



Workshop-Report:
**Smart Grids Security Requirements: Economic,
Legal and Societal Aspects**

**Brussels,
European Parliament
19th of October 2016**

Table of Content

1	Participants	3
2	Agenda.....	4
3	Executive Summary	5
4	Background of the workshop.....	5
5	Objectives of the workshop	6
6	Summary of introductory statements.....	6
6.1	Josef Weidenholzer	6
6.2	Manuel Sánchez-Jiménez.....	6
6.3	Sujeet Shenoj.....	6
6.4	Paul Smith and Ivor Bradley.....	7
7	Content and Results.....	8
7.1	Applicability of the NIS-Directive	8
7.2	Cooperation between Member States.....	9
7.3	NIS-Strategy	11
7.4	Incident Notification.....	12
7.5	Data Protection Impact Assessment	13
8	Conclusion	14
9	Annex 1: Slides	15
10	Annex 2: Food for thought.....	34

1 Participants

Benintendi Daniele	Novareckon
Bertoncini Massimo	Engineering Ingegneria Informatica
Boubekeur Menouer	United Technologies Research Center
Bradley Ivor	Queen's University Belfast
Bracco Stefano	Agency for the Cooperation of Energy Regulators (ACER)
Costante Elisa	SecurityMatters B.V.
Daeleman Kurt	Commission de Régulation de l'Electricité et du Gaz (CREG)
Demirel Can	Biznet Bilisim
Escravana Nelson	INOV
Fichtner Laura	Delft University of Technology
Gatti Alexander	Assistent of MEP Josef Weidenholzer
Georgieva Ludmila	Austrian Chancellery
Gorts-Horlay Pierre-Emmanuel	Commission de Régulation de l'Electricité et du Gaz (CREG)
Harris John	Landis+Gyr
Holzleitner Marie-Theres	Energieinstitut an der Johannes Kepler Universität Linz
Hufnagel Sebastian	Dell
Hutle Martin	Fraunhofer Institute AISEC
Jackson Stephan	FTI Consulting
Klein Peter	Ductis GmbH
Köndorfer Petra	Austrian Institute of Technology, Digital Safety & Security
Luijff Eric	TNO innovation for life
O'Mahony Niamh	EMC Information System International
Olivera Alberto	Comisión del Mercado de las Telecomunicaciones
Paschalidis Panagiotis	P3 communications GmbH
Reichl Johannes	Energieinstitut an der Johannes Kepler Universität Linz
Sánchez Jiménez Manuel	European Commission Directorate General for Energy
Schmitt von Sydow Helmut	Professor for European Law at the University of Lausanne and at the European College of Parma
Schroers Jessica	KU Leuven CiTiP – imec
Smith Paul	Austrian Institute of Technology, Digital Safety & Security
Steinmüller Martin	ORF Österreichischer Rundfunk
Sujeet Shenoj	University of Tulsa
Szucs Laszlo	Hungarian Energy and Public Utility Regulatory Authority (MEKH)
Toftegaard Øyvind	Norwegian Water Resources and Energy Directorate
Weidenholzer Josef	Member of the European Parliament
Wolf-Petersen Erik	Energinet Denmark

2 Agenda

Session I

The first session illustrates the importance of the security of the energy system for the European Union's economic development and the wellbeing of its citizens, and introduces the topic of smart grid cyber security in this context. The urgency of a comprehensive consideration of cyber security of critical infrastructures is then demonstrated 1) through a talk giving examples of real attacks on real assets, and 2) shows the process and technical requirements of a cyber attack on a smart grid facility in a live demo.

Topic: The European Perspective on Smart Grids Security

13:00 – 13:15: Welcome and introductory statement; Josef WEIDENHOLZER (EP)

13:15 – 13:35: Targets and progress of the European Energy Cybersecurity Expert Group; Manuel SÁNCHEZ JIMÉNEZ (DG Energy)

Topic: Cyber Threats in Theory and Practise

13:35 – 14:15: Why are critical infrastructures so easy to attack? Sujeet SHENOI (Univ. of Tulsa)

14:15 – 15:00: An Introduction to smart grid cyber security and the SPARKS project; Paul SMITH (AIT), and a Live Demo on a Smart Grid facility; Ivor BRADLEY (Queen's Univ. Belfast)

Session II

The second session discusses certain important requirements that are defined in the NIS-Directive and the General Data Protection Regulation, with respect to their interpretation and implementation in light of smart grids and the energy sector.

Each of the topics selected for discussions (see below) is briefly explained, along with points that were considered the most critical in preceding consultations with stakeholders.

Participants are then asked for statements to these points in a guided discussion, collecting opinions regarding how best to implement the NIS-Directive and the General Data Protection Regulation for smart grids, identifying those discussion points for which consensus about a best practice implementation exists, and assessing which points require further attention.

Topic: Harmonization for a Secure Society

15:30 – 17:50: Aims and Scope of the discussion session; Johannes REICHL and Marie HOLZLEITNER (EI at the JKU Linz)

Guided discussion about the NIS-Directive and the GDPR

1. **Applicability**
2. **Cooperation between Member States**
3. **NIS-Strategy**
4. **Incident Notification**
5. **Data Protection Impact Assessment**

17:50 – 18:00: Wrap-up and closure of the workshop

3 Executive Summary

In order to improve traditional power grid efficiency and resilience, the smart grid initiative will transform the electricity grid. This can be achieved by capitalising on highly distributed energy sources and introducing enhanced monitoring and fine-grain control capabilities. As a result, the implementation of the smart grid concept will depend heavily on increased use of ICT systems and pervasive interconnectivity. The significantly increased level of connectivity and use of ICT systems raises concerns about the security of future smart grids especially from the perspective of cyber-attacks' risks. In response to the current challenges of the energy systems, the smart grids vision has already influenced several European directives and regulations, relevant to the smart grid implementation.

Therefore the first session of the workshop illustrated the importance of the security of the energy system for the European Union's economic development and the wellbeing of its citizens and introduced the topic of smart grid cyber security in this context. The urgency of a comprehensive consideration of critical infrastructures' cyber security was demonstrated during a discussion, providing examples of attacks on real assets. After that the mechanism and technical requirements of a cyber attack on a smart grid facility were shown in a live demo.

During the second session certain important requirements, defined in the NIS-Directive and the General Data Protection Regulation, were discussed with respect to their interpretation and implementation in the light of the smart grids and the energy sector. Each of the topics selected for discussions (see below) was briefly explained, along with the points that were considered the most critical in preceding consultations with stakeholders. Participants were then asked to make statements about these points in a guided discussion. The goals of the discussion were to collect expert opinions on the best way to implement the NIS-Directive and the General Data Protection Regulation for smart grids, to identify the discussion points for which consensus about the best practice implementation exists, and to assess which points require further attention.

4 Background of the workshop

This workshop was held in cooperation with the SPARKS Project, which receives funding from the European Union's Seventh Framework Programme for research, technological development and demonstration.

The future smart grid represents a significant evolution in the way electric grids function. At the core of this change is an increased use of ICT to implement enhanced monitoring and control in the distribution network on medium and low-voltage levels. Ensuring the cyber security and resilience of smart grids is of primary importance. This is the target of the EU-funded SPARKS – Smart Grid Protection Against Cyber Attacks – project.

The project aims to provide innovative solutions in a number of ways, including approaches to risk assessment and reference architectures for secure smart grids. The project will make recommendations regarding the future direction of smart grid security standards. Furthermore, key smart grid technologies will be investigated, such as the use of big data for security analytics in smart grids, and novel hardware-supported approaches for smart meter (gateway) authentication. All of these contributions and technologies will be assessed from a societal and economic impact perspective, and evaluated in real-world demonstrators.

The smart grid initiative will transform the traditional power grid in order to improve its efficiency and resilience. NIS Directive and GDPR have both been set into force in 2016. Member States have to implement the Directive until May 2018 into national law resp. General Data Protection Regulation shall apply from May 2018. However, both provisions are generic and not specifically made for the energy sector. Precise vision how to implement it best in the energy sector is pending.

5 Objectives of the workshop

The workshop focused on the security of the European power system, providing an opportunity for discussions about the best way to implement European regulation on the national level to foster smart grids security. Discussions encompassed the Directive on Network and Information Security (NIS-Directive) as well as the General Data Protection Regulation, while also considering ongoing work with respect to the Protection of Critical Infrastructures.

Therefore the two key objectives of the workshop were to analyse necessary national implementations of smart grid security policies and to identify potential fields for additional harmonization. Since power grids in the European Union have not yet been hit by a disruptive cyber attack, awareness and potential criticality of such an incident on the European economy and society are frequently underestimated. Therefore, the workshop also showed how cyber attackers could perform such an attack, using a live demonstration of such an attack on a smart grid facility. This live demonstration starts the attack from the premises of the workshop, showing the impact on the attacked smart grid facility via a live stream connected to the workshop premises. All the steps of executing a cyber attack were explained during the demonstration, as well as the technical prerequisites for the scenario, including the resources needed by the attackers.

6 Summary of introductory statements

6.1 Josef Weidenholzer

Josef Weidenholzer (MEP) hosted the workshop in the European Parliament.

He started the workshop by welcoming all the participants and pointed to the importance of cyber security for the EU economy and its citizens.

Now that the NIS-Directive was set into force and should be implemented in all Member States at latest in May 2018, it is clear that this provision is not directly addressing the Energy Sector.

However, it is necessary to pay attention to the Energy Sector, especially from the perspective of potential integration and creation of a common European Digital Market.

6.2 Manuel Sánchez-Jiménez

Manuel Sánchez-Jiménez is the Team Leader for Smart Grids in the European Commission, Directorate-General for Energy. He talked about the targets and progress of the European Energy Cybersecurity Expert Group.

The target of this group is to collect different expert opinions and not to propose any new legal provisions. A list of the 15 members of the EECSP Expert Group can be found here:

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341>

In order to support a correct implementation of the NIS Directive, especially in the field of energy, the Commission services are preparing a Strategy on cybersecurity for the energy sector (electricity, oil, gas, nuclear). To that effect, in December 2015 an Energy Expert Cyber Security Platform (EECSP) kicked-off to advise the Commission.

Mission of this Expert Group is to give guidance to the Commission on policy and regulatory directions at European level. Therefore, energy sector-related key points including infrastructural issues, security of supply and smart grids technologies should be addressed. The outcome and ideas of the group will be reported to the Cooperation Group which was organised due to the NIS-Directive. The EECSP Expert Group analyses existing legislation (including NIS and GDPR) and cyber security strategies related to all parts of the energy sector to identify areas, where a sectoral approach is needed. Vulnerabilities in the Energy Sector shall be pointed to and actions identified to tackle these vulnerabilities.

6.3 Sujeet Shenoj

Sujeet Shenoj is professor at university of Tulas, US and expert on Cyber-Security. He showed why critical infrastructures are so easy to attack.

According to Mr. Shenoj there are three main infrastructures : the Energy Sector, the Financial Sector and the Telecommunication Sector.

Mr. Shenoj presented 6 case studies (Bank, coal mine, pipeline, voting machine, wind farm, smart meter infrastructure).

By now there has not been a comprehensive attack on a smart meter, but according to Shenoj's opinion it is only a matter of time. Such an attack could incapacitate a comprehensive electricity grid for quite a long time.

Therefore the goals of Cyber-Security have to be: Availability, Integrity, and Confidentiality.

Unfortunately the slides for this presentation cannot be shared due to restricted content.

6.4 Paul Smith and Ivor Bradley

Paul Smith and Ivor Bradley presented a realistic multi-stage attack scenario showing how an attacker can infiltrate a power company's network and perform a man-in-the-middle (MITM) [1] attack on smart grid equipment that uses the IEC 61850 protocol. Custom attack tools, which perform the man in the middle function between power electronics equipment, controlled via the IEC61850 [2] protocol and the upstream SCADA server, have been developed. The demonstration is structurally very similar to the Ukrainian power system attacks that took place in December 2015.

The network presented in Figure 1 represents a typical energy supply company or electricity utility. There are two parts: an Admin Network and an Operational Network. The Admin Network is an enterprise class network that caters for the administration, human resources, marketing, customer support, finance and billing functions typically found in a commercial company. This is depicted as the Admin Network (subnet 101.101.1.0) in Figure 1. The initial victim of the cyber-attack will be an office worker in the power company who uses a typical office desktop PC that sits on the Admin Network.

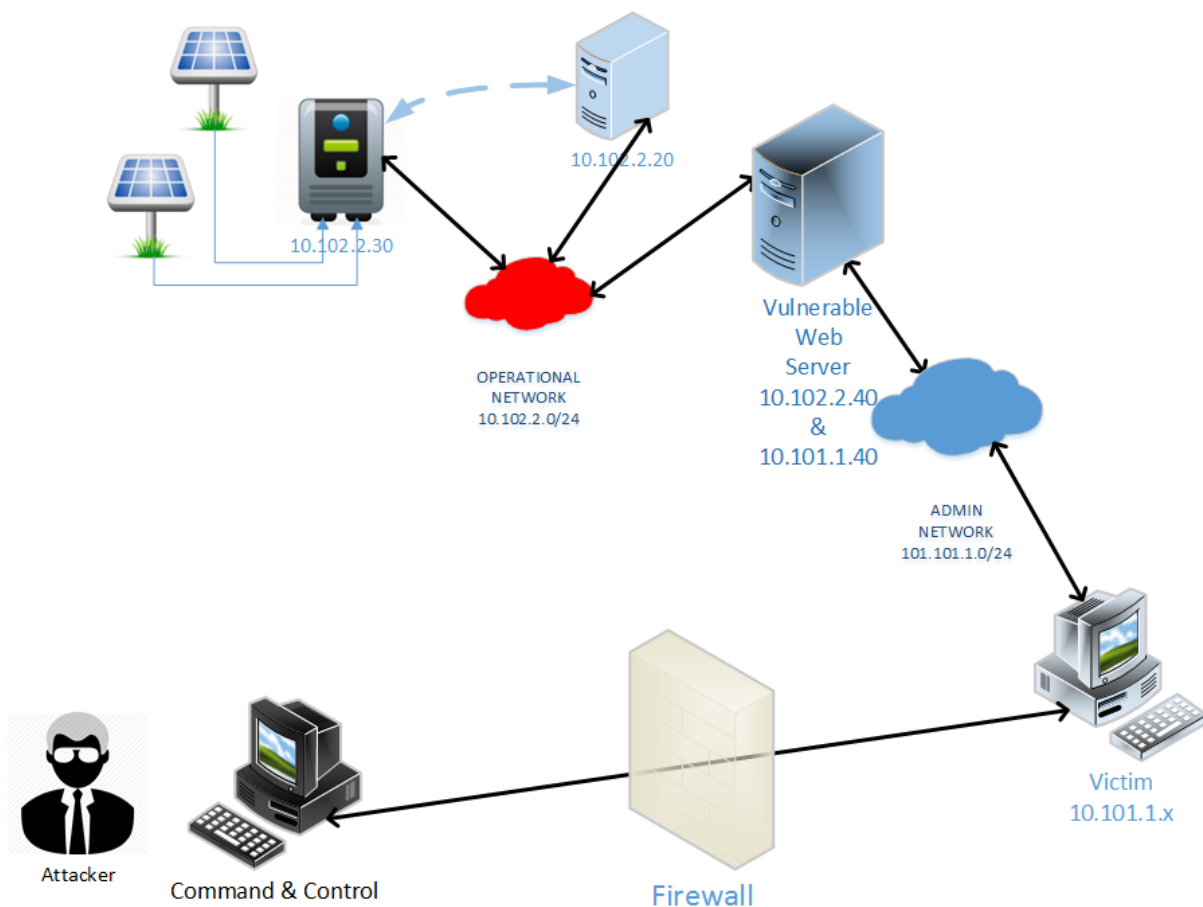


Figure 1: Network Overview

The Operational Network controls the power generation and distribution functions in the electricity grid. This is based on time critical, real-time control over the power electronics components that maintain the quality of supply to customers i.e. the voltage, phase angles, active and reactive power levels etc. The substation automation protocol commonly used for such real-time control applications is known as IEC/ISO 61850. In this scenario the IEC61850 protocol is used to control a photovoltaic inverter that sits on the Operational Network (subnet 10.102.2.0) as shown in Figure 1: Network Overview. This PV Inverter is the ultimate target of the cyber-attack.

Network separation between the Operational and Admin networks is generally enforced within energy companies. Normally a firewall device will sit between the two networks and its function is to police all communications entering the Operational Network from the less secure Admin Network. In order to reduce the length of time needed to demonstrate the attack we have decided not to include a firewall between the two network segments. Technically it is not a challenge to circumvent such a firewall and our demonstration will in fact break through a similar firewall used to protect the external facing Admin Network from potentially malicious Internet traffic (as shown in Figure 1: Network Overview).

One computer system does span both network segments. This is a customer care application that allows staff on the Admin Network to check the fault status of customer premises equipment. It is a simple homespun web application that returns readings from the Operational Network. As such it does not violate the functional separation-of-duties policy inherent in the Operational/Admin network architecture. This computer system is labelled Vulnerable Web Server in Figure 1: Network Overview.

This is the scenario presented to the attacker. This malicious actor has no direct access to staff of the company or the Operational Network. As we will show the Victim is on a separate network segment from the operational network, both protected from the wider Internet via a firewall and yet the attacker will be able to take control of the PV Inverter and cut supply to customers at will. Worse still, operations staff will be unaware that the attack is taking place.

7 Content and Results

For the second part of the workshop five aspects of the two new legal provisions, the NIS-Directive and the General Data Protection Regulation were chosen and briefly presented. After the short presentation all participants were able to express their opinion and discuss open questions.

7.1 Applicability of the NIS-Directive

Application of the NIS-Directive is mandatory for the so called *operators of essential services* and *digital service providers*. The Directive applies to seven different sectors including the energy sector, however, it does not apply to the sectors which are regulated separately in other provisions with at least equivalent requirements. Concerning digital service providers, those requirements should not apply to micro- and small enterprises. Restricting the applicability of the Directive to larger entities only is done to avoid imposing financially disproportionate burdens on these small companies.

An operator of essential services is defined as a public or a private entity which provides a service that is essential for the maintenance of critical and economic activities depending on a network and information system. Furthermore an incident would produce a significant disruptive effect¹ on such service. The decision which operators or service companies in the energy sector can exactly be considered as operators of essential services or digital service providers is to be made by each member state.

There are many actors in the smart grids environment and a successful attack on one of them can potentially lead to severe negative impact on the whole electricity system. Consequently, it is highly important that all the actors in a smart grid, including those whose vulnerability may induce risks to others, are covered by the Directive. The Directive applies to operators of essential services without further reference to the definition of “essentiality” and thereby leaving the applicability of the Directive somewhat unclear. Some EU countries may address this issue proactively and opt to provide a taxative list of obliged entities or services to avoid any ambiguity. In Austria it is

¹ Art. 5 (2) lit a-c NIS-Directive.

discussed to define a conclusive list with all operators being informed individually, which means that the list will not be published and operators of essential services will not be publicly identified. While member states are preparing such lists of entities or services, they should focus on the provision of a definition of “essentiality” in the context of the electricity system first in the authors’ opinion. A cornerstone of the definition could be the likelihood of an incident to spread to superordinate or subsequent entities. The authors therefore consider it important to include in this definition the entities that would not necessarily experience a failure of their services in case of a cyber attack themselves but provide some key input for other entities, relying on uninterrupted services along the whole value chain.

So when defining the operators of essential services their role in the electricity system should be assessed and the potential impact on other entities has to be judged. A classification of only those entities as operators of essential services, that will themselves experience the negative impact of a successful attack, may come too short in the authors’ opinion.

Regarding the second class of entities addressed in the Directive, namely digital service providers, it is quite unclear yet if there even exist any digital service providers in the smart grid environment. A digital service provider is defined as any legal person that provides a digital service including entities such as online marketplaces, online search engines, and cloud computing service providers.² Contrary to operators of essential services the definition of digital service providers in the Directive is set which means that Member States do not have to define a more detailed clarification. The Directive and all related explanations mention Google or Amazon as examples for an online marketplace or a search engine. But what about data aggregators in the smart grids environment (such as data hubs collecting all data from smart meters across different metering service providers to allow uncomplicated access to e.g. energy service companies) – would that be a cloud computing service provider which has to fall within the scope of the the Directive?

Despite the fruitful discussion there are still many questions which could not be answered during the workshop.

The issue of responsibility for the Internet of Things, which may also be connected to a grid and feed data into the energy system, causing insecurity, was also raised.

Depending on which services are classified as essential, additional challenges arise when considering that not all thereby identified operators of essential services necessarily stem from the EU. It has not yet been decided whether manufacturers and vendors of equipment for the smart grid may be obliged to the Directive. Considering the complexity and number of components installed in smart technologies, it may be hard to list all vendors and manufacturers. How can international vendors and manufacturers be identified and controlled? What if companies buy equipment from outside of Europe? Who would be responsible if an incident happens in a grid while equipment from abroad caused the incident? How secure can different components of a smart grid be? How much security can be included in a smart meter which costs 100\$ compared to one which only costs 35\$? Can the security level be charged to the customer? How can all different components of a smart meter be secured?

7.2 Cooperation between Member States

The NIS-Directive calls for establishing two new transnational institutions to foster cooperation between member states with respect to cyber security: the Cooperation Group and the Computer Security Incidence Response Team (CSIRT) Network.

On national level every Member State has to establish three Cyber Security institutions (the Competent Authority³, the Single Point of Contact, and the Computer Security Incident Response Team - CSIRT) and provide

² cf. Annex III of NIS-Directive.

³ Each Member State shall designate one or more national competent authorities.

adequate technical, financial, and human resources therefor. The three institutions⁴ are responsible for consulting, cooperating, and coordinating with the relevant law enforcement national and data protection authorities. Furthermore CSIRT's are responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector.

The CSIRTs network consists of representatives of national CSIRTs and CERT-EU⁵ as well as members of the European Commission with the role of observers. The European Union Agency for Network and Information Security (ENISA) should act as the secretariat and actively support the cooperation among the CSIRTs. This network lays down its own rules of procedure. The network of CSIRTs is intended to support trust and confidence development between the Member States and to promote undelayed and effective cooperation in case of an incident. The network's tasks include exchanging information about national incidents, providing Member States with support in addressing cross-border incidents, and exploring and identifying further forms of operational cooperation. The network of CSIRTs has had their 3rd informal meeting on the 9th of November 2016⁶, while the first formal meeting will be organised six months after the entry into force of the NIS Directive.

In addition to the operational scope of the CSIRTs network, the NIS-Directive establishes the Cooperation Group with the aim to support and facilitate strategic cooperation, to exchange information among Member States, and to develop trust and confidence. The Cooperation Group will be composed of representatives of Member States, the European Commission, and ENISA, with the European Commission acting as the secretariat.

A core topic on the Cooperation Group's agenda is to take care that the member states implement the Directive in a converging manner for all sectors and across national borders. During the first two years supporting member states in the best implementation of the NIS Directive into national law will therefore be the most important task of the Cooperation Group. A coherent approach is needed which means a minimum harmonisation with respect to security standards and respective framework conditions. However, every Member State is free to set higher standards than those required by the Directive. The Cooperation Group will examine which issues are equivalent within the sectors and which issues in the energy sector need specific considerations. Europe needs a baseline with precisely defined minimum security standards to prevent heterogeneous security levels in some countries to become a risk for the whole EU energy sector. The task of defining these minimum standards across the European Union is crucial and at the same time extraordinary challenging.

The NIS-Directive does not provide guidance whether the Cooperation Group shall be one body covering all sectors at the same level, or it shall designate sector specific sub groups, or even establish such sub groups for different subsectors. As such, the energy sector could be divided into different sub sectors (electricity, gas oil, nuclear) because of the fundamental differences of these sub sectors. While a cyber attack leading to only a very short imbalance of demand and supply may result in a pronounced outage in the electricity domain, the same incidence may be resolved without consequences for the final customers in the gas sector. However, a segregation within the Cooperation Group into "sub groups" is not yet foreseen, but will be assessed once the Cooperation Group has a clear picture of existing threats, respective developments, and potential shortcomings of the cross-sectoral approach.

