Cyber Security in Smart Grid Substations

Thijs Baars

Lucas van den Bemd

Michail Theuns

Robin van den Akker

Machiel Schönbeck

Sjaak Brinkkemper

Technical Report UU-CS-2012-017

September 2012

Department of Information and Computing Sciences

Utrecht University, Utrecht, The Netherlands

www.cs.uu.nl

ISSN: 0924-3275

Department of Information and Computing Sciences
Utrecht University
P.O. Box 80.089
3508 TB Utrecht
The Netherlands

CYBER SECURITY IN SMART GRID SUBSTATIONS

Thijs Baars
T.Baars@uu.nl

Lucas van den Bemd
L.vandenbemd@uu.nl

Michail Theuns
M.Theuns@students.uu.nl

Robin van den Akker
R.vandenAkker1@students.uu.nl

Machiel Schönbeck
M.J.Schonbek@students.uu.nl

Sjaak Brinkkemper
S.Brinkkemper@uu.nl

Abstract. *This report describes the state of smart grid security in Europe, specifically the Netherlands, and the cyber security of substations in particular. The focus of this study is the perception of risks and threats in smart grid cyber security and the international standards implemented in smart grids. The created overview is based on semi-structured interviews with 13 experts originating from eight different European countries. These participants are employed at electricity producers, grid operators, technology consultants and technology providers in the utilities sector. Their expertise ranges from information security to electricity grids, specifically smart grid security. Some of them are members of smart grid security related standard committees.*

The key results of the state of practice are the following:

1. *The interconnectivity of the smart grid with multiple stakeholders and European colleagues is indicated as the biggest threat to the security of the smart grid.*
2. *Another often mentioned threat is awareness. The experts generally indicate that awareness within top management is high. However, personnel on lower levels are reluctant to incorporate security in their processes.*
3. *All organizations are in a certain stage of implementing standards, the ISO27000 series most often. However, the experts indicate that they are waiting what standard is becoming the de facto before implementing it.*

From the interviews it can be concluded that the current state of cyber security is fragile. As the smart grid cyber security relies on an interconnected chain of organizations, it is as strong as its weakest link. Efforts are currently undertaken to prevent security threats and tackle risks, but these efforts are disparate; nearly none of the organizations in this research have fully implemented a

relevant standard, a single is already certified. There is still a long way ahead before the European and specifically the Dutch smart grid is fully secured. See chapter 5 for a detailed overview.

Besides these results, a Smart Grid Substation (SGS) Security Benchmark is presented in this report. This tool can be used to benchmark the level of cyber security of the smart grid within a utility organization. An organization can create a maturity profile by stating which of the 68 capabilities are implemented. Based on the results of the benchmark, the organization can identify areas of improvement and assist in creating a plan to improve its cyber security practices, thereby reaching a higher maturity level. The SGS Security Benchmark is based on capabilities described in international and North-American standards, and evaluated based on two rounds of semi-structured interviews with the aforementioned experts. See chapter 6 for a detailed overview.

1 INTRODUCTION

Because it is crucial to predict supply and demand for a continuous and efficient flow of electricity through the grid, the utilities sector has been investigating and implementing new technologies over the past few years. Especially with the advances in electric and hybrid cars, fluxes in the grid are becoming more apparent. Where formerly the demand was predictable because of rigid life patterns, such as time of breakfast, work-related travel and dinner time, electric cars and distributed energy sources, such as farmers with windmills and housing with solar panels, are distorting those patterns. This implies that supply and demand are harder to regulate, with consequences up to international power outages. The utilities sector is therefore increasingly adopting information technology to support their electricity grids, creating so-called smart grids. These smart grids can regulate the increasingly blurring line of supplier and customer, as they are selling and upstreaming energy produced by solar panels, or upstreaming unused energy in electric cars (Faruqui, 2010; Amin & Wollenberg, 2005). The electric grid's IT infrastructure has to be upgraded to account for this new usage. By interconnecting parts of the grid that were formerly separate and autonomic, it allows the grid to communicate with other parts in an effort to regulate, or micro manage, the electricity flows on a lower scale (see Figure 1.1). This, however, introduces a series of new vulnerabilities and threats to the grid.

There is widespread awareness of the importance of securing information systems. Shortly after the inception of the World Wide Web, various worms, Trojan horses, viruses and tools were developed to exploit weaknesses in information systems. Since then it has been a cat-and-mouse game played by security officers and attackers. However, with the introduction of new technologies within organizations and infrastructures, new potential vulnerabilities arise and should be addressed. Because of the potentially high impact of a successful attack on the electric grid, it is highly important that new smart grid technologies are secure.

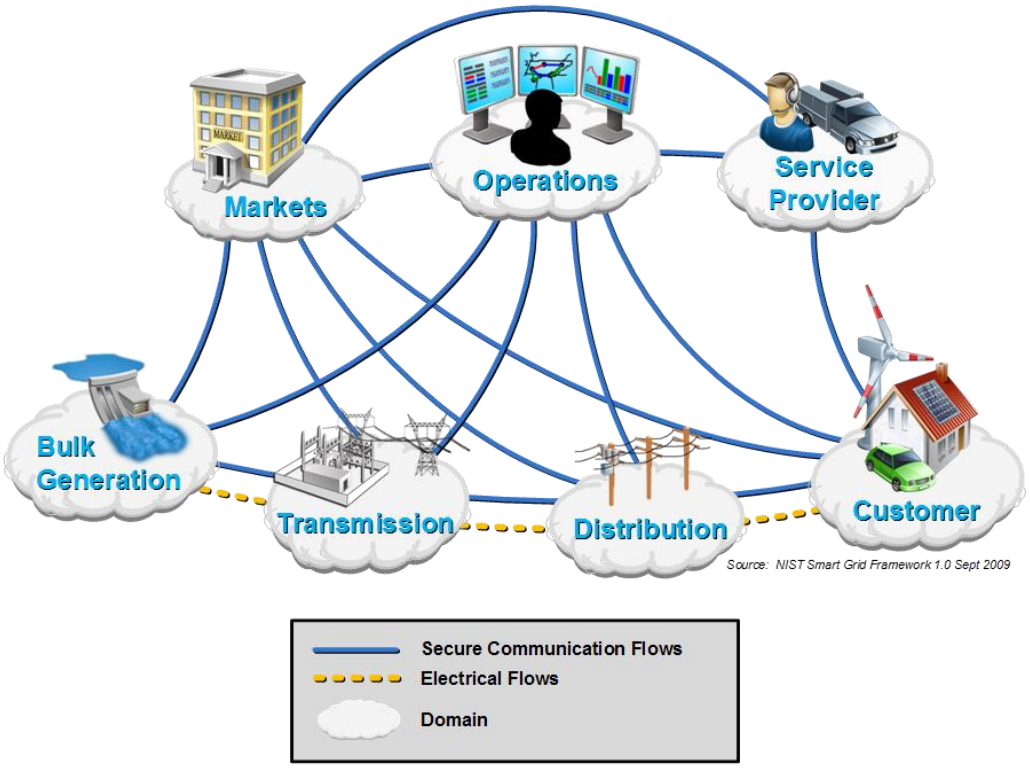

Figure 1.1: Interactions between actors in different smart grid domains (NIST, 2010)

Because it is crucial to predict supply and demand for a continuous and efficient flow of electricity through the grid, the utilities sector has been investigating and implementing new technologies over the past few years. Especially with the advances in electric and hybrid cars, fluxes in the grid are becoming more apparent. Where formerly the demand was predictable because of rigid life patterns, such as time of breakfast, work-related travel and dinner time, electric cars and distributed energy sources, such as farmers with windmills and housing with solar panels, are distorting those patterns. This implies that supply and demand are harder to regulate, with consequences up to international power outages. The utilities sector is therefore increasingly adopting information technology to support their electricity grids, creating so-called smart grids. These smart grids can regulate the increasingly blurring line of supplier and customer, as they are selling and upstreaming energy produced by solar panels, or upstreaming unused energy in electric cars (Faruqui, 2010; Amin & Wollenberg, 2005). The electric grid's IT infrastructure has to be upgraded to account for this new usage. By interconnecting parts of the grid that were formerly separate and autonomic, it allows the grid to communicate with other parts in an effort to regulate, or micro manage, the electricity flows on a lower scale (see Figure 1.1). This, however, introduces a series of new vulnerabilities and threats to the grid.

There is widespread awareness of the importance of securing information systems. Shortly after the inception of the World Wide Web, various worms, Trojan horses, viruses and tools were developed to exploit weaknesses in information systems. Since then it has been a cat-and-mouse game played by security officers and attackers. However, with the introduction of new technologies within organizations and infrastructures, new potential vulnerabilities arise and should be addressed. Because of the potentially high impact of a successful attack on the electric grid, it is highly important that new smart grid technologies are secure.

For that reason, the study described in this report has two main objectives:

1. Provide an overview of the current state of cyber security at electricity producers and grid operators, in Europe in general and the Netherlands specifically.
2. Present a tool for benchmarking the level of cyber security in utility organizations.

In this report, we address the cyber security of 120KV-20KV substations in the electric grid. Substations are generally controlled by autonomous SCADA systems, but can also be controlled through a local wired or wireless connection. Substations provide the link between power plants and the customer, and a successful attack on one of these substations could have fatal and expensive consequences.

To address the cyber security of smart grid substations, we develop a benchmarking tool for the cyber security of smart grid substations. The benchmarking tool is based on a maturity matrix, and can be used to measure the relative maturity of a company for a certain group of capabilities. The benchmark is specialized for smart grid cyber security, based on the current international standards on (smart) grid security. While the tool is based on maturity matrices used in enterprise architecture (Steenbergen, Schipper, Bos, & Brinkkemper, 2010) and software product management (Weerd, Bekkers, Brinkkemper, 2010), no developments towards a maturity matrix for the field of energy distribution has taken place in previous literature. This first version of the benchmark is then refined by evaluating it through a series of expert interviews.

In the next few sections, we respectively describe our research approach, the scientific background related to smart grid cyber security and an overview of related international standards. Following is a description of the process of creating the smart grid cyber security maturity matrix and a presentation of the results. This report concludes with a discussion of the results, conclusions and directions for future research.

This research is commissioned by DNV Kema. DNV Kema is a global energy consultancy company headquartered in Arnhem, the Netherlands. It offers management consulting, technology consulting and services to the energy value chain. Activities include business and technical consultancy, operational support, measurements and inspection, and testing and certification services.

Acknowledgements

We would like to thank DNV Kema, and Maurice Adriaensen in particular, for providing us with the resources required to conduct this research. We also would like to thank the experts for participating in this research and for providing us with valuable feedback.

2 RESEARCH APPROACH

This chapter elaborates on the research approach, with Figure 2.1 depicting a visualization of the steps taken throughout the project. First, a quick overview of the approach is provided, followed by an explanation of the separate parts of the approach.

This study was set up in six steps. The first step is a literature study, starting with the identification of the various internationally established standards regarding the security of smart grids (1.1). These standards are then transformed into a capability list (1.2). Related capabilities are categorized in focus areas, and related focus areas are grouped in three business functions (see section 3.2 for more information about capabilities, focus areas and business functions). The resulting groups of focus areas are used to construct the first draft version of benchmarking tool. At this point, the capabilities were not yet placed in the benchmarking tool.

In step two, we execute semi-structured interviews to gain an overview of the state of cyber security in the utilities industry, Europe-wide. During these interviews, the list of capabilities is evaluated. The interviews are conducted with experts in the utilities sector from different European countries (2.1). After refining the capability list with the feedback received during the interviews, the capabilities are placed in the benchmarking tool. This version is again evaluated during a second round of interviews with the same experts (2.2), which leads to several adjustments of the tool and the capabilities placed within the different levels.

The final results are an overview of the current state of cyber security in smart grids (see chapter 5) and a first usable version of a benchmarking tool for cyber security in smart grids (see chapter 6).

2.1 Literature study

At the start of this study a literature review on smart grids and its security issues is executed. The purpose of this literature review is twofold: it provides insight in current issues regarding smart grid security and it extends the body of knowledge of recent technological developments and standards in the field. The review is followed by the identification and extraction of relevant requirements. Many standards describe the importance of fire prevention, physical security and so forth, however, as our research focuses on the cyber security of smart grids and its components, such requirements are out of scope. All internationally accepted standards known by the researchers are used for the initial input of suitable requirements. These documents are gathered through internal sources at DNV Kema. The choice of included standards is furthermore determined by their scope (international) and availability in the English language. Including standards that did not qualify to these measures would threaten the generalizability of the maturity matrix and its international focus.

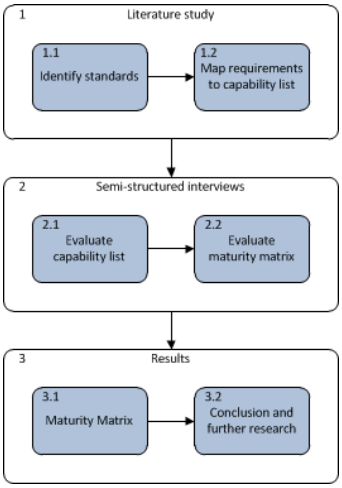

Figure 2.1: Research approach visualization

2.2 Semi-structured interviews

The interviews are constructed in a semi-structured nature. The objective of the interviews is to not steer away from the topic, while providing the freedom for the interviewee to talk about details or ideas that are not part of the initial interview protocol. The initial interview protocol can be found in "Appendix A: Interview protocol".

The participants for the interviews are carefully selected on four criteria.

1. *Country of operation*. In an effort to provide an overview of the state of cyber security in an European perspective, we selected participants from multiple European nations. In total, eight different countries are represented in this research.
2. *Type of organization*. Smart grids are diverse in the types of businesses that are operating it. In an effort to encompass that, this research includes technology providers, energy producers/grid operators and technology consultancies.
3. *Expertise*. As the smart grids are complex, one cannot expect every participant to have expertise in every asset of the smart grid. To counter this, participants with different expertise are selected. The expertise of the participants includes smart grids, grid security and information security. Smart grid security is composed of information security and grid security.
4. *Committee membership*. With a diverse range of standards, discrepancies in definitions and perspectives might obfuscate the results. We selected participants whom have membership in different committees to understand these discrepancies. By understanding the different perspectives of the standards, the deliverables could be designed to be objective yet making them understandable from these different viewpoints by inserting the necessary nuances.

In Table A an overview of the participants is shown, including their country of operation, expertise, business type and committee membership, if any.

#	Function	Business	Expertise	Committee
1	Security Consultant	Technology consulting	Information Security	Cigré WG B2, IEEE
2	Cyber Security Officer	Energy Producer/Grid operator	Information/Grid Security	IEC 62351, IEC 60870
3	Director	Technology provider	Smart grids, information security	-
4	Project Manager Operations	Energy Producer/Grid operator	Smart grids	IEC 61850, IEC 60870
5	Security Officer	Energy Producer/Grid operator	Information security	-
6	Program Security Manager	Energy Producer/Grid Operator	Information Security	-
7	Security Consultant	Technology consulting	Information security	ISO27000
8	Asset Manager	Energy Producer/Grid operator	Smart Grid	Cigré WG D2
9	Sr. Architect	Energy Producer/Grid Operator	Information Security	ISAC NRG member
10	Information security Officer	Energy Producer/Grid operator	Information Security	-
11	Cyber Security Engineer	Energy Producer/Grid operator	Information security	-
12	Consultant	Technology Consulting	Smart grids	IEC 61850
13	Director	Energy Producer/Grid operator	Smart grids	EC TF for Smart Grids: expert group 1 & 2

Table A: Research participants

Two rounds of interviews are held. The first round of interviews contains questions regarding the knowledge of the interviewee on smart grids, cyber security and the standards that their organization applies. The short overview of the topics to be discussed in this round of interviews was sent to the participants beforehand. This way, participants can gather information needed for the interview beforehand because during the interview there would not be a possibility as the interviews are executed per telephone. Also, not all participants spoke fluent English. Sending a basic frame of reference allows those participants to prepare themselves and lowers the language barrier. By sending a topic list in advance, and not the actual questions, participants could prepare on the topic without the risk of returning politically correct answers. These interviews provide insight in their opinion on the risks and solutions in cyber security, but also on the matter of how standards are used in practice. Additionally, this round of interviews evaluates the capability list, resulting in an improved list of capabilities which we sequentially assigned to the different levels of maturity in the benchmarking tool, as part of step 2.2.

In the second round of interviews the benchmarking tool is evaluated. The feedback of the capability lists, including the focus areas, is processed and the capabilities are given their respective locations in the tool. The interviewees were given the opportunity to give critical feedback regarding:

1. The new capability list. The order of the capabilities and the focus areas, as well as the capabilities itself.
2. The location of the capabilities on the benchmarking tool, concerning their individual maturity level
3. The location of capabilities relative to one another. The correctness of the estimated differences in maturity between capabilities.

The received feedback is sequentially compared with one another and the literature. In certain cases the perspectives of the literature and the feedback differed significantly, in other there was consensus. As the maturity matrix is a “best practice” tool, feedback from participants are given precedence, unless common sense restricts to do so.

The feedback of the experts led to the following changes:

- 48 capability changes were suggested
- capabilities were removed from the SGS Security Benchmark
- 9 capabilties were added to the SGS Security Benchmark
- 12 capabilities were placed on a higher maturity level
- 10 capabilities were placed on a lower maturity level

2.3 Matrix development

One of the deliverables of this research is to create a tool for benchmarking the level of cyber security within a utility organization. A maturity matrix is a perfect tool for this goal, as it allows the measuring of a topic at multiple factors in a detailed way. The level of maturity of an organization is determined by the lowest implemented capability in the matrix. The capabilities not implemented indicate a plausible vulnerability that can be exploited by possible attackers. This study presents a benchmarking tool which can be used to incrementally improve the cyber security of substations.

To aid researchers and practitioners in developing maturity models for incremental process improvement in new functional domains, Steenbergen et al. (2010) developed a standard method for developing maturity models. The method is presented by the process-deliverable diagram depicted in Figure 2.2. The left-hand side of the diagram represents the activities to perform, and the right-hand side represents the deliverable concepts that result from carrying out the activities.

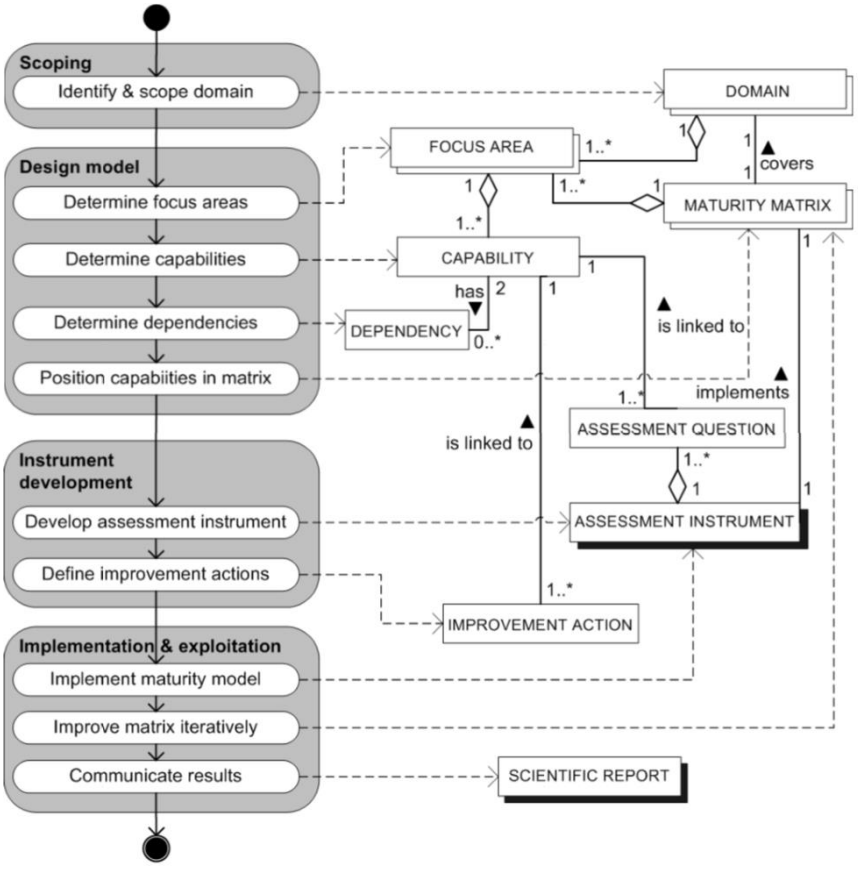

Figure 2.2: Process-Deliverable Diagram of the development method for maturity models (Steenbergen et al., 2010)

The method consists of ten steps and results in a maturity matrix for a specific functional domain (see section 3.2 for more elaborate information on maturity matrices). However, the last five steps concern the implementation and incremental improvement of the maturity matrix.

As implementation of the maturity matrix it out of the scope of this research, only the first five steps are executed:

1. *Identify and scope domain*: In this case, the functional domain is the cyber security of smart grids in general and electric substations between 120KV and 20KV in particular.
2. *Determine focus areas*: After deriving a long list of requirements from various international standards, the requirements are categorized into fourteen focus areas. References to the requirement's literature were kept to maintain visibility for later processing.
3. *Define capabilities*: From the focus area, an average of four to five capabilities are derived. These are ordered from very basic to advanced. The resulting list of capabilities is evaluated through semi-structured interviews with field experts. The experts are given the opportunity to study the list and return feedback and suggestions on how the list could be improved. After the first round of interviews is completed, the capability list is updated according to the feedback from the experts.
4. *Determine dependencies*: dependencies between capabilities are determined to ensure that capabilities that are dependent on the implementation of other capabilities are given a higher level of maturity.
5. *Position capabilities in matrix*: the capabilities are positioned in the first concept version of the maturity matrix based on the dependencies defined in the previous step, the literature, experience and knowledge of the researchers. The position of the capabilities is evaluated through expert interviews (as can be read in more detail in section 2.2), which led to refinement of the benchmark ing tool and the final positions of the capabilities.

This results in the final benchmark tool, discussed in chapter 6.

A more detailed description of the process of maturity matrix development can be found in "Appendix B: Matrix development".

3 SCIENTIFIC BACKGROUND

3.1 Smart Grids

In the traditional electric grid, high-voltage electricity is generated in power stations and transported through transmission networks and distribution networks, each transforming the electricity to a lower voltage level. These lower voltage levels, ultimately 230V, reach the consumer. However, this one-way downstream of electricity is slowly converging into a dynamic network of up– and downstream of electricity. Customers are generating their own electricity using solar panels or wind generators, electric cars require peak electricity and flow it back when unused. According to Rodriguez, et al. (2007), the increased amount of distributed systems that are connected to the electric grid can create instability in the power systems and in the worst case even lead to outages. Moreover, the control of these new systems is a challenge due to the uncertainty in the availability of sunlight or wind (Blaabjerg, Chen, & Kjaer, 2004), whilst the renewable energy levels produced increase annually (Vries, Vuuren, & Hoogwijk, 2006). Consequently, it becomes necessary for utility companies to actively monitor the demand in electricity and adjust their generation of electricity accordingly. To counter the aforementioned problems, utility organizations are implementing an increasing amount of 'smart devices' into the electric grid.

