10 October 2011

Programme of Work

Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids

DRAFT 1.1

Table of contents

1. Introduction

02 In recent decades the application of ICT systems in our Critical Infrastructures, like drinking water grids, energy grids, financial and communication infrastructures has been enormous. These systems have opened an unforeseen amount of opportunities. Infrastructures became highly efficient and flexible, which has been beneficiary for society. In the energy infrastructures, for instance, 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. In order to keep our infrastructures resilient we have to invest in secure and resilient architectures. This Program of Work focuses on the security and resilience of communication networks and information systems for Smart Grids. Improvements in information security increase the robustness and resilience of Smart Grids against all hazards, thereby reducing the probability and consequences of e.g., manmade mistakes, technical failure, deliberate attacks, and natural disasters in the future.

1.1. Mission, vision and goals

The mission of this Program of Work is to contribute to a coherent and increased effort to improve the cyber security for smart grids. In our view 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.[1] 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. Strategy

The strategy to accomplish a coherent and increased effort to improve the cyber security for smart grids is by aligning the Program of Work with current on-going work as executed by expert groups and associations within the European Union. In other words, instead of considering the Program of Work as a starting document for initiatives in the field of cyber security, it should be 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.

1.3. Scope

The scope of the Program of Work will be the security and resilience of communication and information systems that impact on the performance of the physical electricity infrastructure.[2] The physical threats of security are only taken into account in case it has a direct relation with communication and information systems. 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.

The topics that are covered under this Program of Work are typically approached with frameworks of COBIT and ISO/IEC 27001:2005. These frameworks help us to disentangle the subject of cyber security and to cover all relevant topics within the subject of cyber security. For example, COBIT defines 34 high level processes that are grouped into the following four domains:

1. Plan and organize: focusing on strategy: How can IT contribute to business objectives?

2. Acquire and implement; the topic of which is the identification, development or acquisition and integration of IT solutions to realize IT strategy.

[1] See MM Lessing (2008) "Best practices show the way to Information Security Maturity" for Generic Security Maturity Models.

[2] i.e. the gas network is out of scope.

3. Deliver and support, the domain whole is about delivering and supporting the whole range of IT services.

4. Monitor and evaluate the domain which focuses on the continuous assessment of all IT process to ensure their quality and compliance.

When applying an overall enterprise security approach based on the ISO/IEC 270xx family, ISO/IEC 27002 contains 11 different categories that have to be considered:

1. Security policy

2. Organisation of information security

3. Asset management

4. Human resources security

5. Physical and environmental security

6. Communications and operations management

7. Access control

8. Information systems acquisition, development, and maintenance

9. Information security incident management

10. Business continuity management

11. Compliance

The CEN/CENELEC/ETSI Joint Working Group on standards for Smart Grids proposes 5 security levels of smart grid information as shown in the table below.

Smart Grid Information Security Levels
(proposal- to be captures in a central repository for SG-IS Security levels interlinked with the Data protection class repository)

SG IS Security levels	Technical areas to be defined Agreed set of SG-IS and DPP must contain requirements in the following areas	Organizational areas to be defined Agreed set of SG-IS and DPP must contain requirements in the following areas	Comments
1 Low	SGIS SL 1 requirements in the following areas	SGIS SL 1 requirements in the following areas	
2 Medium	SGIS SL 2 requirements in the following areas	SGIS SL 2 requirements in the following areas	i.i.e. psuedonymized, annonymized data, that needs to be trustworthy (Data Authenticity)
3 High	SGIS SL 3 requirements in the following areas	SGIS SL 3 requirements in the following areas	This is normal operation band Personal Daten , Protection of privacy. Energy managment of Devices control functions directly (contract based) or via incentives based on contract or business data i.e. incentive offerings not yet covered by existing contracts End2End signatures .....
4 Very High	SGIS SL 4 requirements in the following areas	SGIS SL 4 requirements in the following areas	this is the level for critical Infrastuctures For Connecting Objects this level may be required for the Switch off Energy supply to the Object (from the point of view of the objects this is critical) This may also be the level required for distributing Customer Credentials(ID,Keys) or Admin People
5 Top Secret	SGIS SL 5 requirements in the following areas	SGIS SL 5 requirements in the following areas	reserved for country authorities - i.e. intelligence , police, fire department ...

