

    - Consists of one hour classroom teaching, six hours table-top exercise (learning by doing during a serious gaming exercise) and a one hour wrap-up.
    - This class can be given in-house at the company.
- Classical training (including demonstration)
    - Enhancing security awareness and providing good and tangible practices.
    - Focus on cyber security aspects at the operational and tactical levels of professional organisations.
    - Either in-house at the company location or at the training organiser location.
    - Training courses will be available.
- Hands-on training
    - Cooperation with, e.g., INL which provides for instance the advanced ICS Security Training (also known as Red/Blue team training). This training should be tweaked towards smart grids. Also companies like Red Tiger Security in the US provide similar hands-on courses.
- Web-based training
    - Modules for different target groups will be developed. Internet courses will be available.

3. ANNEX I– Terms of Reference of the Expert Group

Expert Group on the security and resilience of communication networks and information systems for Smart Grids

1. INTRODUCTION

Smart Grids have been defined by the European Smart Grid Task Force[22] as electricity networks that can efficiently integrate the behaviour and actions of all users connected to it — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. Smart Grids could be described as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added.

Based on recent experiences, Smart Grids will substantially improve control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators[23]. 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. At the extreme, 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.

The development of Smart Grids exemplifies the increasing reliance of European economy and society on Information and Communication Technologies (ICTs). ICT infrastructures have become the underpinning platform for other critical infrastructures without which some services (e.g. in electricity transmission and distribution) could come to an abrupt halt. To tackle this challenge a multi stakeholders and multidisciplinary approach is needed involving relevant Energy and ICT experts.

2. POLICY CONTEXT

- The importance of interdependencies in general, and between ICTs and the energy sector in particular was first highlighted by the European Programme for Critical Infrastructure Protection[24] (EPCIP). The Directive on the identification and designation of European Critical Infrastructures[25] stressed the importance of identifying and analysing interdependencies, both geographic and sectoral in nature in order to improve the protection of national and European critical infrastructures. The EPCIP programme may therefore provide a general knowledge-pool to understand interdependencies, in particular between the ICTs and the electricity sector[26].

---

[22] See http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf.

[23] COM(2011)XXX of 12.April 2011, TBC

[24] COM(2005)576 of 17.11.2005, see
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF
COM(2006) 786 of 12.12.2006, see
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[25] Council Directive 2008/114/EC of 04.12.2008, see
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[26] In the context of the financing scheme accompanying EPCIP, a number of projects and studies were launched on this subject and an expert group on cross-sectoral interdependencies between the ICT sector and electricity networks was established. Further information on the on-going studies and projects as well as on the expert group is provided in the annexes.

- On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection[27] which set up the CIIP action plan to strengthen the security and resilience of vital ICT infrastructures.
- On 17 November 2010, the Commission adopted the Energy Infrastructure Package[28] which identifies the roll-out of smart grid technologies as a European energy infrastructure priority requiring particular attention in the Energy Infrastructure Package[29].
- On 31 March 2011, the Commission Communication on Critical Information Infrastructures Protection: 'Achievements and next steps: towards global cyber-security'[30], took stock of the results achieved since the adoption of the CIIP action plan in 2009. It describes the next steps planned for each action at both European and international level, including addressing cyber security challenges of smart grids.
- On12 April 2011, the Commission Communication on Smart Grids[31] underlines the importance to ensure the security and resilience of the ICT infrastructures supporting the deployment of Smart Grids in Europe.

3. OBJECTIVES OF THE EXPERT GROUP

The Expert Group will discuss how to strengthen at European Level the security and resilience of communication networks and information systems for Smart Grids.

Objective 1

Identify European priority areas for which action should be undertaken to address the security and resilience of communication networks and information systems for Smart Grids. The Expert Group is also expected to define recommendations on how to progress on each priority area at European level.

Objective 2

Identify which elements of the smart grid should be addressed by the Expert Group (e.g. smart appliances, smart metering, smart distribution, smart (local) generation, smart transmission) and to what level. The use of an existing common concept model should be considered.

The Expert Group will:

- Identify key strategic and high level requirements for ensuring the security and resilience of communication networks and information systems for Smart Grids.
- Identify a good practices guideline based on lessons learned and that develops how to secure and increase the resilience of the ICT lay down infrastructure of Smart Grids. Furthermore it will provide proposals on the way forward to ensure that cyber security challenges of smart grids are approached from a multidisciplinary perspective encompassing a dialogue and synergies between ICT security experts and energy/smart grids experts.
- Propose mechanisms/messages to raise awareness of decision makers related to the security risk of communication networks and information systems for Smart Grids, as well as possible measures to manage such risk.

This group will pave the way for high-level discussion on cyber security challenges of Smart Grids under the European Public Private Partnership for Resilience (EP3R).[32]Moreover, given the global dimension of cyber security challenges, a discussion on a common framework of cooperation between public and private sector at international level is already started under the EU-US Working Group on cyber security and cyber crime established in the context of the EU-US summit of 20th November 2010, held in Lisbon[33].

---

[27] COM(2009) 149 of 30.03.2009, Communication on Critical Information Infrastructure Protection – Protecting Europe from large scale cyber-attacks and cyber- disruptions: enhancing preparedness, security and resilience'
[28] See e.g. section 5.4.2. in COM(2010) 677 final of 17.11.2010 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SPLIT_COM:2010:0677(01):FIN:EN:PDF
[29] See e.g. section 5.4.2. in COM(2010) 677 final of 17.11.2010 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SPLIT_COM:2010:0677(01):FIN:EN:PDF
[30] COM(2011) 163 of 31.03.2011, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
[31] COM(2011)XXX of 12.April 2011, TBC
[32] Communication on Critical Information Infrastructures Protection COM(2009) 149.
[33] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597

4. MEMBERSHIP OF THE EXPERT GROUP

The Expert Group will be composed of European private and public stakeholders including representatives from:

- Member State authorities in charge of Network and Information Security (NIS), Critical Information Infrastructure Protection (CIIP) and energy sector;
- ICT industry and industrial associations;
- Organisations with experience in cyber security standards;
- Electricity generators and industrial associations;
- Distribution and transmission network operators and industrial associations;
- Suppliers of automation and control systems and associated technologies;
- Energy (and related, including emissions) trading entities;

The Expert Group is convened by the European Commission with the support of ENISA.

5. WORKING METHODS AND TIMING

To achieve the agreed objectives, and depending on the result of the identification of specific recommendations under each domain, the work could be carried out by different subgroups of experts.

It is proposed that the Expert Group will work until the end of 2012. The Expert Group should provide an initial set of deliverables by January 2012.

4. ANNEX II– Program of Work and deliverables (separate document)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu