FP7 Grant Agreement N° 607109

***S*ecurity for smart *E*lectricity *GRID*s**

D1.6 Recommendations of improving smart grid security policies

Due date of deliverable: 01-03-2017
Actual submission date: 02-03-2017
Work package: WP1 Use cases and security goals
Number of pages: 32
Revision: Version 1
Classification level: Public

Project type:	Collaborative project – small or medium scale focused research project
Thematic Priority:	FP7-SEC-2013-1
Start date of project:	October 1st, 2014
Duration:	36 months

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

Management summary

During previous research by SEGRID into gaps in policies, legalities and regulations, we discovered multiple gaps that hinder in one way or another innovation and research in smart grids, within the field of cyber security and data protection. We have refined this research by sending out a questionnaire, and taking several interviews with various stakeholders within the energy sector, smart grid innovators, Distribution System Operators, etc.

From this research we found similarities to our previous research to underpin our findings, as well as new insights that were found to be highly relevant to this research. One of our primary findings is the requirement for harmonisation in policies, legalities and regulations between member states of the EU, due to the interconnected nature of smart grids. Another is the value of information sharing between member states on cyber security incidents, for example the requirement for reporting a breach of personal information. Based on the gaps found we propose recommendations on improving policies, legalities and regulations in order to boost innovation for smart grids, with regards to security and data protection.

Authors	Ruben ten Hove (TNO) Eric Luiijf (TNO)
Contributors	Nuno Medeiros (EDP) Johan Rambi (Alliander) Marcial Valmorisco (INCODE) Reinder Wolthuis (TNO)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	01-03-2017
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 5
1.1 The SEGRID project objectives 5
1.2 Work Package 1 – Use Cases and Security Goals 6
1.3 Deliverable D1.6 7
1.4 The structure of Deliverable D1.6 9
2 SURVEY 9
2.1 Questionnaire 9
2.2 Interviews 9
2.3 Selection of participants 11
3 GAP ANALYSIS 12
3.1 Gaps from previous SEGRID research 12
3.2 Gaps caused by regulatory issues 15
3.3 SPARKS workshop 16
3.4 Gaps based on other relevant work 18
4 RESULTS AND CONCLUSIONS 19
5 RECOMMENDATIONS 20
6 GLOSSARY 22
7 REFERENCES 26
ANNEX A: QUESTIONNAIRE 28
Introductory text 28
Questions 28
Description of scales for question 4 29
ANNEX B: GENERAL INTERVIEW QUESTIONS 31
ANNEX C: INTERVIEWEE LIST 32

List of Figures

Figure 1 - SEGRID storyline 6
Figure 2 - Dependencies in WP1 7

1 Introduction – Rationale of this document

This section introduces the SEGRID project and defines the goals of this deliverable.

1.1 The SEGRID project objectives

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In the coming years, the level of automation in electricity distribution grids will grow substantially. Smart meters will be deployed at home premises, and remote terminal units (RTUs) will be placed in distribution substations. The increased automation should provide a better view of how electricity flows to the medium and low voltage grids. It will provide grid operators increased control of that flow. But the increased automation also has major consequences for the cyber security of the enhanced electricity grid. Not only does it add new attack vectors through which cyber attackers can enter and attack the networks of grid operators, the automation also offers other possibilities to damage the electricity grid itself.

From a technical point of view, it is not sufficient to only consider all the different components in a Smart Grid separately; they will together form a truly integrated system-of-systems. Moreover, the Smart Grid will neither be completely owned, nor completely controlled, by a single power system operator. There will be many smart grid services and components that are operated by other organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new methods for connecting with various smart grid applications using a diverse set of communication channels, such as local connection interfaces, distributed web access, and smart apps on smart phones. Many new cyber security issues become critical in this context.

This new utility-wide system (-of-systems) will not come into existence overnight; the smart grid will be composed of a mix of old, even legacy, and new components. Therefore, we look at the smart grid as a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the smart grid at large. The required security solutions to cope with this situation range from improvements in current security, privacy and operational, technical and organisational measures to the introduction of new security and privacy paradigms.

The term 'Smart Grid' is used for a wide variety of developments related to the automation of electricity grid. Focusing on the efforts of the project, SEGRID will work on five concrete use cases, shown in Figure 1. These have been further elaborated in the deliverable D1.1 of the project [1]. The five SEGRID use cases are:

1. Smart meters used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.

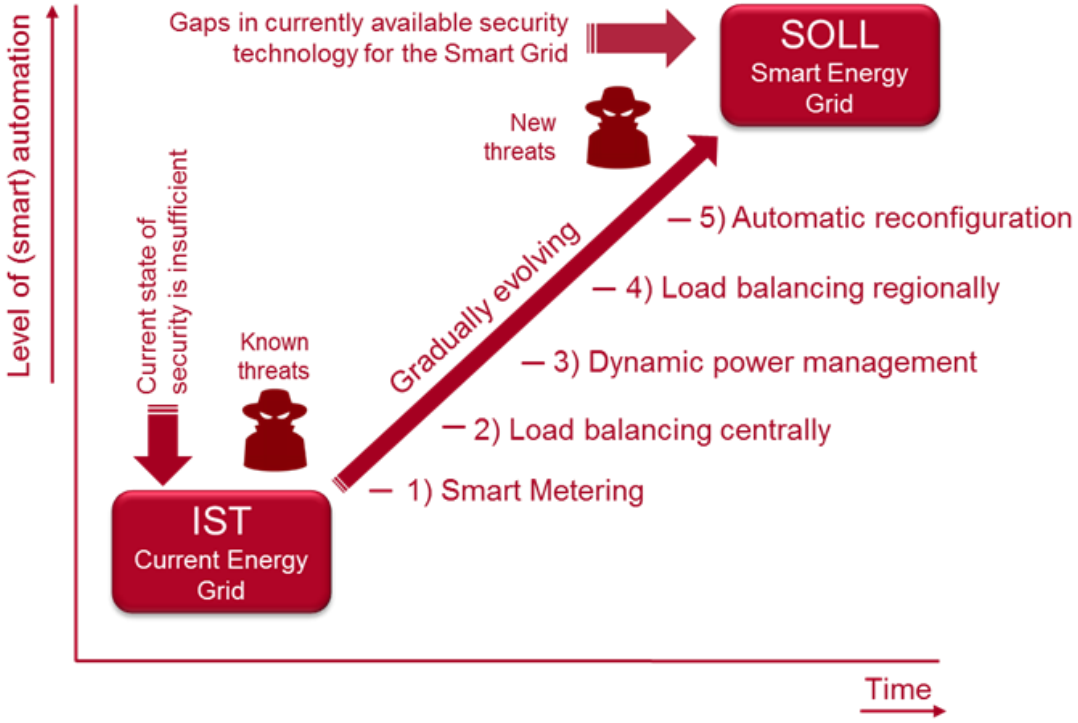

Figure 1 - SEGRID storyline

The SEGRID use cases reflect important steps of the smart grid developments until 2020 and beyond. They cover the most relevant security and privacy issues that will arise from the increasing complexity of smart grids.

SEGRID will formulate privacy and security goals for these five use cases and perform a risk analysis of these use cases (WP2). Vulnerability assessment frameworks and tools to identify the risk in real systems will be developed (WP3), and gaps in the currently available security solutions will be identified (WP2). Solutions for some of these gaps will be developed in WP4. Selected vulnerability assessment tools and novel security solutions will then be tested in SITE (WP5).

1.2 Work Package 1 – Use Cases and Security Goals

Work Package 1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

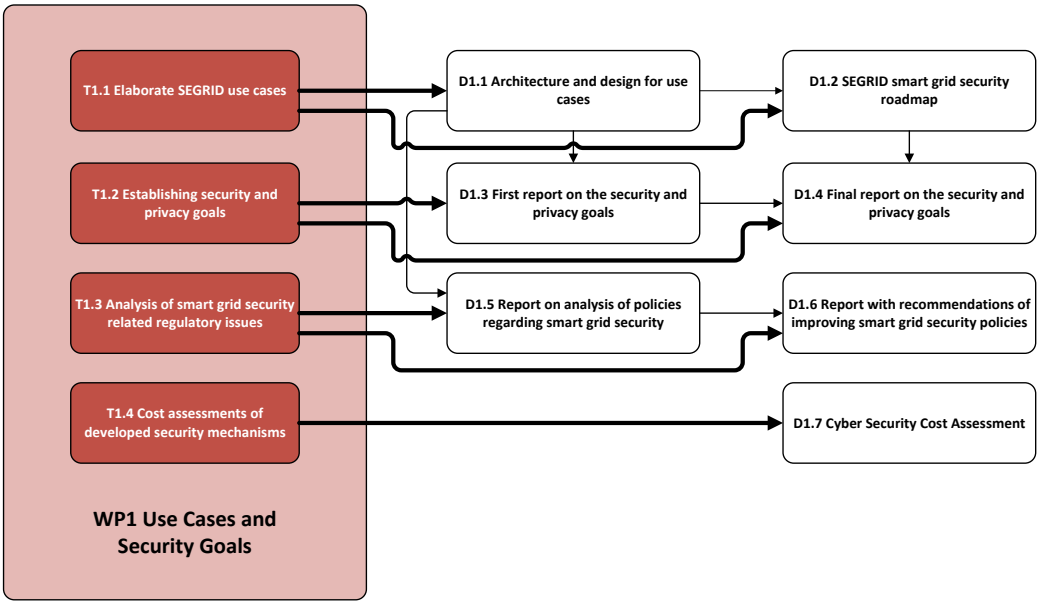

Figure 2 - Dependencies in WP1

The Work Package 1 main objectives are:

- Elaborate on the SEGRID reference architecture and describe the five use cases.
- Establish the security & privacy (S&P) goals for each of the SEGRID use cases.
- Identify points of improvement with respect to Smart Grid security and privacy in policies.
- Assess the cost of implementing security protection technologies that are developed in WP4 for each of the smart grid use cases.

1.3 Deliverable D1.6

Policy background

The European Smartgrids Security and Resilience Task Force states in [19]: "*By 2020, it is expected that 20% of the EU energy demand will be met by renewable generation. In the context of the targets proposed, it is expected that the electricity sector would be largely decarbonised by 2050, with potentially significantly increased levels of electricity production and demand driven by the integration of segments of heat and transport sectors (ed. electric vehicles) into the electricity system.{…} the key issue regarding the future evolution of operation and design practices and standards is associated with the question of efficiency of the use of existing assets and the role that advanced, smart grid technologies could play in the future development and delivery of security of supply to consumers.*" These goals, called the 20-20-20 goals, are derived from the European Strategic Energy Technology Plan (the SET-Plan) [20]. The second milestone of the SET-Plan is 2050. The EU strives for a worldwide transition to a low carbon economy limiting climate change to a global temperature rise of no more

than 2 °C compared to 1990 levels. The 2015 United Nations Climate Change Conference in Paris has introduced a new milestone: over 40% less greenhouse gasses, over 27% energy use from renewable energy resources, and a 27% higher energy efficiency in 2030. It is even expected that the EU will aim at an over 30% higher energy efficiency.

To achieve such goals, innovative technologies are developed that fall under the scope of smart grids. These advanced technologies are, in the context of SEGRID, required to be cyber secure and that the privacy of citizens is duly protected.

Moreover, [17] states "*cyber security is a key issue as the deployment of increased ICT introduces new vulnerabilities to the (ed. energy) system. These must be proactively addressed across all sectors of the electricity system as opposed to simply meeting regulatory requirements. This will require increased effort for regulators, system operators and technology providers.*"

Objective

As part of SEGRID's Work Package 1, we concentrate in this deliverable on the juridical and regulatory context of smart grid developments.

Our primary objective is to research the following:

- To what extent do existing policies, laws and regulations accommodate and support the (experimental) use of smart grid technologies and innovation in the field of smart grids?[1]
- The introduction of smart grid technologies may flourish from accompanying juridical and regulatory measures at a wider scale than just in a national (EU member state) context. To paraphrase upon [18] clause 43: "*The challenge is to ensure that legal, regulatory and grid operation frameworks facilitate the deployment of smart technologies and smart solutions. These frameworks must incentivize innovation and efficiency and support new commercial arrangements, whilst protecting consumer and customer interests, the security of supply and the cyber security of the smart grid.*"
  During the development and introduction of new smart grid technologies, care should be given to existing non-smart grid European and national laws and regulations, such as the General Data Protection Regulation (GDPR) [10].

To achieve this objective, we conduct interviews, send out a questionnaire, and consolidate findings from previous research within SEGRID as well as in other efforts to improve smart grid security policies, legalities and regulations. These results will be used to provide recommendations to European standardisation bodies, policymakers and regulators in their development of smart grid-related policies, legalities and regulations.

[1] This aligns with the Way Forward paragraph 3.5 in [1].

1.4 The structure of Deliverable D1.6

This deliverable is structured as follows:

- Chapter 1 introduces this deliverable and describes its objectives and content.
- Chapter 2 presents the survey. This is where the participant selection method, questionnaire format, and the interview methods are described.
- Chapter 3 summarises the gap analysis results of deliverable D1.5 "Report on the analysis of policies regarding smart grid security", as well as the results of background research and the findings from the survey.
- Chapter 4 summarises the results and conclusions from our analysis.
- Chapter 5 presents the recommendations based on the aforementioned results, which allow to enhance existing legal frameworks, policies and regulations to further support the development and innovation within smart grids.

2 Survey

We have sent a questionnaire to a group of relevant stakeholders from EU member states and associated countries participating in the SEGRID project, as well as to relevant stakeholders from countries that are actively developing and innovating within the field of smart grids. In the questionnaire, we presented our findings from deliverable D1.5 for further refinement. The second part of the survey is a series of interviews with a set of policy, regulatory, operational and smart grid manufacturing representatives, EU-wide, to further understand and incorporate their views on current policies and regulations regarding smart grid development and innovation. We use these results to refine our gap analysis and most importantly our recommendations.

2.1 Questionnaire

The questionnaire was setup on an open source, web based questionnaire platform called LimeSurvey. This platform was hosted on servers managed and owned by TNO and could be reached via https://survey.segrid.eu. The questionnaire was focused on a specific list of policy documents from the list that was identified and reviewed for deliverable D1.5. For each of these policy documents, a short set of questions was presented to determine the relevance of that document to that specific participant, and what role that document plays for their specific field. The setup of the questionnaire can be found in Annex A: Questionnaire.

2.2 Interviews

To extend the results of the questionnaire with a more detailed analysis, we performed interviews with a selected group of stakeholders who have extensive knowledge on different fields

pertaining to smart grid security and data protection. The individuals were selected based on the selection framework shown in paragraph 2.3 below.

A set of questions was used as a starting point for all interviewers to ensure a consistent structure, and to be sure that these subjects were covered. The interviewers were free to ask further questions as they deemed fit for SEGRID's purposes, depending on the course of the interview. The set of base questions is given in Annex B, which we have summarised below:

Personal

We discuss the tasks and responsibilities in relation to smart grid policies/regulations of the interviewee.

General policies and regulations

We discuss the way the interviewee deals with smart grid security and data protection documents and regulations, as well as their experience and opinion on these.

After that we continue the discussion on the possible issue of data protection in smart grid development, what the role should be of regulators and who the main stakeholders are for data protection.

EU

After discussing more general topics, we discuss the role of the EU, how they should respond and how they currently respond to the changes occurring due to the development of and experimentation with smart grids. We also discuss the expected future of the involvement and roles of the EU, as well as the role of the GDPR.

Other

Finally, we conclude the interview with a broad topic where we discuss public/private partnerships and collaboration, as well as education in cyber security and data protection.

The goals of these interviews were to:

- Understand the experience of the interviewees with Smart Grid cyber security and privacy policies, legalities and regulations; and,
- Support and refine our recommendations based on these experiences.

Interviews were done by two interviewers. One person focused on the discussion with the interviewee, and the other focused on documenting the discussion.

2.3 Selection of participants

Individuals that were invited to fill-in the questionnaires or be interviewed, were selected as such to have an even distribution among a selection of domains, function types, and countries. An overall requirement for participants was their knowledge and experience with smart grid related policies and regulations.

Only a small group of people met our strict set of requirements and thereby could contribute significantly to our research efforts. This increases the risk of a low response rate, but since each response is expected to be highly informative, this is not expected to be an issue.

We selected several relevant stakeholder groups to ensure the correct focus on the most relevant topics for our research. From these stakeholder groups, we expect to gather insights into knowledge on gaps that impede or hinder innovation for smart grids, as well as how gaps may be alleviated from a juridical or regulatory perspective. Our selected potential participants fall within the following categories:

- Stakeholder groups
  - Distribution Service Operators (DSO)
  - Independent/academics
  - Smart grid equipment manufacturers
  - EU representatives
  - National authorities
  - Consumer association
- Function types
  - Privacy
  - Security
  - Governance
- Countries
  - Netherlands
  - Germany
  - Spain
  - Portugal
  - Sweden
  - Norway
  - Italy

All results were processed anonymously. We summarise the interviewees by role and country/region in Annex C.

3 Gap analysis

Based on our previous research in SEGRID, literature research, a workshop participation and the survey, we have identified and described gaps that we have found to further answer the question in our objective. A gap is defined as the difference between current policy or regulation and the (by SEGRID) identified need for guaranteeing the security of supply, a balanced and reliable power grid, fair markets, and guarantees with respect to data protection (privacy) in smart grids.

3.1 Gaps from previous SEGRID research

In this deliverable (D1.6) we build upon the results and conclusions of deliverable D1.5, in which an analysis was performed to provide an expert overview of current policy gaps and regulatory issues related to smart grids at the EU and national levels. These gaps have been summarised below:

In most EU member states only specifically designated critical infrastructure operators ("operators of essential services") will need to report cyber security breaches to national authorities and ENISA based upon the national implementation of the NIS Directive [3].[2] Similarly, according to the GDPR [10], energy operators need to report data security breaches that affect the personal data protection and/or the privacy of citizens.
However, in some EU member states (e.g. The Netherlands), each critical infrastructure operator is already legally obliged to report both privacy and data protection breaches to one or more authorities.

As EU member states have different opinions about what comprises their national critical infrastructure (NCI), see e.g. [4], and "operators of essential services" [3] article 5(2), cyber security incident reporting and other obligations accruing to [3] about cyber security incidents in smart grids may not be obliged for all smart grid operators. Based upon our analysis in D1.5, the security, safety and reliability of smart grids requires a firm European-wide harmonised approach with a *fast* and *effective responsiveness* to new cyber threats and incidents:

GAP 1: There is no effective framework for mandatory sharing of cyber security incidents in smart grids in the EU between the *competent authorities* and the *computer security incident response teams ('CSIRTs')* in the member states and ENISA.

[2] Note that reporting privacy-related cyber security breaches by utilities and other organisations is mandated in [11]. Some of the national Data Protection Authorities are given mandates to fine non-compliant organisations.

In the end, all smart grid operators and the citizens benefit from early shared knowledge in trusted (inter)national settings about threats and vulnerabilities to smart grids.

GAP 2: Not every energy operator that operates a Smart Grid is designated as an 'operator of essential services' in the national implementation of the NIS Directive, which causes ambiguous differentiation between interdependent stakeholders.

Sharing cybersecurity-related information amongst electric utilities operating smart grids in e.g. settings as Information Sharing and Analysis Centres (ISACs) is widely considered to be an effective measure to prevent, counter and respond to cyber security threats. However, sharing information between utilities about cyber security of smart grids may be regarded in conflict with business drivers, anti-trust laws, national security, regulations, and other barriers [5].

At the same time, the US Smart Grid Interoperability panel developed a white paper [6] on the sharing of cybersecurity-related information amongst electric utilities. Moreover, the European Communications [7] and [8] articles 4, 13, 14 and 17, the NIS Directive [3] articles 10, 14, 16, 19, and 20, and Recommendation 6 in [15] push for effective countering cyberattacks by sharing information.

Although a European Energy ISAC (EE-ISAC) has already been established as a public-private partnership (PPP), materializing the results of the DENSEK European project, funded by the DG Home Affairs, it is still an open and non-EU based initiative from a group of organizations that believe that information and incident sharing are key levers for the success on the protection of the European Smart Grids against cyber threats. EU support and provision, namely from DG Energy or ENISA, could facilitate the adoption of the EE-ISAC as the platform per excellence for an effective information and incident sharing in the EU.

GAP 3: The lack of an effective community and framework for sharing cyber security-related information including breaches, incidents and vulnerabilities amongst the European Smart Grid operators.

The publication [9] may help to overcome internal and national barriers, and to stepwise develop a culture of sharing by addressing the problem of information sharing step by step.

In Europe, current investments in smart grids are market-driven, e.g. households and companies get simple access to consumption information so they can keep their energy costs down. The EU promotes to incentivise Smart Grid investments and deployment. EU's Communication on smart grids [12] states as a third objective that EU's Electricity Directive [13] and the Energy Services Directive [14] should enable the emergence of a regulatory framework that provides incentives for such investments. Within that context, EU's second objective with

respect to smart grids is data privacy. However, there is no clear notion of how cyber security is to be addressed within these directives.

GAP 4: **The notion of *cyber secure* smart grids is yet to be clearly and thoroughly described in both Directives**.

On page 16 of [15], it is stated that "*Cyber security has become one of the main concerns regarding the implementation of smart grids, and especially regarding the networks used for the interconnection of all the assets that make up this new grid. Therefore, an inherent requirement is to protect these communication networks, the data that travels through them and the devices connected to them.* {…} *Each European country has a different regulation and infrastructure regarding power grids, in many cases due to the specific needs of each one. Furthermore, they tend to make use of different standards for these implementations, architectures and assets in use*." and "*There is the need to harmonize European requirements and standards for smart grid communication networks, especially regarding the homologation of security devices and protocols.*" ENISA therefore recommends "*The European Commission should ensure the alignment of policy approaches across EU countries to establish a common posture for smart grid communication interdependencies.*"

From our analysis in D1.5, we conclude that this recommendation needs to be widened.

GAP 5: There is no alignment of EU-wide policies to cover the full spectrum of cyber security in smart grids; where it also should not only cover the data communication and data transport parts.

On pages 60 and 61 of a Dutch study [16], it is debated that national Telecommunication laws and related EU telecom sector directives concentrate on the classical telecommunication sector. With the evolvement of smart grids, integration between the telecommunication and energy sectors grows much faster. Regarding laws and regulations, [16] we can split the domain into three areas[3]:

1. Rules that apply to all (end users), independent type of networks and services. For smart grids, no specific issues arise.
2. Rules that apply to electronic communication networks including access to user data areas using the public communication networks.
3. Rules that apply to the providers of electronic communication networks, e.g. registration with the Regulator, privacy protection, interconnectivity, legal interception.

[3] A fourth area is omitted from this list as it is specific for the Netherlands telecom market situation.

It can be debated whether some specific telecommunication rules apply to smart grids. Often it is an interpretation of the definitions which have been defined before any notion about smart grids became evident.

GAP 6: **EU-wide Telecommunication sector laws and regulations narrowly consider telecommunication service security and privacy aspects. There is a gap with respect to the legal and regulatory security and privacy aspects of telecommunication services which are essential to cyber-physical systems such as smart grids**.

3.2 Gaps caused by regulatory issues

We also describe gaps caused by regulatory issues, which are summarised below. A regulatory issue is defined as a mismatch between the current regulation and the need for innovation for Smart Grid developments, e.g. current regulation hinders or even blocks Smart Grid development.

[19] states: "Over the past decade, the actual reliability performance of electrical distribution networks in EU has been considered. In other words, regulatory regimes have recently introduced incentives for network operators to minimise the consequences of interruptions, through enhancing supply restoration processes. Although these initiatives represent a step in right direction, the focus has been mostly on the system rather than on customer focused indices, which may need to be reviewed, as the security of supply seen by real customers may be radically different from these system level indices used in the current incentive mechanisms."

GAP 7: Metrics for the reliability performance of electrical distribution networks in the EU do not consider the system and customer aspects on a fair balance.