According to Fan, et al. (2010), the 'smart grid' is an "intelligent electricity network that integrates the actions of all users connected to it and makes use of advanced information, control, and communication technologies to save energy, reduce cost, and increase reliability and efficiency". A high-level overview of a typical smart grid is depicted in Figure 3.1. As can be seen in the figure, renewable energy sources as well as traditional power plants deliver electricity to its customers. A number of smart devices is implemented to handle the problems described above. When a disturbance in the grid is detected, smart devices in substations can isolate the areas in which the disturbance occurred. Additionally, using a number of smart devices, utilities and customers exchange information in real-time to support load balancing, consumption management, distributed energy storage (e.g. in electric cars) and distributed energy generation (e.g. from renewable energy sources).

Implementing these smart capabilities into the electric grid brings forth several security risks. Most of the devices in the electric grid were purpose-built and do not have extra capacity to perform security functions (Clements & Kirkham, 2010). For example, the smart grid is no longer used by a sole corporation, but by many actors. All these additional actors mean different roles, levels of authorization and a more fragmented data classification landscape. To allow all these actors access, current smart devices therefore employ internet technologies for communication. Examples include short-range wireless technologies such as Bluetooth for the interface between meters and end-customer devices, and cellular wireless technologies such as GPRS and UMTS for the communication between smart devices and the central system (Fan et al., 2010). However, wireless communications

bring a series of risks and threats along with them. Risks unseen before in the utilities industry, but already very prone to issues in other industries.

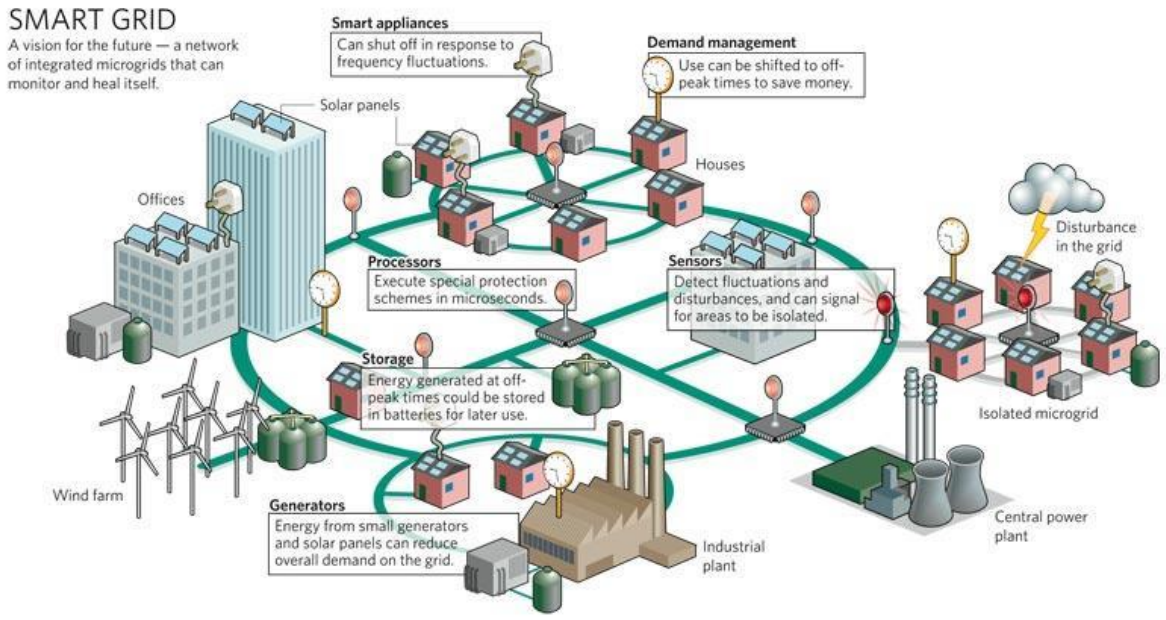

Figure 3.1: Overview of a typical smart grid (SG2030 Smart Grid Portfolios, 2010)

Figure 3.2 presents a conceptual model displaying all the communication channels in the smart grid. As can be seen, grid operators employ a large number of devices and communication channels to communicate with consumers about energy consumption, with service providers to support the billing process, and with the grid itself to monitor electricity transportation. These new technologies and mechanisms introduce new vulnerabilities into the power grid, because consumers and adversaries can use them to gain access to the smart devices.

The risks and vulnerabilities involved with deploying smart devices in the electric grid can be divided in risks with a low impact and risks with a high impact.

Low impact risks include malicious consumers spoofing the smart meters to attribute energy consumption to other accounts or manipulating data sent from the smart meter to falsify consumption reports. The goal for the malicious consumer is to gain economic benefits by reducing their electricity bill.

Another low impact risk involves gaining access to the utility's energy consumption registration systems to identify electricity use patterns to determine not only how much energy customers use but also when they are at home, at work, or traveling (Khurana, Hadley, Lu, & Frincke, 2010).

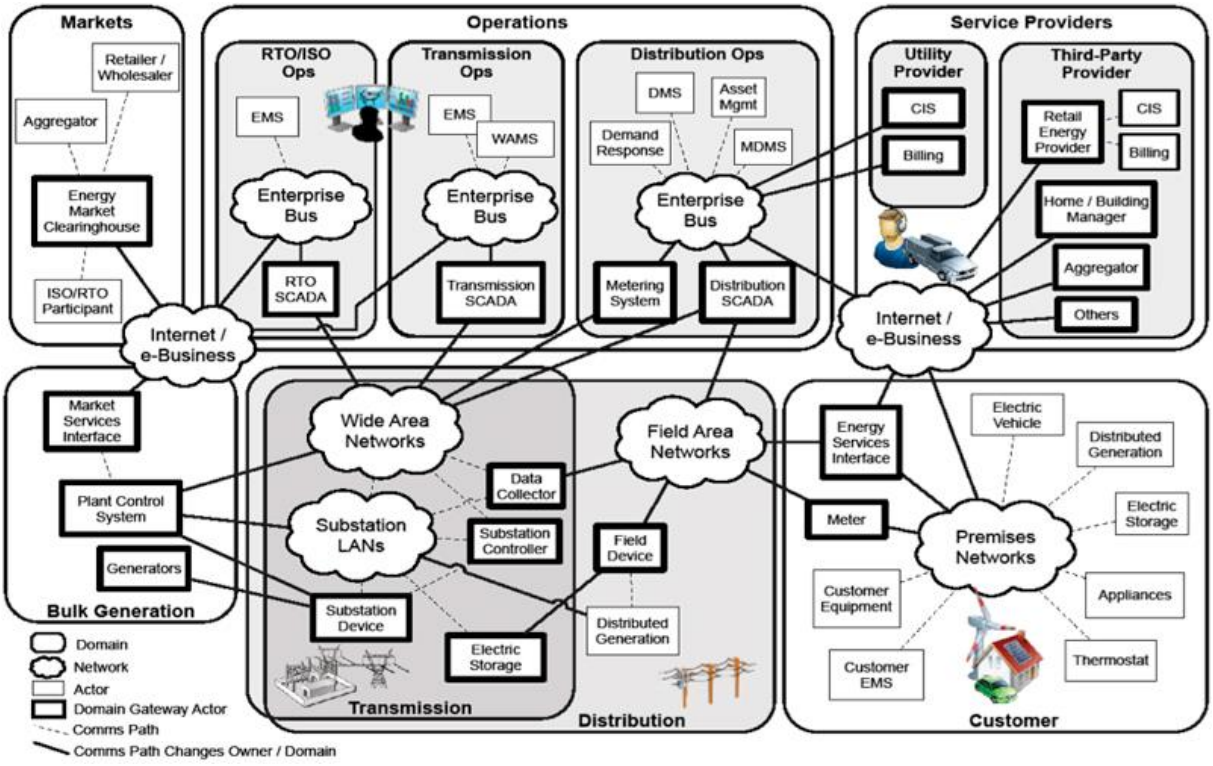

Figure 3.2: Information networks in the smart grid (NIST, 2010)

High impact risks may come from someone with more malicious motives, for example to gain access to transmission substations to shut down (part of) the electric grid. The goal here is to damage the utility in specific, or the economy in general.

A good overview of smart grid risks and vulnerabilities has recently been published by NIST (Lee & Brewer, 2009). While organizations try to mitigate all these risks, availability of electricity is seen as top priority. Confidentiality and integrity follow. Availability of energy is considered more important to most users than making sure that information about energy flows is confidential (Khurana, et al. 2010).

To counter these specific cyber security vulnerabilities, several international standards are being developed. Chapter 4 provides an overview of thirteen of these standards.

3.2 Maturity Matrices

Just as utilities are looking for ways to improve the cyber security of their smart grids, organizations in general are looking for ways to improve their processes. To assist organizations in this endeavor, several maturity models have been developed to assess the maturity (i.e. the competency, capability, level of sophistication) of a selected domain, based on a more or less comprehensive set of criteria (Bruin, Rosemann, Freeze, & Kulkarni, 2005).

In scientific literature on maturity models, three different variants can be distinguished (Steenbergen, Berg, & Brinkkemper, 2010):

- Staged 5-level maturity models distinguish five maturity levels, which in turn are associated with a number of processes that have to be implemented.
- Continuous 5-level maturity models also distinguish five maturity levels, but instead of attributing specific processes to the five levels, these models distinguish the five levels within each of the processes.
- Focus area oriented maturity models depart from the idea that there is a fixed number of maturity levels and assign each process with its own number of progressively mature capabilities (Steenbergen, Schipper, Bos, & Brinkkemper, 2009).

Because the staged and continuous 5-level maturity models (such as the CMM, its successor CMMI, and SPICE) try to fit many processes within five levels, they are often found to be too large to implement (Kuilboer & Ashrafi, 2000). Another limitation of these models is that they provide little guidance in determining the order in which to implement the processes, because they are not designed to express interdependencies between the processes making up the maturity levels (Bruin, Rosemann, Freeze, & Kulkarni, 2005). Focus area maturity models on the other hand, distinguish more than five overall stages of maturity, giving room for incremental process improvement by providing more detailed guidance into which steps to take in order to achieve a higher maturity level. Examples of these maturity models include the Dynamic Architecture Maturity Matrix (Steenbergen, Schipper, Bos, & Brinkkemper, 2010) and the Software Product Management Maturity Matrix (Weerd, Bekkers, Brinkkemper, 2010). An example of the latter with a filled-in maturity profile is depicted in Figure 3.3.

As can be seen in the maturity matrix in Figure 3.3, the matrix consists of columns and rows, which depict the two dimensions of the model. The left-hand column presents a number of focus areas (activities that are important to the domain of subject). The columns 0 to 10 represent the maturity levels, 0 being the lowest level of maturity and 10 being the highest. Each focus area can be carried out at different levels of maturity, which is represented by the capital letters A to F. The actual maturity of an organization can be revealed by coloring the cells up until the next capability that is not yet implemented. The rightmost column that is completely colored indicates the overall level of maturity of the organization. In the example in Figure 3.3, the overall maturity is level 2, because capability A of 'Scope change management' in column 3 is not implemented.

The capabilities are placed in best-practice order for implementation, meaning that (when reading the matrix from left to right) the first capabilities encountered are the first areas to address.