2. Statement of Work

2.1. Work Package 1: Risk, threats and vulnerabilities

WP 1.1 Identify and categorise all relevant Smart Grid assets

Team lead: Rajesh Nair, Swiss Grid

Objective: In order to execute the work on the security and resilience of communication networks and information systems for Smart Grids, all relevant assets that are in scope need to be identified and defined.

Approach: The approach could be to study the existing first ideas on the Smart Grid Architecture (from Mandate 490) and Smart Meter Technology (from Mandate 441) and derive all relevant assets in scope of this Programme of Work. Furthermore, the EU issued a Reference Security Management Plan for Energy Infrastructure[3] which provides an example of an inventory of electricity grid assets. Moreover, Subject Experts Group 2 (Expert Group Smart Grids ICT Security and Resilience) covers this subject as it proposes a concept model for the identification and categorisation of smart grids assets, which comprises of the advanced meter infrastructure, the advanced distribution automation and the distributed energy resources.[4]

Results: A clear scope of assets involved.

Deliverables: A general identification, classification and definition of all relevant Smart Grid assets.

WP 1.2 Develop a threat and attack taxonomy for relevant assets

Team lead: Eric Luiijf, TNO

Objective: In order to be aware of the various threats that are relevant to Smart Grids, all hazards taxonomy has to be devised. The analysis and weighting of these threats makes it easier to determine how measures can be taken in order to mitigate the overall risk. This exercise needs to encompass both the information and the infrastructure dimensions of smart grids: It needs to consider threats to the confidentiality, availability and integrity of data in the system, as well as threats to the resilience, security and proper use of the infrastructure as a whole.

Approach: The approach would be to research which other taxonomies in the field of threats are already available and to assess to which extend these taxonomies would hold specifically for smart grid security. In addition to the all-hazards approach, key deliberate attack avenues and scenarios should be covered, encompassing the full palette for example from individual fraud attempts to large scale attacks against the infrastructure…
The development of attack/threat taxonomy is to a large extent covered by the work of Subject Experts Group 1 (ICT security and resilience of Smart Grids) which proposes the investigation of all hazards, vulnerabilities (location, technical elements, human elements, etc.) and impacts (severity, continuity of operation, etc).[5]

Results: A clear scope and classification of possible threats and their use by actors with hostile intend (e.g., attack paths) with regard to smart grids.

---

[3] EU (2010) A Reference Security Management Plan for Energy Infrastructure, Prepared by the Harnser Group for the European Commission, Under Contract TREN/C1/185/2009.

[4] Subject Expert Group 2 (2011) Challenges and recommendations for ICT security and resilience of Smart Grids. Recommendation to the European Commission. Working draft.

[5] Subject Expert Group 1 (2011) ICT security and resilience of Smart Grids: High Level Risk Analysis and Security Requirements

Deliverables: A general classification of the possible threats and their use by actors with hostile intend (e.g., attack paths).

Note: on long-term, the threat landscape for smart grids may evolve. The WP1.2 deliverables shall be developed in a way that it allows the re-use of the method and underlying materials for reassessment of the taxonomy of threats.

WP 1.3 Develop a countermeasure taxonomy for relevant assets

Team lead: Prof. Dr. Bernhard M. Haemmerli, Lucerne, University

Objective: In order to grasp the numerous possible countermeasures to Smart Grids taxonomy can be devised.

Approach: The approach would be to study which other taxonomies in the field of countermeasures to threats are already available and to assess to which extend these taxonomies would hold specifically for Smart Grids security. This is covered by the work of Subject Experts Group 1 (ICT security and resilience of Smart Grids) which proposes countermeasures (security requirements) for improving security and resilience after the risk assessment.

Results: An overview of possible countermeasure categories.