The CEER (Council of European Energy Regulators) Work Programme envisages a 'CEER Status Review on European regulatory approaches enabling smart grid solutions ("smart regulation")'. With respect to privacy their last report [2] states: "*There was no clear consensus on whether the NRA (ed. National Regulatory Authorities in Europe) will be involved in* data security *regulation for smart meter data. Nevertheless, in Belgium, data security will form part of the DSOs core duties, which the NRA will oversee the compliance of. In the Czech Republic, data security will be the responsibility of the Office for Personal Data Protection, as in France, where there is also a separate and dedicated agency in charge of data security. In Germany, this is the responsibility of the Federal Office for Information Security. In the UK, the NRA will approve data aggregation plans from the DNO* [(Distribution Network Operator)], *and data privacy requirements are covered under licence conditions. In Slovenia, the NRA will conduct a CBA for smart metering which will include security issues. Finally, in the Netherlands, the NRA and the Data Protection Authority operate in conjunction with each other on data security matters.*"

It is obvious that the National Regulatory Authorities do not have a harmonised and standardised approach to privacy, more specifically the GDPR [10], in smart grids. Moreover, with respect to security, [2] discusses only the general security of supply and safety objectives. No specific mentioning and therefore analysis of cyber security aspects can be found in [2].

GAP 8: The National Regulatory Authorities in the EU Member States do not have a harmonised and standardised approach to cyber security and privacy in smart grids.

The above summarised our findings in our previous research. In the following chapters we build upon these findings by gathering information from external stakeholders and efforts within our research domain.

3.3 SPARKS workshop

In preparation for the discussions at the SPARKS workshop "Smart Grid Security Requirements: economic, legal and societal aspects", European Parliament, Brussels on 19.10.2016 [21], the set of gaps summarised in the previous chapter was extended with several new gaps.

The NIS Directive requires central reporting of cyber security breaches. The Directive does not give direction with respect for what needs to be done with that information other than providing an anonymised summary report. Given the high societal risk of disrupted Smart Grids, each incident should be investigated independently in a way to derive market-wide lessons identified to be implemented by all manufactures and utility operators that use smart grid components.

GAP 9: Currently only statistical incident collection is done for incidents by competent authorities and ENISA. There is no independent root cause analysis on cyber security and data protection (near miss) incidents, from which lessons learned can be derived.

VEMW, the Dutch cooperation of bulk energy consumers, has warned for an increase of cumulative power outage duration in The Netherlands due to a new legislative proposal that mandates less redundancy for certain power distribution systems than is currently the case [23]. Due to this change, he VEMW also pushes for the obligation of an independent root cause analysis after major power disruptions in The Netherlands.

GAP 10: Lessons identified are not shared and applied sector-wide by manufacturers of Smart Grid equipment and software and by utility operators that apply to smart grids.

In addition to the central reporting of cyber security breaches by operators of essential services, smart grid operators can derive lessons from cyber security and privacy-related incidents which have the potential of a serious impact to society and the citizens.

We were also able to identify new gaps and other sources for recommendations by inspiration from presentations and discussions during the workshop, in combination with previous research in the SEGRID project:

- EU member states are at a different pace of implementing Smart Grids, and as such also at designing and implementing policies, legalities and regulations regarding cyber security and data protection. Harmonisation may assist in alleviating this issue, but it should not be an objective in itself, meaning that smart grid innovation and implementation cannot take place before (after a long period of discussions) harmonisation has taken place. [21] A negative aspect might be that frontrunners need to adapt to the new harmonised approach afterwards.

- Consider the move of responsibilities of the Transmission System Operator (TSO) to the DSO, because there is a redefinition of the interface between the grid and customers/prosumers. This interface is now both physical and Information and Communication Technology (ICT)..
  Besides that, new (yet unknown) actors / manufactures / services start to emerge from the combined ICT-energy sectors. From this a new role emerges, that of cyber security and privacy in relation to the security of supply policies.

- The Smart Grid will connect millions of smart meters, and easily a ten to twentyfold of smart appliances, e-vehicles, and other appliances. Most of these will not be updatable without physical access/replacement. During the design phase, any possible needs for cyber security related hardware, firmware and software upgrades should be considered.

GAP 11: Smart Grid designs have improper measures for dealing with the security upgrade of a myriad of smart grid components without the need for accessing each component individually.

- During a SPARKS presentation, several cyber security measures regarding smart grids were proposed, for example, awareness and incident response time. We commented that the presented view lacked attention to the full incident response cycle, for exam-

ple to introduce measures for investigations to connect 'inforensics'[4], and identifying lessons from incidents and near misses.

- Sector-wise information sharing of cyber security and privacy breach information shall go above anti-trust and national security approaches and should not lead to fines by the energy regulator.

3.4 Gaps based on other relevant work

Other research efforts that are not related to SEGRID but have done relevant work, have been summarised below. From these we also derived gaps that need to be addressed.

The Smartgrids Security and Resilience Task Force has identified various requirements for changes in the standards used for electricity network reliability [19]. A primary finding in their effort is the reliance on currently used standards that are based on historic philosophies around the energy sector. The unprecedented level of uncertainty that characterises smart grid development is not addressed in current reliability standards and grid codes [19].

GAP 12: Reliability standards that are based on traditional and historic setups may impose cyber security measures that counteract the efficiency that smart grids are expected to give.

GAP 13: Smart grid development is characterised by unprecedented levels of uncertainty, and these are not properly addressed in reliability standards and grid codes.

It is expected for DSOs to invest heavily in innovation of systems within the domain of smart grids in order to achieve policy goals, for which [22] found market driven and incentive-based regulatory schemes to be key enablers for such investments.

[4] A.k.a. digital forensics

4 Results and conclusions

Our primary results come from the combination of questionnaires and interviews. Although the questionnaires gave interesting insights, they have only been processed as a qualitative source due to the low response rate. The most important findings from both the questionnaire as well as the interviews are as follows:

1. There is a broad agreement on the lack of harmonisation when it comes to policies, legalities and regulations on smart grid security and data protection across the member states of the EU. The GDPR may change that for the data protection of end-user information. From the point of view of the member states, this may be interpreted as there not being a clear plan to adhere to for commercial and public organisations.
2. Current policies and regulations show a misbalance between cyber security and data protection, where the balance is mostly towards data protection.
3. Cyber security is separated from the general discussion on smart grids as a secondary subject, and cyber security is not yet viewed as an integrated and fundamental part of smart grid design and development.
4. Member states are mostly reactive instead of proactive towards cyber security and data protection. As such, member states rely on actions by the EU (e.g. the GDPR and the NIS Directive).
5. Some member states already have laws and regulations which cover parts of, for example, the NIS directive. Such laws and regulations may introduce conflicts for DSOs that operate smart grids in multiple nations.
6. There is a shortage of people with the right skillset to address the (upcoming) cyber security and data protection issues, both at the technical level and the strategic/tactical where legal, business, and technical aspects meet each other.
7. There is currently a difference in maturity of smart grid introduction and operations between member states. These differences can be quite large. This is not expected to synchronise soon across the member states.
8. Mandatory sharing of cyber security related incident information is found to be highly valuable. This should also include root cause analyses of incidents and near miss incidents. Information sharing collaborations are in place in several member states and across member states, although their maturity may differ a lot.