In any case, the Cooperation Group has to foster security of all sectors and needs to be careful in the sense that guidelines or suggestions are equally qualified for all the sectors. The authors consider the achievement of this ambition as very challenging, due to the fundamental differences between sectors like finance, energy, and transport.

The cooperation group already had an informal meeting and has its first formal gathering planned in February 2017. This group is the first formal cooperation in the field of cyber security with representatives from all EU nations. Since the topic of cyber security is usually part of a member state's national security agenda, a

⁴ the different institutions can be designated as three different institutions but can also be combined in one.

⁵ the Computer Emergency Response Team for the EU institutions, agencies and bodies.

⁶ <https://www.enisa.europa.eu/events>.

formalised exchange of respective information and practices between nations may be considered as a great achievement, or even a game changer towards a more integrated security policy in the EU.

7.3 NIS-Strategy

The NIS-Directive requires the member states to adopt a national strategy defining specific policy and regulatory measures to achieve and maintain a certain level of network and information security. The right level has to be defined at first. According to the Directive, European or internationally accepted standards have to be used. However, specific standards have not yet been agreed on. Required measures include designating a national competent authority for information security and setting up a computer emergency response team (CERT) that is responsible for handling incidents and risks.

Member states have to develop and communicate their NIS-strategy to the Commission within three months from their adoption. The NIS-strategy has to include:

- Strategic objectives, priorities and the foreseen governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Measures for raising awareness, training and education
- Research & development plans related to the NIS-strategy
- Risk assessment plan
- List of actors involved in the strategy implementation⁷

The Directive does not demand including specific provisions for the energy sector, which means that member states have to decide if, and if so, how they include such provisions for the energy sector in their national NIS-Strategy (like concrete measures, awareness rising, ...). The Directive itself requires monitoring and reporting of measures and incidents with the objective to decrease response times to any irregularities and problems, however, it does not propose concrete measures. The responsibility to elaborate these measures, while transforming the Directive into national laws (a process that many member states have already started), lies on the member states.

Although the NIS-strategy has to be defined by each member state on a national level, an EU wide convergence of the national NIS-strategies would be favourable in the authors' opinion. An important pillar for acquiring support for the convergence of national strategies will be a high level of trust among the concerned parties from national governments and industry. An additional useful aspect within the NIS-strategy is that already existing national CSIRTs will now cooperate in a formalised way. However, the level, quality, and outcome of the cooperation will depend on the trust among members.

Beyond the level of strategic cooperation, the authors consider establishing clear and comprehensive minimum standards essential for achieving homogenous security level across the EU. However, additional to the provision of minimum standards, the provision of support and guidelines on the upgrade of existing systems (e.g. grid operators) in a cost-efficient way seems important. One of the core issues with smart grids cyber security is no different from security considerations in all other sectors: the trade-off between costs and security improvements. However, before discussions about what trade-off reflects best the needs of the EU economy and society, a common approach to "pricing" security is required along with a common way of assessing the risks of cyber attacks. It seems natural that higher levels of security are associated with higher costs for the related technology as well as higher maintenance costs of the system. Nevertheless, identifying the effect that different formulations of minimum standards will have on the remaining risks for the smart grids is an unanswered question. The authors consider a comprehensive scientific approach to developing a common methodology for assessing the risks of cyber threats, along with the effects certain measures have on these risks, as a precondition to a

⁷ cf. Art. 7 NIS-Directive.

successful development of minimum standards. Only when a common understanding of this relationship has been achieved, discussions can turn towards the aforementioned trade-off.

Member states have different levels of experiences with cyber attacks, and consequently the status of implementing legal and regulatory framework conditions differ. Therefore, less advanced member states could significantly benefit from the lessons-learned and experiences of other member states. Trust among member states and market actors will play an important role whether mutual learning can become an important source of knowledge. Therefore, it is essential to build trust to foster European harmonisation.

7.4 Incident Notification

A main aspect of the NIS- Directive is the compulsory notification about cyber incidents. Both operators of essential services and digital service providers have to promote a culture of risk management by reporting serious incidents to the respective Competent Authority or CSIRT. Digital service providers must notify incidents having a "substantial impact", whereas operators of essential services are subject to the broader-ranging requirement of notifying any incident having a "significant impact".

The Directive provides some parameters for determining such incidents more narrowly, but some uncertainties about the definition and distinction of "substantial" and "significant" impacts remain. In case of such an incident national competent authorities or CSIRT have to be notified.

In order to decide whether the incident is "significant", an operator has to take into account the number of users that are affected by the disruption of the service, the duration of the incident and the geographical spread with regard to the area affected by the incident. However, the duty to notify incidents will only apply to digital service providers if they have access to the information needed to assess the impact of an incident against the parameters referred to.⁸ The terms "significant" or "substantial" are not explained more precisely in the Directive, passing the ball to the member states that will have to find a definition ensuring that the incidents, which are actually important for fostering learning and improving the quality of responses, are notified.

Informing the public on individual incidents by the notified authority is set as an option, as it may be decided where public awareness is necessary to prevent an incident or to deal with an ongoing incident. Besides that the public is to be informed only after consultation of the concerned Operator of Essential Services. A key challenge with respect to notifying the public is to find a balance between the public interest of being notified, the perception of the public about cyber security levels in their country, and the interest of firms about the effects frequent notifications may have on their reputation. On the one hand, if every incident is reported, people will soon get careless of incident notifications. On the other hand, if very narrow criteria are set, this could lead to impactful incidents not being notified about. The guiding principle for defining which incidents need to be notified and which not should be the objectives of notifying either the public or authorities. It should be ensured that the public is notified about incidents actually having an impact on their privacy levels or their daily routines. However, notifying authorities even when an incident does not show what is usually understood as "significant" nor "substantial" impact on the operations or services of a firm may still be justified. The actual dimension of a cyber attack may be revealed only gradually, and a notification as early as possible can be decisive for its containment.

Furthermore, there is a notable overlap between the GDPR and the NIS-Directive. Both provisions require the implementation of risk-based security measures and both provisions require notifications in case of an incident, although the requirements will apply to different types of incidents. However, when a security incident involves personal data, operators have to comply with both: the NIS incident notification obligation and the GDPR personal data breach notification requirement. This means that there may be operators or providers being simultaneously subject to both the NIS Directive and the GDPR. The Regulation contains various new measures to safeguard personal data of EU data subjects⁹ and also includes significant fines and penalties for infringement. While the NIS

⁸ cf. 15 (4) NIS-Directive.

⁹ cf. Art. 4 (1) GDPR, "data subject" means an identified or identifiable natural person.

Directive covers any type of data breach in case of a service failure, the data protected under the GDPR is limited to personal data¹⁰.

Technically, an incident affecting data could therefore trigger notification obligations under both provisions. That implies, in case of an incident which involves data breach, it is possible that an operator is penalized because of missing security measures according to the NIS-Directive for service failure and according to the GDPR for data breach.

7.5 Data Protection Impact Assessment

Debates on data protection and data security in the energy sector are often emotionally charged. An essential characteristic of smart grids is the collection and processing of high quantities of sensing data and its transfer and exchange via communication networks. Data is collected on all the levels of the smart grid infrastructure including smart meters in the residential sector and SMEs¹¹, so these data collections include consumers' homes, premises of SMEs and possibly electric vehicles. Collecting detailed energy consumption data from smart grids and smart metering may induce new risks for data breaches, data losses, or data misuse on the household level, making data protection a major concern in the smart grids environment.

European legislation addresses this challenge by requiring a Data Protection Impact Assessment (DPIA) in the GDPR. The DPIA is mandatory for organisations or institutions that initiate or already manage smart grid deployments as well as those introducing changes to existing smart grid architecture platforms. A positive effect for carrying out a DPIA is that organisations are enabled to take adequate measures for reducing the identified risks (such as the risk of non-compliance, legal and operational risks) in order to reduce the potential impact of the risks on the data subject, the risk of non-compliance, legal actions, and operational risks, or to create a competitive advantage by developing common trust.¹²

Operators, that fail to conduct a DPIA or do not consult with regulators about appropriate safeguards, when high risk processing activities are identified, face fines under the new Regulation.