Maturity / Focus area	0	1	2	3	4	5	6	7	8	9	10
Requirements management											
Requirements gathering			A	B	C		D	E	F		
Requirements identification			A			B		C			D
Requirements organizing				A		B		C			
Release planning											
Requirements prioritization			A		B	C	D			E	
Release definition			A	B	C				D		E
Release definition validation					A			B		C	
Scope change management				A		B		C		D	
Build validation					A			B		C	
Launch preparation		A		B		C	D		E		F
Product planning											
Roadmap intelligence				A		B	C		D	E	
Core asset roadmapping					A		B		C		D
Product roadmapping			A	B			C	D		E	
Portfolio management											
Market analysis					A		B	C	D		E
Partnering & contracting						A	B		C	D	E
Product lifecycle management					A	B			C	D	E

Figure 3.3: Example of the Software Product Management Maturity Matrix (Weerd, Bekkers, Brinkkemper, 2010) depicting an overall maturity of level 2.

4 OVERVIEW OF CYBER SECURITY STANDARDS

This section provides an overview of the standards included in this research. These standards are used to identify the focus areas and individual capabilities. The first six standards are international standards, developed by international standards organizations. The last eight standards are focused on the North-American market, created by either North American standards organizations or the United States' National Institute of Standards & Technology. Table B reviews each standard's title and purpose.

Standard	Title	Purpose
ISO 27002	Information technology - Security techniques - Code of practice for information security management	Describes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
WIB 2784-X10	Process Control Domain – Security Requirements for Vendors	Gives recommendation for IT security to be fulfilled by vendors of process control & automation systems to be used in process control domains.
IEC 60870	Telecontrol equipment and systems	Defines systems used for telecontrol (supervisory control and data acquisition).
IEC 61850	Communication networks and systems in substations	Provides guidelines for the design of electrical substation automation.
IEC 62351	Power systems management and associated information exchange - Data and communications security	Provides guidelines for handling the security of TC 57 series of protocols.
IEEE 2030	Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads	Provides guidelines for smart grid interoperability
NIST SP800-53R4	Security and Privacy Controls for Federal Information Systems and Organizations	Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.
NIST SP800-30	Risk Management Guide for Information Technology Systems	Provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.
NIST 7328	Security Assessment Provider Requirements and Customer Responsibilities	Stimulates discussion and comments on the minimum capabilities security assessment providers should have to provide thorough and effective security assessment services.
NIST 7628	Guidelines for Smart Grid Cyber Security	Provides a comprehensive set of cyber security requirements.
NERC 1200	Cyber Security	Provides guidelines to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.
NERC 1300	Cyber Security	Provides guidelines to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.

NERC Security Guidelines	Security Guidelines for the Electricity Sector	Describes general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems.

Table B: Overview of all the cyber security standards used to form the first version of the cyber security matrix

ISO 27002. The ISO/IEC 27002 standard is an information security standard that describes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in organizations. The standard consists of 11 security control sections which contain 39 main security categories.

WIB 2784-X10. The WIB 2784-X10 standard provides recommendations for IT security which should be fulfilled by vendors of process control and automation systems. The standard consists of a list of "process areas" which are divided in multiple "base practice objectives". These objectives are composed of "base requirements" and "enhanced requirements". An organization can attain a certain level of compliance, i.e. bronze (base requirements), silver or gold (enhance requirements), when complying with these requirements.

IEC 60870. The IEC 60870 standard defines systems used for telecontrol (supervisory control and data acquisition). Such systems are used for controlling electric power transmission grids and other geographically widespread control systems. By use of standardized protocols, equipment from many different suppliers can be made to interoperate. The standard is developed by the IEC Technical Committee 57.

IEC 61850. The IEC 61850 standard has been defined in cooperation with manufacturers and users to create a uniform, future-proof basis for the protection, communication and control of substations. It focuses on station automation in substations. It defines the communication between Intelligent Electronic Devices and related system requirements. One of the main goals of the standard is to facilitate a faster and more reliable data communication. Purpose of the communication is to ensure that the right information is transferred and that this information is interpreted according to the standard. The standard is created by the IEC Technical Committee 57.

IEC 62351. The IEC 62351 is a standard for data and communication security. It is developed by the IEC Technical Committee 57 for the purpose of providing information security for power system control operations. Its primary objective in a broad sense is to take on the development of standards and/or technical reports defined by the IEC Technical Committee 57 on end-to-end security issues. The reason the IEC 62351 is developed is the increasing need for safety, security and reliability and the awareness that ensuring end-to-end security requires more than simple technological measures. Additionally, the current standards are not prepared to contain security measures. The 62351 series serves as an umbrella for the 60870- 5, 60870-6 and 61850 standards on the areas of authentication and communication security.

IEEE 2030. IEEE 2030 provides alternative approaches and best practices for achieving smart grid interoperability. It establishes the smart grid interoperability reference model (SGIRM) and provides a knowledge base addressing terminology, characteristics, functional performance and evaluation criteria, and the application of engineering principles for smart grid interoperability of the electric power system with end-use applications and loads. The IEEE 2030 SGIRM defines three integrated architectural perspectives: power systems, communications technology, and information technology. Additionally, it defines design tables and the classification of data flow characteristics necessary for interoperability.

NIST SP800-53R4. The purpose of this standard is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the minimal security requirements of for federal information and information systems, as defined in the NIST FIPS 200. These guidelines are developed to achieve more secure information systems and effective risk management within the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. Geographical focus area of this standard is the United States of America.

NIST SP800-30. The NIST SP800-30 standard provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks. In addition, this standard provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information.

NIST 7328. The purpose of the NIST 7328 standard is to stimulate discussion and comments on the minimum capabilities security assessment providers should have to provide thorough and effective security assessment services. The success of the assessment process is dependent on the partnership and cooperation of the providers and the customers. It aids federal agencies in selecting adequate security assessment services.

NIST 7628. The NIST 7628 standard provides guidelines for smart grids cyber security. The standard consists of high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for organizations. This information can be used to create strategies to protect the modernizing power grid from attacks, malicious code, cascading errors, and other threats.

NERC 1200. The NERC 1200 cyber security standard apply to actors within the smart grid, performing various electric system functions, such as control areas, transmission owners and operators, and generation owners and operators.

NERC 1300. This cyber security standard applies to entities performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission owner, transmission operator, generator owner, generator operator, and load serving entity.

NERC SG. This standard provides guidelines describing general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. Specific program or implementation of security considerations must reflect an individual organization's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk.

5 THE CURRENT STATE OF SMART GRID CYBER SECURITY

This chapter describes the results from the interviews with 13 participants. First, the general results are discussed concerning the perspectives on smart grids, smart grid security and their applications. Second, we address the state of smart grid security in Europe, focusing specifically on the perception of the risks and threats in smart grid security and the implemented standards. Third, we address the same issues, but then for the Netherlands specifically.

The benchmarking tool is a part of the results from this study, however it is separately discussed in chapter 6.

The definition of a smart grid remains vague. Of all the thirteen participants, we did not receive a duplicate answer. The different perspectives from the participants, identified primarily by their expertise, resulted in different answers. However, we were able to identify certain key aspects recurring in the definitions. Many participants mentioned the transition from the current, or legacy, systems towards integrated information systems. This includes the integration of current systems to enable them to communicate with other systems, at different levels in order to react in real time to real world events. A specific notion is made often for new users of these systems, or new systems in general that currently do not connect to the chain of implemented grid systems. These can be end-users becoming (micro) energy suppliers, other firms within conglomerates exchanging information within that conglomerate, or the interaction with other countries.

Smart grid security is defined as the protection of the assets, communication and data within a smart grid. The answers ranged from dictionary definitions to derivatives of them. Key in all definitions was the enhanced communications smart grids supply over its legacy brethren. Cyber security in this study is treated as equal to smart grid security. The participants did so as well.

From all participants, securing their grids in an information security fashion is a recent development that started less than half a decade ago. Stuxnet and other highly malicious code initiated many cyber security projects. This development has also brought awareness to higher management. Nearly no one mentions management to be troublesome in providing the means to execute the security measures. The step towards a smart grid is by some attributed to the overloading of the European grid in 2006

Smart grid security is perceived different among the participants. Some participants understand the issues primarily caused by the outdated legacy systems but see these as minor inconveniences as the environment does not allow for millions of users at the substation level. Those who believe the issues to be a minor burden have already experience in other fields and see smart grid security as “yet another implementation of information security”. They state that information security in the end is all the same, with minor adjustments to the specific industry. On the other hand, there are participants

who mention smart grid security as a major leap and foresee many issues. These particularly have a background in utilities and cyber security as a new endeavor.

The participants are active in committees, boards and platforms. All mentioned attending conferences and spreading their knowledge by means of white papers, presentations and such.

5.1 Smart Grid Security in Europe

Having interviewed participants from seven different European countries, a pattern emerged that allows us to believe that the results show an overview of the overall state of smart grid security in Europe. The interviews discussed the perception of security, the changes to be expected and the involvement of the organizations in cyber security. We detail this in section 5.1.1. The other main part of the interview discussed the standards and compliance. This provided with an overview of the implementations in process and finalized. This overview is detailed in section 5.1.2.

5.1.1 Perception of security

Looking at the results from all European participants, security is a high priority. The efforts have, all but a few exceptions, mainly begun around 2008 and are now fully running. However, that does not mean that all are in the same stage. Where some are reevaluating and restarting their efforts, others are practically finished.

In the eyes of the participants, security is very important, and most believe they are well secured. An interesting side note on that perception is that, as mentioned by few, the complete interconnection of Europe's grids has not been in effect. When that happens, new risks may arise.

There are no significant trends in cyber security noticed, except for a general rise in demand, and a higher priority of cyber security within organizations. This has also led that in the majority of organizations, management is not a burden. Awareness is great within the top management layers, and has ample capital available to support cyber security efforts.

The most common threat mentioned is the interconnectivity. As one participant mentioned, it is a weakest-link problem. All the utility companies can be well secured, but when one organization has not put enough effort in it, all the others efforts are effectively undone. The chain is as strong as its weakest link. Also often mentioned are high profile incidents. This is interesting, since most attacks in information security are not high profile. On the other hand, one could say that incidents at utilities companies are generally high profile as they affect the everyday life of many people. Employees are also frequently mentioned as the biggest threat. The experts identify that a large cultural overhaul is needed, and that at this moment the majority of personnel is not well aware of the risks of thumb drives and malicious downloads.

From our perspective, current utility organizations still have a lot to improve. Efforts are undertaken, but nearly none have fully embraced the standards regarding cyber security. A few participants mentioned that they feel they are secure since they have never had an incident.

Even though all participants state that much effort is being put into cyber security, nearly all of them also indicate that more should be done. There is however no consensus where these additional efforts should be allocated to. International relations, awareness, education, international policy in communication protocols, European wide mandatory standards were all mentioned.

5.1.2 Implemented standards

In all but one of the interviews it was made clear that the more abstract international standards such as those from the ISO and IEC are favored over those from the North American continent. The one organization that has fully implemented a North American standard, has implemented NERC version 3, which in essence is a wide variety of standards, concerning cyber security among others. The organization felt that the more opinionated NERC standards provides more guidance on the implementation of the standard and a more effective way of securing their organization and the assets that are part of it. They have fully implemented it, and used an accompanying tool to evaluate their implementation, and with that believe they are well protected and are in no need for other standards implementations. In the view of the researchers, they are at this moment the best protected utilities firm of the sample. Aside from this utility company, a technology provider (particpant #3) also adheres to the NERC standard.