These findings demonstrate that there is a need for EU-wide standardisation and harmonisation, where the effort from member states needs to be increased to ensure this happens on a balanced level where the strong differences between member states have to be considered.

Our findings show an important baseline for improving policies, legalities and regulations to further guarantee the security of supply, a balanced and reliable power grid, fair markets, and guarantees with respect to data protection (privacy) in smart grids, as well as to boost innova-

tion by alleviating regulatory obstacles for (experimental) implementation of innovative smart grid technologies and processes.

Since the innovation and evolution of smart grids is a process that is highly volatile in its current stage of experimentation and large volume rollouts, the future of smart grids will probably require a different approach. As such, this research should also be used as a framework on which further analysis should be done on how to optimise the balance between freedom for innovation, cyber secure and reliable smart grids, and privacy.

5 Recommendations

Based on the results of our internal gap analysis, further research and analysis, and the survey, we have devised the following legal, policy and regulatory recommendations. The following cyber security and data protection related juridical and regulatory recommendations for smart grids were also derived from the previously discussed literature, either directly or by inspiration.

We divide the recommendations between EU-level, the national level, and grid operators. Presented as such, the right target audience can be selected when reading these recommendations.

EU-level

1. We recommend to setup a framework for a community for sharing cyber security-related information, including breaches, incidents and vulnerabilities amongst the European Smart Grid operators. This is to address gap 3, by developing a culture of sharing such information in a way that benefits the sector in improving the cyber security of smart grids at any stage. The existing EE-ISAC could take on this role if formally supported and sponsored by the EU.

2. The CEER is recommended to include cyber security related aspects explicitly in their assessment framework, to address gap 8 and ensure cyber security is addressed with the same strictness and capability as data protection.

3. The European Commission is recommended to ensure the alignment of policy approaches across EU member states to address gap 6:
    - establish a common posture for smart grid cyber security (also including communication infrastructure dependencies).
    - avoid ambiguities with respect to applicability to smart grids in telecommunication-related directives.

4. We recommend the EU to not only highlight data protection and security of supply in Smart Grid related EU Communications, but to highlight as well the need for *cyber*

security in smart grids. This would first require gap 4 to be addressed, for which we recommend the European commission to create a clear and thorough description of *cyber secure* smart grids.

5. Performing root cause analysis helps organisations to identify lessons learned in such a way that these can be shared with organisations in their own and similar domains. From this it is possible to derive recommendations for such organisations to further minimise the possibility of repeat or similar incidents. As such we recommend organisations to learn from countries already performing such analyses. An example is the obligation for Dutch organisations to report leaks of data. This would alleviate the gaps 1, 9 and 10.
    - Based on gap 9, near misses may not mandate a root cause analysis, but may require changes on a broader scope. As such reporting of near misses allows parties to learn lessons from where an incident could have happened, and how future incidents may be avoided within the sector/domain.

6. For smart grid hard- and software design we recommend describing requirements that ensure security upgrades can be performed within a strict time window with minimal investments, to address gap 11. Such requirements should be set by the user (e.g. the DSO) for their supplier, or should be set by a governing body.

7. When incidents occur, these currently mainly impact the customer, compared to the other stakeholder groups. Even though reduction of impact from incidents is a primary goal, the impact difference between stakeholder groups needs to be rebalanced in order to address gap 7.

8. To further support the continued development of cyber secure smart grids, we recommend to incentivise skill building within the field of cyber security, to ensure this growing dependency on cyber security can be supported by people with a matching skillset.

National level

1. Awaiting an EU-wide approach, we recommend that either the member states, National Competent Authorities or Energy-related Regulators designate all smart grid operators as “operators of essential services” per the NIS Directive ([3] article 5(2)) in order to address gap 2. This recommendation is in support of NIS Directive [3] article 6 “Significant disruptive effect” (1a-1c) considering 1d (wider spread across nations in Europe).

2. Awaiting an EU-wide approach, we recommend that either the Member States, National Competent Authorities or Energy-related Regulators designate all smart grid

component manufacturers as "digital service provider" per the NIS Directive in order to address gap 9. This recommendation is in support of NIS Directive [3] article 6 "Significant disruptive effect" (1a-1c) considering 1d (wider spread across nations in Europe).

3. We recommend nations to remove conflicts between telecommunication laws and regulations with respect to smart grids to address gap 5.

4. National Regulatory Authorities are recommended to harmonise and standardise their approach to privacy-related regulation in smart grids based on the GDPR [10] to address gap 8. This will result in a much clearer standardised focus point for any stakeholder to adhere to.

Grid Operators (TSO, DSO) in their Grid Codes

1. As stated in [19] page 6, the current N-1 / N-2 network design code may need to be reassessed in the light of the smart grid dynamic demand regulation possibilities such as curtailment of non-essential demand and the use of new local energy storage possibilities, e.g. in electric vehicles and batteries at homes. This addresses gap 12.

2. The unprecedented levels of uncertainty need to be addressed by grid operators, but for this the reliability standards need to be adjusted towards the development of smart grids to address gap 13.