Deliverables: Countermeasure taxonomy for relevant smart grid assets.
A general classification per asset (see 2.1.1) of the countermeasures given a certain attack/vulnerability/risk, according to the proposed taxonomy as elaborated in paragraph 2.1.2.

WP 1.4 Develop a high-level security risk assessment methodology for relevant assets

Team lead: Zoltan Precsenyi, Symantec

Objective: Policy issues will include (but not limited to): objectives of risk analysis, enumeration of levels at which stakeholders should conduct risk analysis, process for prioritising risk factors, and phases and stages for risk mitigation.
With clear threat profiles taxonomies (see 2.1.1. and 2.1.2.); a general risk assessment methodology for Smart Grids should be developed to aid in taking complete and effective measures against the identified risk factors in a way that the remaining risk is acceptable to the responsible organisation.

Requirements: The risk assessment methodology should cater for a continuous improvement rather than seeing security as an absolute. The typical stages of an in-depth security approach (pro-act, prevent, prepare (e.g., training & exercising), detect, defend, recover, and incident follow up (e.g., identify lessons, remedies for future, in forensics, legal prosecution of perpetrators ...)) 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 calls for an end-to-end security perspective both within a single organisation and across the chain of multiple organisations. This is also to be included in the threat landscape and also brings identity and access management to the forefront of a secure system design.

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.

Possibly a case study can be conducted by applying the assessment methodology to an existing grid incorporating the smart grid plans in order to determine the adequateness of the high-level security risk assessment methodology for Smart Grids.

Approach: Use an existing risk assessment methodology and customize it for smart grids. The EU issued a Reference Security Management Plan for Energy Infrastructure[6] which provides a good high-level risk assessment methodology for electricity grid assets.[7] In addition, the holistic EURAM/EURACOM methodologies for risk assessment in combination with dependency analysis shall be taken into account. These methodologies were developed for EU DG Home with a focus on/application in the energy sector.
This particular subject is covered by the work of Sub-Working Group 1 (ICT security and resilience of Smart Grids) which proposes a high level risk analysis.[8] It proposes security requirements for improving security and resilience after the risk assessment.[9]

Results: A methodology for Smart Grids security risk assessment to aid in taking complete and effective measures against the risk encountered.

Deliverables: A high-level security risk assessment methodology.

2.2. Work Package 2: Requirements and technology

WP 2.1 Security Requirements

Team lead: David King, National Grid

Objective: Policy issues will include (but not limited to): categories of security requirements, formulation of high level security requirements and attributes of security measures, phases and stages for risk mitigation, and measures to reduce risk levels to acceptable levels and to improve the resilience of the smart grid network.

Approach: Start with the latest version security requirements work of the UK Security Technical Expert Group (STEG). Also, look for similar initiatives in all Member States. Identify best practices and arrive at EU security requirements that Member States could use.
The subject of security requirements is covered by the work of Sub-Working Group 1 (ICT security and resilience of Smart Grids) which proposes a high level risk analysis and security requirements for improving security and resilience.[10]

Results: Security requirements to be used by ESO's (CEN/CENELEC/ETSI) for standardisation work.

Deliverables: Categories of security requirements, formulation of high level security requirements and attributes of security measures, phases and stages for risk mitigation, and measures.

WP 2.2 Extend Smart Grid requirements to include effective security measures

Team lead: Francois Ennesser, Gemalto

Objective: There are currently Smart Grid standard initiatives that are useful in harmonising the design and operation of Smart Grids. In order to effectively secure Smart Grid communications these standards can be extended to include security measures. Standards need to be based on a threat and risk-based approach.

---

[6] EU (2010) A Reference Security Management Plan for Energy Infrastructure, Prepared by the Harnser Group for the European Commission, Under Contract TREN/C1/185/2009.

[7] Moreover, a thematic paper on risk assessment is to be issued soon on the topic of critical infrastructures.