The DPIA is an evaluation and decision making tool intended to help entities with deciding and planning of related investments. It can reduce the risks of harm to individuals through the misuse of their personal information and it can also be useful for designing more efficient and effective processes of handling personal data.

A data protection impact assessment includes at least a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, and measures envisaged to address the risks.¹³ The supervisory authority¹⁴ shall establish and publish a list of the kind of processing operations which are subject to the requirement for a DPIA, and the supervisory authority may also establish and publish a list processing operations for which no DPIA is required.

¹⁰ cf. Art. 4 (1) GDPR, "personal data" means any information relating to an identified or identifiable natural person.

¹¹ Smart Grid Task Force 2012-14 (2014). Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems.

¹² Smart Grid Task Force 2012-14 (2014). Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems.

¹³ acc. art. 35 (z) lit a-d GDPR.

¹⁴ cf. Art. 4 (21) GDPR, 'supervisory authority' means an independent public authority which is established by a Member State.

Privacy certification schemes could be encouraged by member states to support efficient implementation of DPIA, in particular for unexperienced and small market actors. When adopted by independent service providers, these schemes can increase transparency and support trust of final electricity customers.¹⁵

Following the two years tests by the industry, mainly DSOs, the European Commission will release a DPIA template for smart grids and smart metering systems in December 2016,

8 Conclusion

In the era where the wellbeing of society and economy crucially depends on an uninterrupted electricity supply, the European Union has established a competent strategic framework to protect its citizens and business from cyber threats and attacks. EU has made a big step forward with setting into force the GDPR and the NIS-Directive. Still, the workshop was just the first step to analyse white spots resp. open questions. There is still a lot of work that has to be done. Significant responsibilities remain on the member states, which now have to decide on the national implementation of the NIS-Directive and to clarify open issues.

Resuming to the discussions throughout this article, there are three main issues requiring further attention:

- unambiguous and practicable definitions of operators and providers who have to apply the Directive are required.
- selective and practicable definitions of incidents which need to be notified are required. When exactly does the duty to notify an incident exist? How can such a significant incident be further determined? What happens after the notification?
- a definition of minimum security standards within the European Union is needed.

One of the main objectives of the NIS-Directive is fostering cooperation and information exchange between member states. Information exchange on a sensitive issue like cyber security between autonomous countries is not a standard practice. Therefore, building trust between the member states is a precondition to turn the cooperation mechanisms initiated through the Directive into an actually fruitful and impactful instrument.

Shortcomings of the Directive, such as the need for member states to provide national definitions for a number of important subjects, have to be considered in light of the NIS-Directive being the first EU-wide legislation on cyber security. Disaccord about the extent of harmonization that shall be achieved through the Directive comes natural in that respect.

Trust, cooperation, and sharing information are the key elements. Additionally, a framework for knowledge transfer from more experienced and advanced member states to less advanced has been established. Together, the NIS-Directive and GDPR will significantly increase the level of cyber security in the EU and may serve as an example for respective future cooperation beyond national boundaries, which do not exist in the borderless virtual world anyway.

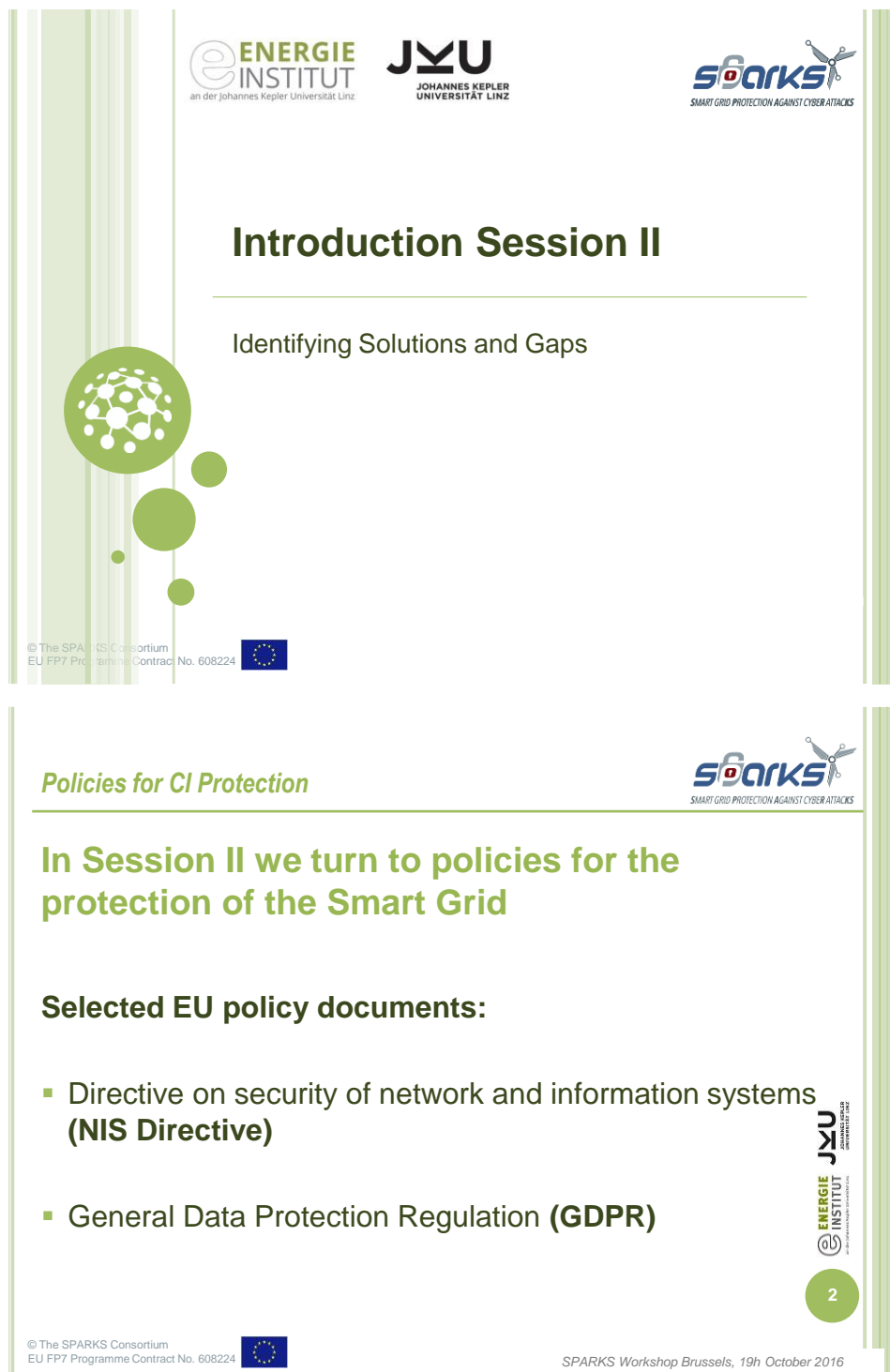
However, to reach this level of cyber security there is still much work to do, for instance to find answers to the open questions and to fill in the open gaps.

¹⁵ Expert Group 2 (2011). Recommendation to the Commission: Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection.

9 Annex 1: Slides

Subsequent Annex contents the slides of the discussion part of the workshop.

Presentation of professor Sujeet and the presentation of the cyber attack cannot be shared due to restricted content.




ENERGIE INSTITUT
an der Johannes Kepler Universität Linz

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

Introduction Session II

Identifying Solutions and Gaps

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224 

Policies for CI Protection

SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

In Session II we turn to policies for the protection of the Smart Grid


Selected EU policy documents:

- Directive on security of network and information systems (**NIS Directive**)
- General Data Protection Regulation (**GDPR**)

ENERGIE INSTITUT
an der Johannes Kepler Universität Linz

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

2

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224 

SPARKS Workshop Brussels, 19h October 2016

- **One key question related to these regulations:**

How best to implement these on the national level to comprehensively foster protection of EU **smart grids**?