6 Glossary

This glossary serves as inventory of abbreviations used in the document.
This is a standard glossary, used for all technical SEGRID deliverables

Acronym	Description
ABAC	Attribute-Based Access Control
AMI	Advanced Metering Infrastructure
API	Application programming interface
APT	Advance Persistent Threat
ASLR	Address Space Layout Randomization
BLP	Bell-LaPadula
BYOD	Bring Your Own Device
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CDF	Cumulative Distribution Function
CEN	European Committee for Standardization.
CENELEC	European Committee for Electrotechnical Standardization.
CERT	Computer Emergency Response Team
CIS	Customer information system

CPS	Cyber-Physical System
CSO	Charge Spot Operator.
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DAN	Distribution automation node
DC	Data Concentrator.
DEP	Data Execution Prevention
DER	Distributed Energy Resources
DMS	Distribution management system
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DoW	Description of Work
DPIA	Data Protection Impact Assessment
DRAACS	Demand-response analysis and control system
DSO	Distribution System Operator.
Dx.y	Deliverable x.y
EA	Enterprise Architecture
EAM	Enterprise asset repository
EC	European Commission
EDSA	Embedded Device Security Assurance
EMS	Energy management system
EMSP	E-Mobility Service Provider.
ERP	Enterprise resource planning
ETSI	European Telecommunications Standards Institute.
EU	European Union
EV	Electric Vehicle.
FE	Front end
FHS	Filesystem Hierarchy Standard
FS	Forecasting system
FTP	File transfer protocol
G3	Alliance for PLC technology.
GIS	Geographical Information System.
GDPR	General Data Protection Regulation
GMS	Generation management system
GOOSE	Generic Object Oriented Substation Event
GPRS	General Packet Radio Service.
GPS	Global Positioning System
GSSE	Generic Substation State Events
GUI	Graphical User Interface.
HAN	Home area network
HE	Head End
HES	Head-End System.
HMI	Human Machine Interface.
HTTPS	Hypertext transfer protocol secure
HV	High Voltage.
ICC	Inter Control Center
ICCP	Inter Control center Communications Protocol
ICS	Industrial Control System
ICS-CERT	Industrial control systems computer emergency response team

ICT	Information and Communication Technology
IDS	Intrusion detection system
IEC	International Electro technical Commission (ISO)
IED	Intelligent Field Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol (IPvx = IP version x)
IPS	Intrusion prevention system
IPSec	IP Security
ISO	International Organization for Standardization.
IT	Information Technology
LAN	Local area network
LCA	Latent Credibility Analysis
LDAP	Lightweight Directory Access Protocol
LN	Local Network.
LV	Low Voltage.
MAC (1)	Media Access Control
MAC (2)	Mandatory Access Control
MDMS	Meter Data Management System.
MMS	Meter management system
MOF	Meta object facility
MU	Merging unit
micro-CHP	Micro combined heat and power.
MV	Medium (level) Voltage.
NAN	Neighborhood area network
NMS	Network management system
NN	Neighbouring Network.
NTP	Network Time Protocol
NVD	National Vulnerability Database
OMS	Outage Management System
OS	Operating System
OSCP	Open Smart Charging Protocol
OSGP	Open Smart Grid Protocol
OSI	Open Systems Interconnection
OT	Operational technology
OTP	One-Time Password
PCT	Programmable communicating thermostat
PHP	PHP: Hypertext Preprocessor (a recursive acronym
PLC	Power Line Communication.
PQ	Power Quality
PV	Photovoltaic
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RF	Radio frequency
RFC	Request for Comments
RTU	Remote Terminal Unit.
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition.
SCS	Substation control system
SDLA	Security Development Lifecycle Assurance
SE	Secure Element.
SEGRID	*S*ecurity for smart *E*lectricity *GRID*s.

SFTP	SSH File Transfer Protocol
SGAM	Smart Grid Architecture Model.
SG-CG	Smart Grids Coordination Group (ETSI).
SMITP	Smart metering Information and Telecommunication Protocol.
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SUC	System under Consideration, or Subject under Consideration
TCP/IP	Transmission Control Protocol / Internet Protocol
TEE	Trusted Execution Environment
TEPT	Trained Execution Path Tree
TOE	Target Of Evaluation
TSO	Transmission System Operator.
TTC	Time To Compromise
Tx.y	Task w.y
UC	Use Case
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VPN	Virtual private network
WAMS	Wide Area Monitoring System
WAN	Wide area network
WAP	Wireless Application Protocol
WMS	Workforce management system
WPx.y	Work Package x.y
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
3G / 4 G	Third/ Forth generation mobile communication.

7 References

[1] WP1 SEGRID, 'D1.1 Architecture and design for use cases', 2015.

[2] CEER, CEER Status Review on European Regulatory Approaches Enabling Smart Grids Solutions ("Smart Regulation"), Ref: C13-EQS-57-04, January 2014. Online: http://www.ceer.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/Tab3/C13-EQS-57-04_Regulatory%20Approaches%20to%20Smart%20Grids_21-Jan-2014-2.pdf

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").

[4] Definitions at CIPEdia©, www.cipedia.eu

[5] Eric Luiijf and Allard Kernkamp, Sharing Cyber Security Information, TNO, March 2015. DOI: 10.13140/RG.2.1.4321.7442

[6] R. Reddi, Cybersecurity Information Sharing in Electric Utilities, SGIP, February 2016.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400}.

[8] Directive 2013/40/EU of the European parliament and of the council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[9] Eric Luiijf and Marieke Klaver, On the Sharing of Cyber Security Information, in: Rice, Mason, Shenoi, Sujeet (Eds.), Critical Infrastructure Protection IX, Springer, 2016, pp 29-46, DOI 10.1007/978-3-319-26567-4_3.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (The "GDPR").

[11] Regulation (EC) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 24 April 2011 - Smart Grids: from innovation to deployment [COM(2011) 202 final.

[13] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Text with EEA relevance).

[14] Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006

on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC (Text with EEA relevance).

[15] R. Mattioli and K. Moulinos, ENISA, Communication network interdependencies in smart grids, ENISA, 2015.

[16] S. Akerboom, G. Buist, A. Huygen, A. Ottow, S. Pront-van Bommel, Smart Grid Pilots Part 2: Handvatten wet- en regelgeving intelligente netten [in English: Hooks for smart grid laws and regulations], UvA, TNO and UU, 2011.

[17] Technology Roadmap Smart Grids, International Energy Agency (IEA), 2011.

[18] Smart Grid Vision and Routemap, Smart Grid Forum, Department of Energy & Climate Change, London, February 2014.