The following analysis will discuss all other participating organization, except the one that implemented the NERC standards.

The ISO27000 series is by far the most prevalent standard to be implemented by the organizations. It is the center point of standardization efforts in all organizations, but the efforts are different in size and state of completeness. Half of the organizations participating have finished their ISO27000 implementation. The other half varies from starting their compliancy process to being nearly done. All but one has implemented or is in the process of fully implementing the ISO27000 standard. Those who implement the standard partially mention that parts are not applicable to them or have been implemented in other forms but are not completely conforming to the standard. Especially continuity has been mentioned often.

Some organization are actively implementing other standards aside from the ISO27000. These are primarily the IEC 68150 and 60870. Most organization mentioned that these are (too) new, hardware does not comply with those standards, and that the efforts are in orientation or very early stages of implementation.

Because of all the various efforts, most organizations are waiting to see which standards become the de facto. They also believe that in upcoming review sessions, the standards will become more mature, and are waiting for that to happen.

Most difficult when applying the standards is the organizational culture. Essentially, this means the awareness of the employees on security and the change in workflows and processes. Key is that higher management is fully aware and supports all efforts. However, security has never been an issue before, and organizations are noticing reluctance in acceptation and difficulty in change of behavior to work in a more securely fashion. The change in workflows as a result of the compliance to the standards has thus been difficult to implement.

5.2 Smart Grid security in the Netherlands

In total, six Dutch organizations have been interviewed, of which four participants were from three different utility companies. These organizations presented the larger companies in the Dutch utilities sector. We can therefore say that the results of the interviews have provided us with enough data to create an overview of the Dutch market. Our dataset represents approximately a third of the Dutch distribution system operators and 17 percent of all Dutch electricity producers.

The interviews concerned the same topics for the Dutch participants as for the Europeans, thus the perception of security, the changes to be expected and the involvement of the organizations in cyber security. We detail this in section 5.2.1. Standards and compliance will be discussed in section 5.2.2. It provides an overview of the implementations in process and finalized.

5.2.1 Perception of security

Compared to other European countries, the Netherlands scores average in terms of cyber security perception. Stuxnet is also here mentioned as the wake-up call. The perception of cyber security is clear: it is established that security is needed. There is awareness, albeit not enough. All of the participants mentioned that higher management have put cyber security on top of their list and are aware of the issues at hand. Some mention that awareness in the board room is not increasing as fast as they would like it to.

The Dutch grid is far from being a smart grid, and is perceived as such. Therefore, the participants believe that the current pace of implementation is correct. The participants indicate that there is ample time to implement the needed measures before the smart grid really takes effect in the Netherlands. They do state that effort is needed to reach that point, and that at this moment the network is not smart grid ready in terms of security.

Like the European participants, no real trends are identified, beside an increase in awareness. The main threats differ also between the participants, mentioning not enough knowledge within the organizations, cooperation with other parties, to cyber warfare, and general unavailability of power.

5.2.2 Implemented standards

The Dutch sector, similar to the European one, is currently implementing the ISO27000 standard. All of the interviewed organizations have started and are well on their way. A few are investigating other IEC standards, but have not yet started the implementation process. They mention the same issues as the Europeans: lack of maturity, lack of hardware support and the lack of a stance by European colleagues or the European Union.

None of the Dutch organizations interviewed are implementing the full standard. They mention that the ISO27000 standard does not fit with the organization and that it is difficult to have all the competencies available that are required by the standard.

Interestingly, there is no consensus on the most prevalent issues when adopting the standard. The answers range from organizational culture, which we see in Europe as well, to lack of awareness at higher management levels, something that European organizations have nearly not mentioned.

Nearly all participants notice the “weakest link” principle and believe that more collaboration with their European counter parts should take place in an effort to make the chain as secure as possible. This is also seen as the biggest gap in the implementation of standards, without cooperation, the implementation of standards is of no use.

Looking at the Dutch sector in reference to their European counter parts, we can state that the Netherlands is in the middle of the ranking. They are, in typical Dutch fashion, sober and pragmatic about the process and expectations. They are definitely not standing out, and are conservative with investing capital in cyber security. This is probably the main difference. It might be that the major outage in 2006 (UCTE, 2007), which did not hit the Netherlands, has brought awareness to key players in the organizations that were hit. European colleagues seem to have less trouble finding capital for cyber security than Dutch organizations.

6 THE SGS SECURITY BENCHMARK

The main deliverable of this project is the benchmark tool, which we dubbed the SGS Security Benchmark (or Smart Grid Substation Security Benchmark). In this section, we describe the process and choices we made while developing the SGS Security Benchmark. We first describe the focus areas and the associated capabilities per focus area. Then, we place each capability on a certain level of maturity within the SGS Security Benchmark.

6.1 Defining focus areas and capabilities

After analyzing the literature and relevant standards, principles and topics relevant to the cyber security of smart grids are extracted. This resulted in a list of more than 400 requirements regarding smart grid security. Since some requirements are related to others (e.g. designing architecture and implementing that architecture not only discuss the same topic but show hierarchy as well), we began clustering the requirements into coherent groups of requirements. The result is a list of 15 initial clusters or focus areas, which contain multiple capabilities.

These focus areas, with their capabilities, are evaluated in the first round of the interviews. The results of these interviews transformed our capability list; some capabilities merged, some were removed, and some were added. This transformed list of capabilities is then re-evaluated during another round of interviews. This led to minor changes, primarily based on consistency.

Finally, the list comprises 68 capabilities divided over 14 focus areas. In the next sections, these are described, including a rationalization for each group. Appendix C provides an overview of all capabilities along with a description and their source.

6.1.1 Governance, risk and compliance

Governance, Risk and Compliance is an emerging topic regarding three closely related topics within organizations. It is "a continuous process that is embedded into the culture of an organization and governs how management identifies and protects against relevant risks, monitors and evaluates the effectiveness of internal controls, and responds and improves operations based on learned insights" (KPMG, 2008). As risks, internal controls and response to insights are an intrinsic part of cyber security, this cluster is one of the largest in the matrix. The group consists of six focus areas with three to five capabilities, presented in Table C.

Responsibility and accountability	
A.	Document allocation of information security responsibilities
B.	Implement authorization
C.	Periodically review responsibilities and accountability of personnel
D.	Termination of responsibilities and access in case of termination of employment

Risk and security assessment	
A.	Implement and execute risk and security assessment regarding sub stations and other smart grid components
B.	Develop risk and security assessment plan and document results
C.	Implement risk security assessment policies and procedures
D.	Respond to risk and security assessment outcomes

Policy	
A.	Implement and maintain policies regarding the cyber security of sub stations and other smart grid components
B.	Ensure that third parties are compliant with the cyber security policies
C.	Define clear communications protocols and infrastructure that is required for protocols to operate.

Monitor user activity	
A.	Monitoring of access to the systems included in the smart grid is implemented
B.	Continuously supervise the quality of access logs
C.	Protect log information to prevent unauthorized access
D.	Perform audit on the monitoring of the logs
E.	Respond to audit outcomes

Standardization	
A.	Implement standards regarding the cyber security of the smart grid
B.	Adhere to established international standards on smart grid cyber security
C.	Perform audits on the standards to which the smart grid adheres
D.	Responds to audit outcomes

Incident management	
A.	Report information security incidents
B.	Identify and analyze cause of incidents
C.	Respond to incidents based on the analysis of the incidents
D.	Implement incident response training
E.	Manage security incidents and improve based on them (learn from incidents)

Table C: Capabilities of the focus area Governance, Risk and Compliance

6.1.2 Security architecture

The second group describes an architecture perspective on cyber security. Smart grids are essentially complex networks, and the architecture of these networks is important. A well-documented and implemented architecture promotes consistency. Many topics discussed in the literature assumed an architecture of sorts. This cluster adheres to that assumption. Additionally, all interviewees agreed on this cluster. Its focus areas and their capabilities are presented in Table D.

Hardware architecture	
A.	Design and document a basic hardware architecture, showing all the components in the smart grid
B.	Implement the designed hardware architecture
C.	Redesign the architecture so that it is secure by design
D.	Perform hardware architecture audits
E.	Ensure that the architecture adheres to international standards
F.	Respond to audit outcomes

Software architecture	
A.	Design and document a basic software architecture for the (smart) devices in sub stations and other smart grid components
B.	Implement the designed software architecture
C.	Redesign the architecture so that it is secure by design
D.	Perform software architecture audits
E.	Ensure that the architecture adheres to international standards
F.	Respond to audit outcomes

Data architecture	
A.	Design and document a basic data architecture structure, showing all the sources and receivers of data in the smart grid
B.	Define data requirements, stating details about integrity, consistency, reliability, standardization of data formats, etc.
C.	Implement the designed data architecture
D.	Ensure that control mechanisms are in place to protect the data from abuse or malpractice
E.	Perform data audits
F.	Respond to audit outcomes

Back-up	
A.	Design and document a back-up strategy for all the data transmitted within the smart grid
B.	Enable local back-ups of the data transported to and from substations
C.	Enable remote back-ups of the data transported to and from substations from within utility networks
D.	Perform audits on the back-up mechanisms
E.	Respond to audit outcomes

Continuity	
A.	Implement a continuity strategy for all systems including in the smart grid (including keeping spare parts for high risk hardware, etc.)
B.	Monitor the continuity strategy

C.	Respond to continuity incidents, such as power outages, network failures, etc.
D.	Perform continuity implementation audit
E.	Respond to audit outcomes

Connectivity and networking	
A.	Provide secure network access to the substations in transmission and distribution networks
B.	Document the network architecture, including all the hardware and software components and their interdependencies, the access rights to the network, etc.)
C.	Implement network policy regarding access and authorization to the information networks in the smart grid
D.	Perform audit on network components to ensure everything is up and running correctly
E.	Respond to audit outcomes

Table D: Capabilities of the focus area Security architecture

6.1.3 Security implementation

Employees have to be aware of the fact that cyber security is an increasingly important topic within smart grids. Only then can there be enough support and consensus among employees and management. Awareness is often mentioned in the interviews and in the literature as an issue and one of the hardest yet most important aspects of cyber security. We therefore chose to make awareness a separate cluster within our SGS Security Benchmark. This way we hope to highlight the importance of this group. Its focus areas and capabilities are presented in Table E.

Training and education	
A.	Develop training policies and procedures
B.	Train users of smart grid components (such as system engineers, technical engineers, auditors, etc.)
C.	Improve the quality of personnel through certification
D.	Keep personnel updated with recent developments

Testing	
A.	Implement test procedures to test the software and hardware components and networks included in the smart grid
B.	Adhere to test procedures
C.	Have test procedures integrated into the system architecture
D.	Act according to test results
E.	Perform audit on test procedures
F.	Respond to audit outcomes

Table E: Capabilities of the focus area Security implementation

6.2 Creating the maturity matrix

After defining the clusters, focus areas and capabilities, the capabilities were individually placed on the matrix. Previous research shows that ten to twelve maturity levels are most appropriate (Bekkers & Brinkkemper, 2010) which coincided with our initial results of placement. This placement is based on dependency of one capability to another, and the relative difference in difficulty of implementation.

The placement of the individual capabilities has been evaluated internally by each respective team member in an iterative manner. The first iteration was done by one team member, the second iteration consisted of a second team member commenting and editing the SGS Security Benchmark, and so forth. Each team member discussed the changes and/or comments and the matrix was changed appropriately. The result is a first version of the SGS Security Benchmark. During the second round of interviews, interviewees received the SGS Security Benchmark beforehand to revise it and discuss their revisions during the interview. This semi-structured interview led to a wealth of information. The different perspectives between the interviewees, which among others includes the positions of capabilities on the matrix and their relative distances to one another, was processed in the final version of the SGS Security Benchmark.