- **(Some) topics with the need of further information exchange:**
 - **Applicability**
 - **Cooperation between Member States**
 - **NIS-Strategy**
 - **Incident Notification**
 - **Data Protection Impact Assessment**

Objectives for the discussion:

- Some questions for discussion have been prepared
 - Do we ask the right ones? Are some missing?
- Want to find out where consensus is already achieved (or at least close)
 - Where do we still disagree? Where do questions need solutions specific made for the energy sector?
- Are there any points where we clearly disagree?
 - Which issues may hamper a homogenous protection across all member states?

Policies for CI Protection



Expected output of the discussion:

- Opinions are summarized in a workshop report
- Draft report is sent to all participants for comments/critics
- Report will be published in full length or as a summary

Objective is to enrich ongoing discussions and help to identify gaps



5



Directive on Network and Information Security (NIS-Directive)





NAME: DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning **measures for a high common level of security of network and information systems across the Union** (NIS-Directive)

Directive (EU) 2016/1148 of 6th July 2016

Entry into force: August 2016

→ *MS have 21 months to transpose the Directive into their national laws*



7



NIS-DIRECTIVE is defined as a common provision for **ALL network and information systems**, e.g. digital infrastructure, financial market infrastructure, banking, ...

NO specific regulation for the energy sector and the smart grid environment

Can a common provision sufficiently cover the specific requirements of the Energy Sector?



8



Aim of the NIS-Directive



What is the aim of the NIS-Directive?

- ensure a high common level of network and information security (NIS)
- improving the security of the Internet and the private networks and information systems
- increase preparedness of Member States (MS)
- improve cooperation between Member States



9



Objectives of the NIS-Directive



What are the cornerstones?

1. national *NIS strategy*
2. creating a *cooperation group* to support and facilitate *strategic cooperation* and *exchange of information*
3. creating a *Computer Security Incident Response Team* (CSIRTs) to facilitate effective operational cooperation



10



Objectives of the NIS-Directive



4. security and **notification requirements** for **operators of essential services** and
5. **digital service providers**
6. **national competent authorities, single points of contact** and **CSIRTs** with tasks related to the security of networks and information systems



11



Applicability

→ Who has to apply the Directive?



12



Applicability of NIS-Directive



Different Sectors

- Energy
- Transport
- Banking
- Financial market Infrastructure
- Health
- Drinking water supply and distribution
- Digital Infrastructure

→ Operators of Essential Services

→ Digital Service Provider

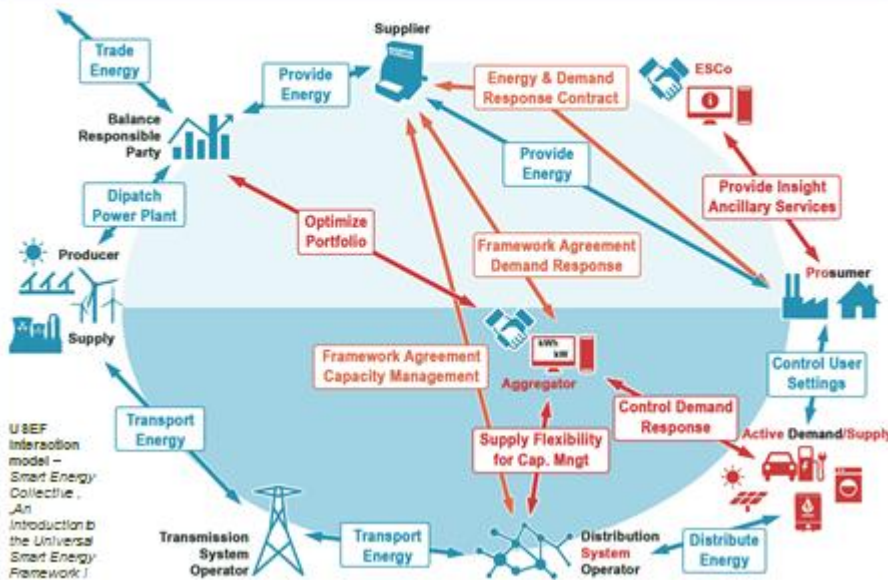
- NOT for Micro and Small DSPs
- NOT for sectors which are regulated separately (with at least equivalent requirements)



13



Applicability of NIS-Directive



Applicability of NIS-Directive



- Who is an operator of essential services in the smart grid environment resp. who is not?
- Are there any digital service providers in the smart grid environment?
- Are there missing any important entities for the European Grid
- All players of a future „European Grid“ covered?



15



Cooperation between Member States



→ Groups, Members, Tasks and
Output?



16



Cooperation Group (strategic cooperation)



- Comission, ENISA, MS
- discussing progress for Network and Information Security - best practices
- **Tasks:**
 - **work program** every 2 years with possible actions
 - **strategic guidance** for activities of CSIRTs network
 - **exchange best practice** on exchange of information, awareness rising, training, research and development, information about risks and incidents
 - discuss European **technical standards**
 - Cooperation group **may evaluate national NIS strategies**



CSIRTs Network (operational cooperation)



- National CSIRTs, CERT-EU, Commission (observer), ENISA (support)
- Build trust and confidence between MS
- **Tasks**
 - Exchange information
 - *discuss **sensitive information** related to specific incident and risks, identify a **coordinated response***
 - Discuss, explore and identify cooperation
 - Categories
 - **Early warnings**
 - Mutual assistance
 - *discuss **capabilites** and **preparedness** of a CSIRT*



Discussion: Cooperation Group



- What should be the **output of the Cooperation Group/C SIRTs Network**?
- **Which Members** should join the cooperation Group to cover the interest of the Energy Sector?
- Should there be any more **useful** or more **precise tasks**?
- How can **cross-boarder cooperations** be optimized?



19



(Inter-)National NIS-Strategy

→ Aim and Scope?



20



NIS Strategy



Aim:

Achieve and maintain high level of security of networks and information systems

Content:

- government **framework for strategic objectives** and priorities
- Measures on **preparedness, response and recovery**
- Cooperation between **public and private sector**
- Indication of education, awareness rising, training programmes and R&D plans
- **Risk assessment plan**



21



Discussion: NIS Strategy



What may be **useful strategic objectives** concerning smart grids?

Which minimum **measures** should be set in (every) MS to rise the level on

- Preparedness
- Response
- Recovery
- Cooperation of Public and Private Sector
- Awareness Rising
- Training Programs
- Education



22



Discussion: NIS Strategy EU-wide Harmonization



- **National** NIS-Strategy vs. **Cross Boarder** NIS-Strategy vs. **International (EU-)** NIS-Strategy?
- Is an **EU-wide convergence** of NIS-Strategies necessary?
 - Does it need **more harmonization** rules?
- How to compensate **different advancement within the EU?**



23



NIS-Directive



- How specific should **national** regulation be to provide faultless services of Smart Grids?
- Do we need more (specific) **EU-wide** regulation (especially for the Energy Sector) to provide faultless services of Smart Grids?



24






INCIDENT NOTIFICATION *according to NIS-DIRECTIVE*



© The SPARKS Consortium
EU FP7 Programme Contract No. 603234 

SPARKS Workshop Brussels, 19th October 2016




Incident Notification according to NIS-Directive




Significant disruptive effect – cross-sectoral factors

- Number of users
- Dependency of other sectors
- Impact on economic and societal activities or public safety (degree and duration)
- Market share
- Geographic spread
- Importance for maintaining a sufficient level
- Appropriate sector-specified factors

How do we classify an incident as **significant** in a Smart Grid environment?