[19] Smartgrids Security and Resilience Task Force, The need for a fundamental review of electricity networks reliability standards, May 2016. Online: http://www.smartgrids.eu/documents/ETP_SG_Future_Network_Reliability_Standards_2016.pdf

[20] European Commission, website European Strategic Energy Technology Plan. Online: https://ec.europa.eu/energy/en/topics/technology-and-innovation/strategic-energy-technology-plan

[21] SPARKS, Workshop report - Smart Grids Security Requirements: Economic, Legal and Societal Aspects, Brussels Oct 19, 2016.

[22] C. Cambini, A. Meletiou, E. Bompard, and M. Masera, 'Market and regulatory factors influencing smart-grid investment in Europe : Evidence from pilot projects and implications for reform', Util. Policy, vol. 40, pp. 36–47, 2016.

[23] AD, '"In toekomst meer stroomstoringen door nieuwe wet"', 2017. http://www.ad.nl/nieuws/in-toekomst-meer-stroomstoringen-door-nieuwe-wet~a390fb4d/.

Annex A: Questionnaire

Introductory text

SEGRID (Security for smart Electricity GRIDs) is an EU Framework 7 project, where several research efforts are undertaken to enhance the protection of Smart Grids against cyber-attacks. In a Smart Grid, it is not sufficient to consider all the different components separately; they will together form a truly integrated system-of-systems. Further information can be found on www.segrid.eu.

We kindly ask for your support as a (potential) Smart Grid stakeholder by completing this questionnaire. At the end of the project you can view the results of, among others, the analysis done on this questionnaire on www.segrid.eu. The objective of this questionnaire is to know the position of all stakeholders about policies regarding smart grid security and the application of them.

In this questionnaire you will be asked several questions about a list of policy documents that were found relevant to the scope of smart grids. This questionnaire will take approximately 30 minutes.

No personal information is collected as part of this questionnaire. Your unique ID is used so you can resume the questionnaire at a later point in time.

Questions

1) Is the content of this document known to you?
   a) Yes
   b) No (in this case, don't show further questions or only 4?)
   c) Partially, why?
2) Have you applied this document?
   a) Yes
   b) No (in this case, don't show further questions or only 4?)
   c) Partially, why?
3) Why is this policy applicable to you?
   a) Is it mandatory?
      i) Yes
      ii) No
   b) Large text field with suggestions for a qualitative answer:
      i) Because it is mandatory
      ii) Useful for application in own company/sector/target group
      iii) Assists in scoping
      iv) Protection of interests
      v) Etc.

4) How do you rate this policy on the following scales?
   a) 5 point scales for (Includes the explanations of each scale from D1.5)
      i) Practicability
      ii) Effectiveness
      iii) Strictness
      iv) Sustainability
5) Does this policy conflict with other policies?
   a) Which policy?
      i) Small text field
   b) How?
      i) Small text field

Description of scales for question 4

Effectiveness: How well does the policy ensure it will have its intended effects?

Scoring:

1. The policy has its objectives defined, but barely shows methods on how to effectuate these policies.
3. The policy has its objectives well defined, and shows methods on how to effectuate these policies, but leaves much room for interpretation of these objectives.
5. The policy has its objectives well defined, and shows methods on how to effectively apply these while ensuring these objectives will be met.

Strictness: What level of detail is required by the policy in the application of its objectives?

Scoring:

1. The policy leaves much room for interpretation, and uses broad terms to define its objectives and how these should be met.
3. The policy defines boundaries on the implementation, and shows several qualitative measures on how to achieve its objectives.
5. The policy barely leaves room for interpretation, and ensures objectives can be tested and measured to ensure if these are met.

Practicability: What is the practicability of implementing the policy? (regarding cost, time, etc.)

Scoring:

1. The policy asks for improbable timelines and has unclear or unrealistic expectations of the cost of achieving its objectives.
3. The policy has set requirements that can be achieved, but does rely on unclear assumptions.

5. The policy takes cost and time into account, and gives clear indication into the possible requirements regarding practical issues.

Sustainability: What is the ability of the policy to sustain its effectiveness on the long term?

Scoring:

1. The policy does not provide means to ensure its effects stay on the long term.
3. The policy provides means to ensure its effectiveness stays on the long term, yet provides little indication on what might be causes to lose its effectiveness.
5. The policy is clear on how to sustain effectiveness, and provides guidelines on how to ensure sustaining the effectiveness.

Conflicting: To what degree does this policy conflict with other policies?

Scoring:

1. The policy has no conflicting policies.
3. The policy may be hindered by several policies.
5. The policy seems unable to be applied (in certain regions) due to clear conflicting objectives.

Annex B: General interview questions

Below we have summarised the generic questions that were used as a starting point for the interviews.

- Personal
  - How would you describe your tasks and responsibilities in relation to smart grid policies/regulations?
- General policies and regulations
  - In what way do you deal with smart grid security and/or privacy policy documents and/or regulations?
    - What is your experience with it?
    - What is your opinion on it?
  - Do you think data protection will be an issue for the smart grid environment?
  - What should be the role of energy regulators on security/data protection matters?
  - What are the main stakeholders to achieve plain and comprehensive regulatory environment in relation to security & privacy in a smart grid environment?
- EU
  - How is EU responding to changes when it comes to security and data protection, related to smart grids? For example, prioritisation.
  - How can the EU commission help with achieving compliance to proposed policies and regulations?
  - What would, in your opinion, be a proper approach to implementing the NIS directive?
    - And what could be the impact of this implementation?
  - Do you think EU will have a growing impact on policies, or will 'we' move towards a more national driven smart grid policies and regulations?
    - What should be the way in your opinion, and why?
  - What do you think the impact will be of the GDPR on smart grids and why?
    - And what would be your recommendations to solve these issues?
    - How would we be able to adapt to the GDPR without jeopardising for example smart meter rollout?
- Other
  - Should public/private partnerships/collaboration be in- or decreased?
    - What is your opinions on roles being played?
  - Do you believe we have the right people/skills to address smart grid security issues within your sector?

Annex C: Interviewee list

The table below gives a list of the function and the location of the people interviewed

Sector	**Country/Region**	**Interviewees**
Governance	Netherlands	1
Governance	EU	2
Governance	Spain	2
Manufacturer	Germany	1
DSO	Spain	1
Manufacturer	Switzerland	1
Governance	Netherlands	1