The final SGS Security Benchmark, based on literature and 13 expert interviews, is depicted in Figure 6.1.

Focus area	0	1	2	3	4	5	6	7	8	9	10	11	12
Governance Risk Compliance													
Responsibility and accountability		A		B		C			D				
Risk and security assessment			A		B					C		D	
Policy			A				B		C				
Monitoring		A		B		C			D			E	
Standardization			A			B				C		D	
Incident management		A			B		C			D			E
Security architecture													
Hardware architecture		A		B		C			D	E			F
Software architecture		A			B		C		D	E			F
Data architecture		A		B				C		D	E		F
Back-up			A		B		C		D			E	
Continuity				A		B		C			D		E
Connectivity and networking			A			B		C			D		E
Security implementation													
Training and education			A	B			C			D			
Testing			A	B			C	D			E		F

Figure 6.1: The final SGS Security Benchmark tool

7 CONCLUSION

This report describes the state of the art of smart grid security in Europe and the Netherlands. Special attention is paid to the perception of risks and threats in smart grid security and the international standards developed to mitigate these risks and threats. The resulting overview of the current state of smart grid security is based on semi-structured interviews with 13 participants originating from eight different European countries. All participants have an expertise related to the security of smart grids. Additionally, a SGS Security Benchmark tool is created that can be used by organizations to benchmark the level of cyber security in the smart grid and to develop a plan to incrementally improve their cyber security practices.

7.1 The state of smart grid security

7.1.1 Smart Grid security

All participants indicated that security is a high priority within their organization. However, the organizations are not in the same stage regarding security implementation: some organizations fully implemented cyber security standards such as the NERC version 3 and de ISO27000 series, while others are reevaluating their efforts.

The biggest risk indicated is the interconnectivity of the smart grid with multiple stakeholders and European colleagues. The cyber security of a smart grid is as strong as the cyber security of its weakest link. This can be a smart meter placed at a consumer, a device controlling electricity distribution in a substation, or a monitoring system at the utility organization. Another major risk is the low level of awareness at the lower personnel levels. In a sector where information security has played no major role for decades, the cultural transition to a security minded attitude will be a huge task.

All experts indicated that more effort should be put into the cyber security of smart grids. There is however no consensus where these additional efforts should be allocated to.

The following initiatives were mentioned:

- Better international relations and cooperation
- Higer levels of awareness
- Education of personnel
- International policy in communication protocols
- European-wide mandatory standards

The comparison of the results of the semi-structured interviews showed that there are major differences between European countries regarding the cyber security of smart grids. For example, one

country has enough cyber security related capabilities implemented to safely accommodate a smart grid while the cyber security of electric grids in another country is still in its infancy.

7.1.2 Implemented standards

The majority of experts made it clear that the more abstract international standards, such as those from the ISO and IEC, are favored over those from the North American continent.

The ISO27000 series is by far the most prevalent standard to be implemented by the organizations. However, the degree to what the standard is implemented varies greatly. Half of the organizations participating have finished their ISO27000 implementation. The other half varies from starting their compliancy process to being nearly done. Those who implement the standard partially mention that parts are not applicable to them or have been implemented in other forms but are not completely conforming to the standard.

The experts indicated the culture within an organization as the greatest pitfall regarding security implementation. This implementation requires changes in behavior of personnel and workflows. However, the organization is often reluctant in accepting these changes. Key is that higher management is fully aware and supports all efforts.

Besides the ISO27000 series the IEC 68150 and 60870 are also implemented within organizations. However, most organizations are waiting to see which standard becomes de facto. Besides that, the experts also believe that in upcoming review sessions, the standards will mature, for which they are waiting.

7.1.3 The Netherlands

Compared to other European nations, the Dutch utility sector scores an average when it comes to the cyber security of the electric grid. The Dutch experts acknowledge that cyber security is needed but indicate that the awareness within top management is not high enough. As a result, budgets for the implementation of cyber security capabilities are low and hence, only small steps for improvement can be made.

The experts state that the Dutch electric grid is far from being a smart grid. Therefore, the participants believe that the current pace of implementation is correct. There is ample time to implement the needed measures before the smart grid really takes effect in the Netherlands. They also indicate that at this moment the network is not smart grid ready in terms of security.

The Dutch sector, like the European, is currently implementing the ISO27000 standard. All of them have started and are well on their way. However, none of the Dutch organizations interviewed are implementing the full standard. They mention that the ISO27000 standard does not fit with the

organization and that it is difficult to have all the competencies available that are required by the standard. A few organizations are investigating other IEC standards, but have not yet started the implementation process. They mention the same issues as the Europeans: lack of maturity, lack of hardware support and the lack of a stance by European colleagues or the European Union.

7.2 The SGS Security Benchmark

The SGS Security Benchmark is developed based on several international standards and on two rounds of semi-structured interviews with experts in the field of smart grids and cyber security. The maturity matrix consists of 68 capabilities divided over 14 focus areas.

The SGS Security Benchmark can be used by utility organizations to benchmark their level of cyber security within the smart grid. An organization can create a maturity profile by stating which of the 68 capabilities are implemented. Based on the results of the benchmark the organization can identify areas of improvement and can help create a plan to incrementally improve its cyber security practices, thereby reaching a higher maturity level. The maturity matrix is depicted in Figure 6.1 and the capabilities are discussed in "Appendix C: Capability list".

The actual application and implementation of the maturity matrix within an organization is beyond the scope of this report. Further research has to be conducted to validate the maturity matrix and to measure the applicability in a real life setting and in terms of incremental process improvement.

Furthermore, as a benchmark needs multiple implementations in order to provide a baseline (an overview of the current state), an organization should save all benchmark results. The to-be executed benchmark can then be compared to the records of previous benchmark executions. Only then a benchmark, as in a comparison to other organizations in the smart grid field, can be successfully executed and prove its usefulness.

7.3 Outlook

It can be concluded that utility organizations still have a lot to improve with regard to the cyber security of the smart grid. Efforts are undertaken to prevent security threats and tackle risks, but nearly none have been finalized. This implies that there is still a long way to go before the smart grid is fully secured. The developed SGS Security Benchmark tool can act as a stepping stone in achieving a more secure organization.

REFERENCES

Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid. IEEE Power and Energy Magazine, 3(5), 34-41. doi: 10.1109/MPAE.2005.1507024

Bekkers, W., Weerd, I. van de, Spruit, M., & Brinkkemper, S. (2010). A framework for process improvement in software product management. In: A. Riel, R. O'Connor, S. Tichkiewitch & R. Messnarz (Eds.), Systems, Software and Services Process Improvement (pp. 1-12). Berlin Heidelberg: Springer-Verlag. doi: 10.1007/978-3-642-15666-3_1

Blaabjerg, F., Chen, Z., & Kjaer, S. (2004). Power electronics as efficient interface in dispersed power generation systems. IEEE Transactions on Power Electronics, 19(5), 1184-1194.

Bruin, T. de, Rosemann, M., Freeze, R., & Kulkari, U. (2005). Understanding the main phases of developing a maturity assessment model. Proceedings of the 16th Australasian Conference on Information Systems, Sydney, Australia.

Clements, S., & Kirkham, H. (2010). Cyber-Security Considerations for the Smart Grid. Proceedings of the IEEE Power and Energy Society General Meeting 2010, Minneapolis, MN, pp. 1-5. doi: 10.1109/PES.2010.5589829

Fan, Z., Kalogridis, G., Efthymiou, C., Sooriyabandara, M., Serizawa, M., McGeehan, J. (2010). The New Frontier of Communications Research: Smart Grid and Smart Metering. Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking, Passau, Germany, 115-118. doi: 10.1145/1791314.1791331

Faruqui, A., Harris, D., & Hledik, R. (2010). Unlocking the €53 billion savings from smart meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment. Energy Policy, 38(10), 6222-6231. doi: 10.1016/j.enpol.2010.06.010

Howard, M. & LeBlanc, D. (2002). Writing Secure Code. Washington: Microsoft Press

International Instrument Users' Association. (2010). Process control domain. Security requirements for vendors (M 2784-X-10). Retrieved from http://blog.industrialdefender.com/downloads/wib-m-2784-x10-v1.0-pcs-requirements-for-vendors.pdf

International Organization for Standardization. (2008). Information technology. Security techniques. Code of practice for information security management (ISO/IEC 27002:2005). Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=50297

Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. IEEE Security & Privacy, 8(1), 81-85. doi: 10.1109/MSP.2010.49

King R.P., Halim, N., Garcia-Molina, H. & Polyzois, C. A. (1991), Management of a Remote Backup Copy for Disaster Recovery, ACM Transactions on Database Systems, 16(2), pp.338-368.

KPMG (2008). Governance, Risk, and Compliance: Driving Value through Controls Monitoring. Retrieved from http://www.kpmg.com/Ca/en/IssuesAndInsights/ArticlesPublications/Documents/GovernanceRiskCompliance.pdf

Kuilboer, J. P., & Ashrafi, N. (2000). Software process and product improvement: an empirical assessment. Information and Software Technology, 42(1), 27-34. doi: 10.1016/S09505849(99)00054-3

Lee, A., & Brewer, T. (2009). Smart Grid Cyber Security Strategy and Requirements. NISTIR 7628, NIST, September 2009

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2009). Developing maturity grids for assessing organisational capabilities: Practitioner guidance. In: 4th International Conference on Management Consulting, Academy of Management (MCD 2009), Vienna, Austria.

NIST (2010). NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST Special Publication 1108). Retrieved from http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

Racz, N., Weippl, E., & Seufert, A. (2010): A frame of reference for research of integrated Governance, Risk & Compliance (GRC). Proceedings of the 11th IFIP TC 6/TC 11 International Conference, pp. 106-117.

Rodriguez, P., Timbus, A. V., Teodorescu, R., Liserre, M., & Blaabjerg, F. (2007). Flexible active power control of distributed power generation systems during grid faults. IEEE Transactions on Industrial Electronics, 54(5), 2583-2592. doi: 10.1109/TIE.2007.899914

SG2030 Smart Grid Portfolios. (2010). Retrieved August 24, 2012 from http://www.smartgrid2030.com/?page_id=445

Steenbergen, M. van, Berg, M. van den, & Brinkkemper, S. (2007). An Instrument for the development of the enterprise architecture practice. In: J. Cardoso, J. Cordeiro, & J. Filipe (Eds.) ICEIS 2007 - Proceedings of the 9th International Conference on Enterprise Information Systems, Funchal, Portugal. pp. 14-22.

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). The design of focus area maturity models. In: R. Winter, J. L. Zhao, & S. Aier (Eds.) DESRIST 2010 – LNCS 6105, pp. 317-332.

Steenbergen, M. van, Schipper, J., Bos, R., & Brinkkemper, S. (2009). The dynamic architecture aturity matrix: Instrument analysis and refinement. In: A. Dan, F. Gittler, & F. Toumani (Eds.) ICSOC/ServiceWave 2009, LNCS 6275, pp. 48-61.

UCTE (2007). Final Report System Disturbance on 4 November 2006. Retrieved from: https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf

Vries, B. J. M. de, Vuuren, D. P. van, Hoogwijk, M. M. (2006). Renewable energy sources: Their global potential for the first-half of the 21st century at a global level: An integrated approach. Energy Policy, 35(4), 2590–2610. doi: 10.1016/j.enpol.2006.09.002

Weerd, I. van de, Bekkers, W., & Brinkkemper, S. (2010). Developing a maturity matrix for software product management. Lecture Notes in Business Information Processing, 51, pp. 76-89.