[8] Subject Expert Group 1 (2011) ICT security and resilience of Smart Grids: High Level Risk Analysis and Security Requirements

[9] Subject Expert Group 1 (2011) ICT security and resilience of Smart Grids: High Level Risk Analysis and Security Requirements

[10] Subject Expert Group 1 (2011) ICT security and resilience of Smart Grids: High Level Risk Analysis and Security Requirements

Approach: The approach is to first analyse existing documents and build upon that to reach an integral overview of effective security measures. These documents could, for example, include the NISTIR Guidelines for Smart Grid Cyber Security[11]. Also the Subject Experts Group 2 (Expert Group Smart Grids ICT Security and Resilience) covers this subject as it proposes a methodology and general recommendations and challenges related to security measures.[12]

Results: Inclusion of effective security measures through smart grid requirements related to security

Deliverables: List of smart grid requirements related to security.

WP 2.3 Research Smart Grid communication protocols and infrastructures to incorporate data security measures

Team lead: Felipe Alvarez-Cuevas, ENDESA

Objective: There are various Smart Grid communication protocols currently in use at the lower OSI-layers. To ensure adequate level of data security, infrastructure security and resilience, it is advisable to include security strategies, measures and controls in the protocols and infrastructures, and to assess whether they are adequate. [13]

Approach: Examples from other industry areas can provide helpful models on how to incorporate data security, especially data confidentiality and integrity as well as business continuity and disaster recovery, into smart grid communications.
Of relevance in Europe in the field of consumer electronic devices (e.g. TVs), CI Plus has been developed as a technical specification adding increased security to the existing DVB Common Interface Standard. The latest CI Plus specification is very instructive. Likewise, in the field of broadband wireless communications, the WiMAX Forum's network architecture requirements (used in the USA, Asia and the Pacific region) rely on state of the art encryption and authentication for security.

Results: From a technological standpoint, data security as well as authorised infrastructure control and operation have has to be based on encryption and authentication. There needs to be standards to create a root of trust for smart meters and smart grid-related SCADA systems and devices, similar to what has happened for CI Plus and WiMAX. Such standards need not necessarily be developed from scratch, as suitable, established, validated and accepted technologies already exist for that purpose (covered in M490).

Deliverables: Data and system security measures and strategies in the protocols and infrastructures.

WP 2.4 (Public) procurement

Team lead: TBD

Objective: In order to push the development of secure components and enhance the security awareness within the vendor community (public) procurement standards need to be developed.

Approach: Using the IEC 62443-2-4 standard within the smart grid community.

Results: Standard for vendor practices of smart grid components, like the IEC 62443-2-4.

---

[11] NISTIR 7628 (2010) Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, the Smart Grid Interoperability Panel – Cyber Security Working Group. This document provides us with in-depth knowledge of smart grid cyber security strategy, architecture, and high-level requirements, privacy issues related to the smart grid including legal issues, and supportive analyses including bottom-up security analysis of the smart grid and research and development themes for cyber security in smart grids.

[12] Subject Expert Group 2 (2011) Challenges and recommendations for ICT security and resilience of Smart Grids. Recommendation to the European Commission. Working draft.

[13] As the subject of privacy is covered in other work programs it will not be covered in the program of work.

Deliverables: (Public) Procurement Standards.

2.3. Work Package 3: Information and knowledge sharing

WP 3.1 Develop a cross-border alliance between Member States and relevant competent bodies and organisations

Team lead: Wouter Vlegels, ENISA

Objective: A trusted network of public and private organizations can aid in sharing information about Smart Grid security. This trusted network should cover all aspects of Smart Grids, including energy sector, governments, IT, telecom, vendors, integrators, academia and research institutions. Public-private partnerships can make investments feasible and should be considered in these initiatives. An alliance where people meet and which has an appropriate technical infrastructure can be set up in order to be able to effectively share information about

(a) incidents, threats, vulnerabilities (e.g. based on proposed taxonomy) and
(b) The good practices of the public/private/international cooperation after occurrence of these incidents, threats, vulnerabilities. Also the cooperation and integration in the national risk plan and the cooperation with the CERTs should be taken into account.
(c) Other lessons learned/pitfalls in coping with incidents, threats, vulnerabilities.