© The SPARKS Consortium
EU FP7 Programme Contract No. 603234 

SPARKS Workshop Brussels, 19th October 2016

Parameters for Incident Notification



Parameters which should be taken into consideration by OoES

- Number of users affected
 - Duration of incident
 - Geographic spread
- + guidelines adopted by the national competent authorities

Parameters which should be taken into consideration by DSP

- Number of users affected
 - Duration of incident
 - Geographic spread
 - The extent of the disruption of the service
 - The impact on economic and societal activities
- + specification of the Commission by means of implementing acts.
+ only if DSP have access to the information needed to assess the impact of an incident against the parameters referred to



27



Incident Notification according to NIS-Directive



Notification to Public

- public awareness necessary to prevent an incident
- deal with an ongoing incident
- disclosure otherwise in the public interest



28



Incident Notification according to **GDPR**



Notification to supervisory authority (**General Data Protection Regulation**)

- risk to personal data
- Personal data breach is likely to risk rights and freedom of individuals
- deal with an ongoing incident
- disclosure of the incident is otherwise in the public interest



29



Incident Notification according to **GDPR**



Difference to **NIS-Directive**

- safeguard personal data
- requires controllers to adopt measures that secure personal data
- breach notification only where personal data is jeopardized
- Notification to data subjects



30



Discussion: Incident Notification



- Difference between significant (OoES) and substantial (DSP) impact?
- How to determine an incident with significant impact?
 - what is a significant impact on a smart grid?
- How should be informed? (which format - additional burden?)
- What about an early warning system?
- Who should react after an incident or an early warning?



31



Data Protection Impact Assessment - DPIA (Template for Smart Grids)



- Who, why and how to carry out a DPIA



32



Data Protection Impact Assessment
(Testing Phase of Template for Smart Grids (European Commission))



- **evaluation** and **decision-making tool**
- helps entities planning or executing investments in smart grids
- identify and anticipate **risks** to **data protection**, **privacy** and **security**



33



Data Protection Impact Assessment
How to execute a DPIA?



- Step 1 - **need** to conduct a DPIA?
- Step 2 - Initiation
- Step 3 - Identification, characterisation and **description** of smart grid systems
- Step 4 - Identification of relevant **risks**
- Step 5 - **Data protection risk assessment**
- Step 6 - Identification and **recommendation of controls** and residual risks
- Step 7 - Documentation and drafting of the DPIA Report
- Step 8 - Review and maintenance



34



Data Protection Impact Assessment How to execute a DPIA?



- Step 1 - **need** to conduct a DPIA?
- Step 2 - Initiation
- Step 3 - Identification, characterisation and **description** of smart grid systems
- Step 4 - Identification of relevant **risks**
- Step 5 - **Data protection risk assessment**
- Step 6 - Identification and **recommendation of controls** and residual risks
- Step 7 - Documentation and drafting of the DPIA Report
- Step 8 - Review and maintenance



34



Data Protection Impact Assessment (Testing Phase of Template for Smart Grids (European Commission))



- **Who** should **carry out a DPIA** - which Smart Grid Operator?
- Who may use **technologies** which are likely **risk to personal data**?
 - Transmission System Operator
 - Distribution System Operator
 - Energy Generator
 - Power Plant
 - Renewable Sources
 - Energy Market Supplier/Retailer
 - Metering Operator
 - Energy Service Company
 - Data Aggregator



35



Data Protection Impact Assessment (Testing Phase of European Commission)



- Which data protection issues may be critical when implementing smart grids?
- Who may use technologies which are likely risk to personal data?

→ DPIA Template for Smart Grid and Smart Metering Systems is **still in test phase**



36



THANK YOU FOR THE DISCUSSION



37



10 Annex 2: Food for thought

The Food for Thought paper was provided to the participants of the workshop along with the agenda two weeks prior to the event.

European Provisions for Cyber Security in the Smart Grid – An overview of the NIS-Directive¹⁶

(Marie-Theres Holzleitner and Johannes Reichl)

Introduction

Experts predict cyber-criminal activities to become a major threat for society and economy in the future if no appropriate measures are taken to counteract. Attacks and incidents may affect the integrity and transfer of personal data and business related information, and thereby potentially hampering economic development, leading to financial losses and corrupting the confidence in information and communication technology (ICT) in general. To address these concerns minimum security requirements at European Union level shall ensure the security of all communication and information systems. A joint approach to tackle the risk of cyber-attacks is the new “Directive concerning measures to ensure a high common level of network and information security across the Union” (NIS-Directive)¹⁷ that was published in the Official Journal of the EU on the 19th of July 2016¹⁸ with the ambition to increase the level of Cyber-Security within the Member States. The NIS-Directive sets new security standards designed to ensure the security of critical network and information systems in central sectors of the economy like banking, energy, health and transport. The objective of the NIS-Directive is to improve and ensure the security of the internet, private networks and information systems.

The NIS-Directive came into force on 8th of August 2016, but is not immediately applicable for Member States. Member States have 21 months to transpose the NIS-Directive into national law, which means it will be implemented by the 10th of May 2018 across the EU. So by 11th of May 2018 the Directive comes applicable for “Operators of Essential Services” and “Digital Service Providers”, which are the two addressees falling under the provisions of the Directive.

Network and Information Systems and Services play an essential role in society. Their reliability and security is necessary for many economic and societal activities, for the functioning of the internal market and to facilitate cross-border movement of goods, services and people. A network and information system is defined in the Directive as an electronic communications network. A network and information system means any device which is pursuant to a program and which performs automatic processing of digital data; including every digital data which is stored or processed, retrieved or transmitted for the purposes of their operation, use, protection and maintenance¹⁹. Network and information systems can be affected by security incidents which may be caused by human mistakes, natural events, technical failure or malicious attacks. These incidents may cause a stop of business functioning, generate substantial financial losses for the EU economy or negatively affect societal welfare. Concerning these threats it is really very important to adopt appropriate measures to secure network and information systems.

¹⁶ This project SPARKS (project-sparks.eu) has received funding from the European Unions’s Horizon 2020 research and innovation programme under the grant agreement No. 608224.

¹⁷ Directive of the European Parliament and of the council concerning measures for a high common level of security of network and information systems across the Union, Directive (EU) 2016/1148.

¹⁸ Official Journal of the EU L 2016/194/1.

¹⁹ Art. 4 (1) NIS-Directive.

So, the aim of the Directive is to ensure a high common level of network and information security, to improve the security of the internet and private network and information systems, to increase preparedness of Member States and to improve cooperation between the Member States.

The Directive defines six main objectives which have to be adopted by the Member States:

- Every Member State has to adopt a national NIS Strategy
- A cooperation group has to be created to support and facilitate strategic cooperation among Member States and to exchange information
- A Computer Security Incident Response Team network has to be created to focus operational cooperation and to work for confidence and trust between Member States
- Every Member State has to establish security and notification requirements for operators of essential services
- Every Member State has to establish security and notification requirements for digital service providers
- Every Member State has to designate three new national institutions: national competent authorities, single points of contact and Computer Security Incident Response Teams (CSIRTs). These three institutions have to be tasked with security of network and information systems.²⁰

According to a consultation on „Improving NIS in the EU²¹“ made by the Commission, it could be determined that the energy sector is the second most important service to be adopted by NIS requirements (directly after the banking and finance sector)²². Despite that the Directive is defined as a common regulation for all network and information systems, but does not specifically address the energy market nor the vital and ICT intensive subdomain thereof: the smart grid. However, considering the significant impact a disruption of energy supply would have on the economy and the society²³, a dedicated regulation may be required to comprehensively address the specific conditions of the energy market and its importance. Such specific regulation may be required as most energy networks (in particular smart grids as part of electricity distribution networks) represent natural monopolies and the level of cyber security thereof is considered a (semi-)public good. In this context, this means that consumer have no possibility to satisfy their demand through the one smart grid offering the best price-security trade-off for their individual requirements, and thereby have low power to signal their preferred security level to the responsible entities. Additional motivation for a dedicated regulating arises from the criticality of an incident: the damage costs experienced by the smart grid operator in case of an incidence may be significantly lower than those of the affected society and economy, possibly leading to biased decisions when it comes to choosing the right level of investments into a networks cyber security when left unguided through regulation.

Applicability:

The Directive applies for Operators of Essential Services and Digital Service Providers, which are defined in the next subsection. However, it does not apply for sectors which are regulated separately in other provisions with at least equivalent requirements. This could mean that the Commission has planned the future development of regulations for specific sectors, like the Energy Sector²⁴. Concerning Digital Service Providers, those requirements should not apply to micro- and small enterprises. In the author's opinion, the reason for this decision may just be that the required security measures may impose disproportionate burdens for those providers. However, if those small and micro digital service provider or any enterprise which is not listed as affected by the Directive would be part of a "future European Grid", those missing security standards could certainly cause major problems. This means that national provisions have to ensure that each enterprise connected to a grid has to follow minimum security requirements, irrespective of its size.