USED STANDARDS

The following standards are investigated to create a body of knowledge and to construct the SGS Benchmark tool:

- ISO 27002 - http://www.27000.org/iso-27002.htm
- WIB 2784-X10 - http://osgug.ucaiug.org/conformity/security/Shared%20Documents/Forms/AllItems.aspx
- IEC 60870 - http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/17445?OpenDocument
- IEC 61850 - http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/33549?OpenDocument
- IEC 62351 - http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/45742?OpenDocument
- IEEE 2030 - http://grouper.ieee.org/groups/scc21/2030/2030_index.html
- NIST SP800- 53R4 - http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
- NIST SP800-30 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST 7328 - http://csrc.nist.gov/publications/drafts/nistir-7328/NISTIR_7328-ipdraft.pdf
- NIST 7628 - http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf
- NERC 1200 - http://www.nerc.com/files/Urgent_Action_Standard_1200_Cyber_Security.pdf
- NERC 1300 - http://www.nerc.com/docs/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf
- NERC Security Guidelines - http://www.nerc.com/files/Continuity-of-Operations.pdf

APPENDIX A: INTERVIEW PROTOCOL

Protocol first round of interviews

This round explores the perspectives of the interviewee on smart grids and its security in a semi-structured interview. In addition, it addresses standards within the interviewee's organization and introduces the SGS Security Benchmark for the first time by means of the capability list. The capability list, distilled from the literature, was send on forehand as well as a list of topics that was to-be discussed.

Interviewee

- Name
- Function
- Employer/Unit
- Standard committees (member/influencer; specific role)
- Expertise

What are smart grids?

Cyber security

- What is cyber security according to you? [our definition]
- What is your perspective on cyber security?
- How does this apply to Smart grids?

- How is cyber security applied right now?
- What are noticeable security trends in this area?
- What is the main current threat?
- How does (organization) contribute to improvements in current and future cyber security?
- Do you feel more should be done?

Standards

- Which standards regarding substations are applied and why?
- Entirely or partially?
- What parts are often left out?
- What are common difficulties when applying these standards?
- do these standards cover enough to prevent risks?
- are you investigating other/future standards?
- do you recognise discrepancies between the standards, different perspectives?

- How do you perceive cyber security risks at substations at this moment? [worried?]
- Has this led to an active search for applying new (better) standards?
- Has there been a shift between physical and cyber security?

Model

- Is the model understandable?
- Is the purpose/goal clear?
- What would you change in this model?
- Do the main security functions (groups) in the model seem appropriate?
- With this structure, could any classification issues arise later on?
- Do you question particular focus areas?
- Because in your opinion they are sufficiently irrelevant for this model?
- Because you deem them to be significantly more important than others?
- Is anything missing in your opinion?

Closing

- Any additional comments to the topics we've spoken about?
- Any other remarks?
- Thanks you for your time. Would you already want to plan the evaluation?

Protocol second round of interviews

The second round of interviews discussed the model only. The complete SGS Security Benchmark was send in front of the interview, including a revised capability list. The focus was to re-evaluate the capability list, and to evaluate the location of these capabilities on the matrix.

- We changed the capabilities. Any remarks?

In the literature, there have been capabilities stating software systems such as antivirus, firewalls, Intrusion/extrusion detection systems, Malware, DOS protection, and so forth. How do you believe these should be implemented in the matrix?

- Did you understand the matrix, could you comprehend how it should be used?

So, what we'll do is move through the matrix, and as mentioned in the email, we will discuss block by block, depicted by the colors (show the blocks by selecting them) and discuss the following:

Per block:

- Are the maturity levels correctly estimated?
- Are the dependencies between one another correctly set?

APPENDIX B: MATRIX DEVELOPMENT

This appendix provides more detail about the process during which the maturity matrix for smart grid cyber security was developed. As stated in the research approach, we followed the method by Steenbergen et al. (2010). The method (depicted in Figure 2.2) follows ten steps:

1. *Identify and scope the functional domain*. In the case of this research project, the functional domain is cyber security of smart grids. The scope is laid down to the international standards concerning the information technology used in smart grids (and in electric substations in particular) and the security issues arising from implementing an increasing number of smart devices in the smart grid.
2. *Identify the focus areas that are relevant within the chosen domain*. Focus areas are basically coherent groups of predefined goals (also called capabilities) that need to be achieved in order to reach the maturity levels with which they are associated (Bekkers, Weerd, Spruit, & Brinkkemper, 2010). In order for the maturity matrix to be effective in its use, the number of focus areas should be approximately twenty (Maier, Moultrie, & Clarkson, 2009). According to Steenbergen et al. (2010), grouping the focus areas into categories can improve the accessibility of the model. Within this research project, the focus areas are derived from all the requirements found in the various international standards, as can be read in Chapter 4.
3. *Define the capabilities that make up each focus area*. The definition of the capabilities in this research project is based on the review of the international standards, as described in chapter 4. Once we had an average of four to five capabilities per focus area, we determined the evolutionary path of each focus area, meaning that we ordered the capabilities from very basic to more advance. This enables each focus area to be implemented incrementally. The resulting list of capabilities was then evaluated through expert interviews.
4. *Determine the dependencies between the capabilities*. As noted by Steenbergen et al. (2010), this not only concerns dependencies between the capabilities within the same focus area, but also the dependencies between capabilities of different focus areas. In the first concept version of the maturity matrix, we based the dependencies on our own knowledge and judgment.
5. *Position the capabilities in the maturity matrix*. In this step it is important to take the dependencies defined in the previous step into account, because capabilities that require one or more other capabilities to be implemented first, should be placed further to the right. In this research project, we positioned the capabilities in the first concept version of the maturity matrix based on the dependencies defined in the previous step, and on our own knowledge and judgment. The position of the capabilities was evaluated through expert interviews, which led to refinement of the maturity matrix and the positions of the capabilities.
6. *Develop an assessment instrument that can be used to assess the current maturity of a functional domain within an organization*. This is usually done by defining a number of questions for each capability (e.g. the questionnaire associated with the Software Product Management Maturity

Matrix employs 68 questions; the questionnaire associated with the Dynamic Architecture Maturity Matrix includes 137 questions). By answering these questions through interviews with relevant stakeholders, organizations can assess the maturity of their processes. Although questions can be derived from the descriptions of the capabilities included in the maturity matrix proposed in this research, developing a questionnaire (and evaluating it through expert interviews) is left out of scope of this research due to time constraints. Future research should hence strive to achieve a complete and comprehensive questionnaire with which utilities can assess the cyber security of the various smart devices in their electric grids.

The next steps described by the model are not addressed in this research, as these steps are typically performed after a maturity matrix is employed to assess the maturity of a certain functional domain. For example, the seventh step is to define actions for improvement based on the initial assessment of the current maturity of an organization. The actions for improvement, when implemented, should lead the organization to a higher level of maturity. The eighth step is to reflect on how well the maturity matrix and its associated questionnaire performed during the assessment, and to improve the maturity matrix and the questionnaire according to the feedback gained in this step. The final step is to describe these results to the benefit of the scientific community. However, these steps are beyond the scope of this research.

APPENDIX C: CAPABILITY LIST

Governance Risk Compliance

Responsibility and accountability

Capability	**A**
Title	Document allocation of information security responsibilities
Description	The allocation of roles and its responsibilities are documented.
Prerequisite(s)	-
Reference	ISO 27000; NERC 1300;

Capability	**B**
Title	Implement authorization
Description	Access rights to resources are specified and used.
Prerequisite(s)	Responsibility and accountability A
Reference	ISO 27000; IEEE 2030; NERC SG, p2; NERC 1300

Capability	**C**
Title	Periodically review responsibilities and accountability of personnel
Description	The responsibilities of personnel are constantly reviewed in order to determine if this information is current.
Prerequisite(s)	Responsibility and accountability B
Reference	[Expert interview]

Capability	**D**
Title	Termination of responsibilities and access in case of termination of employment
Description	As soon as an employee leaves the organization his/her responsibilities and access should be terminated.
Prerequisite(s)	Responsibility and accountability B
Reference	ISO 27000, p.27

Risk and security assessment

Capability	**A**
Title	Implement and execute risk and security assessment regarding sub stations and other smart grid components
Description	An assessment is implemented and conducted in order to identify risks and flaws in security.
Prerequisite(s)	-
Reference	ISO 27000, p.IX; WIB 2784-X10, p.32; NIST SP800-30, p.36; NIST SP800-53R4, p.92; IEEE 2030, p.13; NISTIR 7628, p.6; NISTIR 7328, p.19

Capability	**B**
Title	Develop risk and security assessment plan and document results
Description	A plan is developed which describes how and when the risk/security assessment should be conducted. The results of the assessment are documented.
Prerequisite(s)	Risk / security assessment A
Reference	NISTIR 7328, p.17;

Capability	**C**
Title	Implement risk security assessment policies and procedures
Description	Policies and procedures are developed and implemented.
Prerequisite(s)	Risk / security assessment A
Reference	NIST SP800-53R4, p.89; NISTIR 7328, p.16

Capability	**D**
Title	Respond to risk / security assessment outcomes
Description	An organization should act based on the results of the Risk/security assessment.
Prerequisite(s)	Risk / security assessment A
Reference	-

Policy

Capability	**A**
Title	Implement and maintain policies regarding the cyber security of sub stations and other smart grid components
Description	The organization implements and maintains a policy describing how and when a system is secure.
Prerequisite(s)	-
Reference	ISO 27000, p.7; IEEE 2030, p.31; NERC 1200; NERC 1300; NISTIR 7268, p.3

Capability	**B**
Title	Ensure that third parties are compliant with the cyber security policies
Description	Third parties, e.g. subcontractors or consultants, acknowledge and comply with security policies enforced by the organization.
Prerequisite(s)	Policy A
Reference	WIB 2784-X10, p.18

Capability	**C**
Title	Define clear communications protocols and infrastructure that is required for protocols to operate.
Description	To ensure interoperability and cooperation between components in the smart grid, clear communication protocols should be defined
Prerequisite(s)	Policy A
Reference	IEEE 2030, p.8

Monitor user activity

Capability	**A**
Title	Monitoring of access to the systems included in the smart grid is implemented
Description	The access to the system is monitored continuously and data on who access which (part of the) system is stored in log files.
Prerequisite(s)	-
Reference	ISO 27000, p.56; NERC 1200; IEC 61850, p.13; NERC SG, p.2; WIB 2784-X10, p.27; NIST SP800-53R4, p.89

Capability	B
Title	Continuously supervise the quality of access logs
Description	The log files are continuously checked to decide whether they provide correct and complete information.
Prerequisite(s)	Monitor user activity A
Reference	ISO 27000, p.56; NERC 1200; IEC 61850, p.13; NERC SG, p.2; WIB 2784-X10, p.27; NIST SP800-53R4, p.89

Capability	C
Title	Protect log information to prevent unauthorized access
Description	The logs are protected to ensure that only authorized personnel can access the log files.
Prerequisite(s)	-
Reference	ISO 27000, p.56; NERC 1200; IEC 61850, p.13; NERC SG, p.2; WIB 2784-X10, p.27; NIST SP800-53R4, p.89

Capability	D
Title	Perform audit on the monitoring of the logs
Description	An audit is conducted in order to decide whether the monitoring of logs is performed correctly.
Prerequisite(s)	Monitor user activity A
Reference	ISO 27000, p. 55; WIB 2784-X10, p.18; NIST SP800-53R4, p.89