Approach: A first step would be to identify existing alliances and assess to which extend these alliances could be incorporated in a newly built network covering aspects of smart grids. This should be done in cooperation with ENISA. Second, we should find a modus to sharing sensitive information, whereas threats and lessons learned could be more easily exchanged among bodies and organisations than vulnerabilities.

Results: A network organisation which acts as a flywheel in the sharing of information and knowledge about incidents, threats, vulnerabilities and good practices. Guidelines are provided from this network organisation. This information is being made available for companies to make accurate risk assessments. Member States can use the insights to draw future regulation.

Deliverables: a cross border network platform or organisation via which information can be shared.

2.4. Work Package 4: Awareness, Education & Training

WP 4.1 High level Conference for strategic leaders

Team lead: Alejandro Pinto, European Commission

Objective: Getting government leaders and CEO's to take the leadership role.

Approach: government leaders and CEO's will be invited based on concrete foreseen business impacts in order to convince them to participate in this conference.

Results: Awareness and exposure of the cyber security topic on high level.

Deliverables: A high level CEO conference on the security and resilience of smart grids.

WP4.2 Propose initiatives to increase stakeholder awareness on data security

Team lead: Auke Huistra, CPNI.NL

Objective: Stakeholders should be aware of the security risk for data. In order to raise this awareness, initiatives should be proposed to motivate stakeholders to take action on security measures.

Approach: 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 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).
An example of an existing approach is the German BSI's "Schutzprofil für Smart Meter" (Smart Meter Protection Profile) which gives a fairly accurate overview of where the most privacy-relevant data reside in the smart metering infrastructure, what the related privacy risks are, what level of protection is warranted, and how security should be built. Moving further from the individual smart meter to the whole of the smart grid, data protection and privacy will be related to the long term data retention requirements mandated by legislation, and the policies adopted by operators accordingly. From a technical point of view, these requirements and policies should be addressed by building certain technologies into the data centres and control centres of utilities, e.g. anonymisation, backup, deduplication, etc.

Results: Awareness by stakeholder's security risk. In order to raise this awareness, initiatives should be proposed to motivate stakeholders to take action on security and privacy measures.

Deliverables: A general inventory of key implications/challenges with regard to data security that the potential security requirements would have on smart grid.

WP4.3 Skilled personnel on cyber security in energy industry

Team lead: Klaus Kursawe, Radboud University

Objective: Skilled personnel on cyber security in energy industry

Approach: Develop set of courses in close cooperation with other relevant partners .An example could be the Idaho National Lab as part of the EU-US initiative on cyber security.

Results: Large workforce with sound knowledge and awareness of cyber security issues.

Deliverables: Set of courses from management level to engineers.

3. Timeline

Duration of the Expert Group:

The duration of the Expert Group is from September 2011 onwards until July 2012. From July 2012 the activities of consultation and dissemination start.

Duration of the individual tasks:

WP	Activity	Sep 2011	Oct 2011	Nov 2011	Dec 2011	Jan 2012	Feb 2012	Mar 2012	Apr 2012	May 2012	Jun 2012
1.	**Risk, threats and vulnerabilities**										
1.1.	Identify and categorise all relevant Smart Grid assets										
1.2.	Develop threat and attack taxonomy for relevant assets										
1.3.	Develop a countermeasure taxonomy for relevant assets										
1.4.	Develop a high-level security risk assessment methodology for relevant assets										
2.	**Requirements and technology**										
2.1.	Security Requirements										
2.2.	Extend Smart Grid requirements to include effective security measures										
2.3.	Research Smart Grid communication protocols and infrastructures to incorporate data protection measures										
2.4.	(Public) procurement										
3.	**Information and knowledge sharing**										
3.1.	Develop a cross-border alliance between Member States and relevant competent bodies and organisations										
4.	**Awareness, Education & Training**										
4.1.	High level CEO Conference										
4.2.	Propose initiatives to increase stakeholder awareness on security and privacy										
4.3.	Skilled personnel on cyber security in energy industry										