Capability	E
Title	Respond to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Monitor user activity D
Reference	NIST SP800-53R4, p.89

Standardization

Capability	**A**
Title	Implement standards regarding the cyber security of the smart grid
Description	The organization should implement smart grid standards that deal with cyber security matters. The choice of standard depends on the characteristics of the organization and the location in which the organization is situated.
Prerequisite(s)	-
Reference	-

Capability	**B**
Title	Adhere to established international standards on smart grid cyber security
Description	The organization implements and adheres to international smart grid standards
Prerequisite(s)	Standardization A
Reference	ISO 27000, p.104

Capability	**C**
Title	Perform audits on the standards to which the smart grid adheres
Description	An audit is conducted to measure to what extent an organization adheres to smart grids standards
Prerequisite(s)	Standardization A
Reference	NIST SP800-53R4, p.89

Capability	**D**
Title	Responds to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Standardization B
Reference	NIST SP800-53R4, p.89

Incident management

Capability	**A**
Title	Report information security incidents
Description	Information security incidents are reported as soon as they occur.
Prerequisite(s)	-
Reference	ISO 27002-2007, p.90

Capability	**B**
Title	Identify and analyze cause of incidents
Description	For each incident data is gathered to determine the cause of the incident.
Prerequisite(s)	Incident management A
Reference	ISO 27002-2007, p.93

Capability	**C**
Title	Respond to incidents based on the analysis of the incidents
Description	A workforce is implemented which main task is to resolve occurring incidents.
Prerequisite(s)	Incident management B
Reference	WIB 2784-X10, p.18

Capability	**D**
Title	Implement incident response training
Description	Training is provided for employees to learn them how to act when incidents occur.
Prerequisite(s)	-
Reference	NIST SP800-53R4, p.90

Capability	E
Title	Manage security incidents and improve based on them (learn from incidents)
Description	Information security incidents are management. The organization improves its process based on incidents.
Prerequisite(s)	-
Reference	ISO 27002-2007, p.93; NISTIR 7628, p.6; NERC 1200; NIST SP800-53R4, p.90

Security Architecture

Hardware architecture

Capability	A
Title	Design and document a basic hardware architecture, showing all the components in the smart grid
Description	A design of the hardware architecture is created and documented. This architecture incorporates all the components present within the smart grid.
Prerequisite(s)	-
Reference	WIB 2784-X10, p.39

Capability	B
Title	Implement the designed hardware architecture
Description	The designed architecture is implemented within the organization.
Prerequisite(s)	Hardware architecture A
Reference	-

Capability	C
Title	Redesign the architecture so that it is secure by design
Description	The architecture is redesigned to make it secure. Hereby, the impact of security vulnerabilities is minimized.
Prerequisite(s)	Hardware architecture B
Reference	(Howard & LeBlanc, 2002)

Capability	D
Title	Perform hardware architecture audits
Description	Audits are conducted to decide whether the hardware architecture is fully implemented and secure.
Prerequisite(s)	Hardware architecture C
Reference	NIST SP800-53R4, p.89

Capability	E
Title	Ensure that the architecture adheres to international standards
Description	The hardware architecture is checked to decide whether it adheres to international standards regarding the cyber security of smart grids.
Prerequisite(s)	Hardware architecture C
Reference	-

Capability	F
Title	Respond to audit outcomes
Description	The organization acts based on the results of the audit. This entails the adjustment of the hardware architecture so it fulfills security requirements, or it adheres to international standards.
Prerequisite(s)	Hardware architecture C
Reference	NIST SP800-53R4, p.89

Software architecture

Capability	A
Title	Design and document a basic software architecture for the (smart) devices in sub stations and other smart grid components
Description	Software architecture is documented for all software present in sub stations and its devices.
Prerequisite(s)	-
Reference	WIB 2784-X10, p.39

Capability	B
Title	Implement the designed software architecture
Description	The designed architecture is implemented within the organization.
Prerequisite(s)	Software architecture A
Reference	WIB 2784-X10, p.38

Capability	C
Title	Redesign the architecture so that it is secure by design
Description	The architecture is redesigned to make it secure. Hereby, the impact of security vulnerabilities is minimized.
Prerequisite(s)	Software architecture B
Reference	(Howard & LeBlanc, 2002)

Capability	D
Title	Perform software architecture audits
Description	Audits are conducted to decide whether the software architecture is fully implemented and secure.
Prerequisite(s)	Software architecture C
Reference	NIST SP800-53R4, p.89

Capability	E
Title	Ensure that the architecture adheres to international standards
Description	The software architecture is checked to decide whether it adheres to international standards regarding the cyber security of smart grids.
Prerequisite(s)	Software architecture C
Reference	IEEE 2030, p7

Capability	F
Title	Respond to audit outcomes
Description	The organization acts based on the results of the audit. This entails the adjustment of the software architecture so it fulfills security requirements, or it adheres to international standards.
Prerequisite(s)	Software architecture C
Reference	NIST SP800-53R4, p.89

Data architecture

Capability	A
Title	Design and document a basic data architecture structure, showing all the sources and receivers of data in the smart grid
Description	Data architecture documentation depicting all data sources.
Prerequisite(s)	-
Reference	WIB 2784-X10, p.39

Capability	B
Title	Define data requirements, stating details about integrity, consistency, reliability, standardization of data formats, etc.
Description	The designed architecture is implemented within the organization.
Prerequisite(s)	Data architecture A
Reference	IEC 60870-5-1, p.17

Capability	C
Title	Implement the designed data architecture.
Description	The documented data architecture and requirements are implemented.
Prerequisite(s)	Data architecture A
Reference	WIB 2784-X10, p.38

Capability	D
Title	Ensure that control mechanisms are in place to protect the data from abuse or malpractice
Description	Implement personnel security controls, including personnel clearance.
Prerequisite(s)	Data architecture B
Reference	NIST SP800-30, p.36

Capability	E
Title	Perform data audits
Description	A data audit is performed to assess the quality or the data and if it is correct for its designated purpose.
Prerequisite(s)	Data architecture A
Reference	NIST SP800-53R4, p.89

Capability	F
Title	Respond to audit outcomes
Description	Actions are taken based on the results of the data audit, e.g. processing failures
Prerequisite(s)	Data architecture E
Reference	NIST SP800-53R4, p.89

Back-up

Capability	A
Title	Design and document a back-up strategy for all the data transmitted within the smart grid
Description	A back-up strategy is designed and documented which describes how back-ups are conducted, what type of back-up is conducted, and with what frequency.
Prerequisite(s)	-
Reference	WIB 2784-X10, p.26

Capability	B
Title	Enable local back-ups of the data transported to and from substations
Description	Local back-ups are created containing data that is transported to and from the substation.
Prerequisite(s)	Back-up A
Reference	NIST SP800-30, p.37

Capability	C
Title	Enable remote back-ups of the data transported to and from substations from within utility networks
Description	Next to local back-ups, remote back-ups are in place to ensure that data is retained even after local back-ups are lost, e.g. due to physical damage to the substation.
Prerequisite(s)	Back-up B
Reference	(King, Halim, Garcia-Molina & Polyzois, 1991)

Capability	D
Title	Perform audits on the back-up mechanisms
Description	Audits are conducted to check whether the back-up mechanisms are functioning as expected.
Prerequisite(s)	Back-up B
Reference	WIB 2784-X10, p.26

Capability	E
Title	Respond to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Back-up D
Reference	WIB 2784-X10, p.26

Continuity

Capability	A
Title	Implement a continuity strategy for all systems including in the smart grid (including keeping spare parts for high risk hardware, etc.)
Description	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
Prerequisite(s)	-
Reference	ISO 27002-2007, p.96

Capability	B
Title	Monitor the continuity strategy
Description	The continuity strategy is monitored, tested and maintained to ensure that it is up to date and effective.
Prerequisite(s)	Continuity A
Reference	ISO 27002-2007, p.98

Capability	C
Title	Respond to continuity incidents, such as power outages, network failures, etc.
Description	When a continuity incident occurs, measures have to be taken according to the implemented strategy to ensure that all components remain operational.
Prerequisite(s)	Continuity A
Reference	ISO 27002-2007, p.97

Capability	D
Title	Perform continuity implementation audit
Description	An audit is conducted to check whether the continuity strategy is performed correctly and delivers the desired result.
Prerequisite(s)	Continuity C
Reference	NIST SP800-53R4, p.89

Capability	E
Title	Respond to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Continuity D
Reference	NIST SP800-53R4, p.89

Connectivity and networking

Capability	**A**
Title	Provide secure network access to the substations in transmission and distribution networks
Description	Secured network access is in place for substations devices with authentication for users. Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
Prerequisite(s)	-
Reference	NERC 1200, p.6, ISO 27002-2007, p.45

Capability	**B**
Title	Document the network architecture, including all the hardware and software components and their interdependencies, the access rights to the network, etc.)
Description	The network architecture is designed and documented, showing the interdependencies of all network components.
Prerequisite(s)	-
Reference	WIB 2784-X10, p.39

Capability	**C**
Title	Implement network policy regarding access and authorization to the information networks in the smart grid
Description	An access control policy should be established, documented, and reviewed based on business and security requirements for access.
Prerequisite(s)	Connectivity / networking A
Reference	ISO 27002-2007, p60

Capability	**D**
Title	Perform audit on network components to ensure everything is up and running correctly
Description	Regular audits on the network architecture are performed to ensure it is performing on the desired level.
Prerequisite(s)	Connectivity / networking B
Reference	NIST SP800-53R4, p.89

Capability	E
Title	Respond to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Connectivity / networking D
Reference	NIST SP800-53R4, p.89

Security implementation

Training and education

Capability	A
Title	Develop training policies and procedures
Description	Training policies and procedures are developed which describes what training will be provided and the contents of the training.
Prerequisite(s)	-
Reference	NERC1200, p.14

Capability	B
Title	Train users of smart grid components (such as system engineers, technical engineers, auditors, etc.)
Description	Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities within the smart grid.
Prerequisite(s)	Training and education A
Reference	NIST SP800-30, p.36

Capability	C
Title	Improve the quality of personnel through certification
Description	Personnel are trained according to certified institutions or programs.
Prerequisite(s)	Training and education A
Reference	WIB M-2784-X10, p.19

Capability	D
Title	Keep personnel updated with recent developments
Description	Consistently keep the knowledge of relevant security information of personnel up to date through maintained contact with special interest groups.
Prerequisite(s)	Training and education A
Reference	ISO 27002-2700, p.12

Testing

Capability	A
Title	Implement test procedures to test the software and hardware components and networks included in the smart grid
Description	Test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard.
Prerequisite(s)	-
Reference	NERC1200, p.18

Capability	B
Title	Adhere to test procedures
Description	The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually
Prerequisite(s)	Testing A
Reference	NERC1200, p.18

Capability	C
Title	Have test procedures integrated into the system architecture
Description	Have policies and procedures for security testing, approval and maintenance of software integrated in the system/architecture.
Prerequisite(s)	Testing A
Reference	WIB M-2784-X10, p.22

Capability	D
Title	Act according to test results
Description	Mechanisms are in place to minimize recognized weaknesses.
Prerequisite(s)	Testing B
Reference	WIB M-2784-X10, p.22

Capability	E
Title	Perform audit on test procedures
Description	Conduct audits to decide the used test procedures are correct and up to date.
Prerequisite(s)	Testing A
Reference	NIST SP800-53R4, p.89, NERC1200, p.18

Capability	F
Title	Respond to audit outcomes
Description	Actions should be taken based on the results of the audits.
Prerequisite(s)	Testing E
Reference	NIST SP800-53R4, p.89