²⁰ Art. 1 (2) lit a-e NIS-Directive.

²¹ The online public consultation on 'Improving network and information security in the EU' ran from 23 July to 15 October 2012.

²² COM(2013), 48 final, 7.

²³ See e.g. European Commission (2016); *Schmidthaler/Reichl* (2016).

²⁴ Anyhow, there is no hint for a special regulation by now.

In any event operators or providers for whom the Directive applies, have to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use for their operations or services.

Operator of Essential Services:

An Operator of Essential Services is defined as public or private entity which provides a service that is essential for the maintenance of critical and economic activities and which depends on a network and information system. Furthermore an incident on such service would produce a significant disruptive effect.²⁵

Six months after national implementation of the NIS-Directive every Member State has to identify operators of essential services²⁶ and prepare a list of referred services²⁷. Referring to this provision in the Directive, there will be the question if every Member State will define a conclusive list with all Operators of Essential Services which has to be updated every two years?

However, identified operators of essential services have to take appropriate security measures and to notify serious incidents to the relevant national authority. Those national measures are required to significantly decrease related risks. Measures can be of technical and organisational nature and shall be appropriate and proportionate in relation to the addressed risk. It is also required to ensure security of network and information systems which means that the measures should ensure a level of security of those systems appropriate to the risks. Furthermore it should be ensured that incidents can be handled which means that measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

In the Energy Sector suppliers of electricity and gas, as well as electricity or gas distribution or transmission system operators are listed as types of operators of essential services in Annex II of the Directive. Furthermore gas storage system operators, liquefied natural gas system operators, companies responsible for the production, transmission, distribution, supply, purchase or storage of natural gas and operators of natural gas refining and treatment facilities are also considered as operators of essential services too. Likewise are operators of oil transmission pipelines and operators of oil production, refining and treatment facilities, storage and transmission categorized operators of essential services.²⁸

There are many players in the energy market in general and the smart grids environment in particular for whom it is not yet sure whether they may be identified additionally to the list as operators of essential services. Examples of such players are parties being responsible for balancing in the power grid, energy generators from renewable sources or metering operators?

Digital Service Providers

A Digital Service Provider is defined as any legal person that provides a digital service. The Directive mentions three types of Digital Services which follow the purpose of the Directive:

- Online Marketplace which means a digital service that allows consumers and/or traders to conclude online sales and service contracts
- Online Search Engine which means a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a keyword, phrase or other input and which returns links to related content
- Cloud Computing Service which means a digital service that enables access to a scalable and elastic pool of shareable computing resources²⁹.

However, a recital says that "hardware manufacturers and software developers" are not digital service providers. When examining the NIS-Directive in the context of smart grids, the question arises whether there is any Digital Service Provider in the Smart Grid environment.

²⁵ Art. 5 (2) lit a-c NIS-Directive.

²⁶ out of critical sectors as the energy sector, transport sector, banking sector, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure

²⁷ The referred list has to provide information about national measures which were used to identify an Operator of Essential Services, a list of entities which may provide such a service, the number of respective Operators identified per sector and thresholds to determine the relevant supply level in accordance with the number of users relying on that service.

²⁸ cf. Annex II Sector 1 of NIS-Directive.

²⁹ cf. Annex III of NIS-Directive.

If there would be any Digital Service Provider, it must be examined if e.g. the Data Aggregator³⁰ may be defined as Cloud Computing Service.

NIS-Strategy

Due to the lack of common requirements around Europe, minimum capabilities are needed. In the introductory Chapter 0 it has already been mentioned that every Member State has to adopt a national NIS-Strategy with the aim to achieve and maintain a high level of security of network and information systems.

This strategy has to include:

- Strategic objectives, priorities and governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Awareness raising, training and education
- Research & development plans related to NIS Strategy
- Risk assessment plan
- List of actors involved in the strategy implementation

Art. 7 requires the adoption a national NIS-Strategy but does not include special provisions for the energy sector which means that Member States have to decide on their own how and how much they include provisions (measures, cooperation methods, ...) for the energy sector in the national NIS-Strategy.

It will be interesting if Member States establish concrete measures in their strategies and if general measures will be set or measures defined for each sector. There is also to be decided by each Member State if the strategy should only have a national view to Cyber Security, a Cross Border view or even an international view. European Commission will also have to struggle cope with the difference advancements within the different Member States. According to these points ambitions in national NIS-Strategy may differ among the Member States.

National Institutions

Every Member State has to establish three Cyber Security institutions and provide adequate technical, financial and human resources therefor. The three institutions (the Competent Authority, the Single Point of Contact, and the Computer Security Incident Response Team - CSIRT) are responsible for consulting, cooperating, and coordinating with the relevant law enforcement national authorities and data protection authorities. Member States may request help and assistance of the European Union Agency for Network and Information Security (ENISA).

Competent Authority and Single Point of Contact

Member States have to designate one or more national competent authorities to monitor the application of the Directive at national level. The Competent Authority is to be notified in case of an incident.³¹ After fixing one or more national competent authorities, the designation has to be made public in every Member State. In relation to the Energy Sector and the Smart Grid, it may be useful to designate one Competent Authority for each sector which would be in line with the Directive.

Member States will also designate a single point of contact, which will exercise a liaison function to ensure cross-border cooperation. In case of an incident which may also affect other Member States the Single Point of Contact is responsible to notify the other affected Member States. The single point of contact will also submit a yearly report on received notifications to the Cooperation Group (see Chapter 0; the report shall include the number of notifications, the nature of each incident, the type of the respective security breach, seriousness / duration and action taken). Competent Authority resp. CSIRT will provide necessary information therefor.

³⁰ means any party that provides Data Aggregation services to electricity Suppliers They aggregate data to be submitted into Settlements so that accurate values of what a Supplier's customers have "taken" is allocated to the correct Supplier to enable the accurate billing of that Supplier for the energy their customers have used (source: <http://www.tma.co.uk/services/data-aggregation/> from 20.09.2016).

³¹ cf. Art. 8, par. 6 NIS-Directive

Computer Security Incident Response Team

Member States will designate one or more Computer Security Incident Response Teams which may be settled within the Competent Authority. There may be established multiple CSIRTs (for each sector). CSIRT's are responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector. High availability of communications services by avoiding single points of failure shall be insured and therefore appropriate, secure and resilient communication and information infrastructure at national level is to be ensured for CSIRTs. Additionally CSIRTs have to promote adoption and use of common or standardised practices for incident handling and risk-handling procedures as well as incident, risk and information classification schemes.

Concrete tasks of CSIRTs have to be clearly defined and supported by national policy. A definition who should define the tasks of CSIRTs is missing in the Directive. As the Directive suggests that the CSIRT is established within the Competent Authority and also that assistance of ENISA may be requested, it may be standing to reason that a Member State delegates this task to Members of CSIRTs themselves in consultation with Competent Authority.

CSIRTs may also be informed in case of an incident. The one who detects the incident may decide whether to inform the Competent Authority or the CSIRT. CSIRTs have to be an effective, efficient and secure cooperation part of the transnational CSIRTs network (described below).

Transnational Networks

There are also established two new transnational institutions: Cooperation Group and CSIRTs Network.

Objective of the Cooperation Group is to support and facilitate strategic cooperation between Member States and to exchange information. The Cooperation Group will be composed of representatives of Member States, the Commission and ENISA. It is not defined which persons of a Member State should be participating in the Cooperation Group. In the author's opinion, it may be helpful if each sector is represented in the Cooperation Group through a dedicated expert, but this fact is not defined. The choice lies with national implementation of the Member States. The Cooperation Group will constitute in February 2017.³²

Furthermore, the NIS Directive establishes a network of CSIRTs, in which a representative from each Member State must participate. The network's tasks include exchanging information about security incidents, providing Member States with support in addressing cross-border incidents, and exploring and identifying further forms of operational cooperation. Aim of the CSIRTs Network is to develop trust and confidence between the Member States and to promote undelayed and effective cooperation. CSIRTs Network consists of representatives of national CSIRTs and CERT-EU³³ as well as members of the Commission with the role of an observer. ENISA should act as secretariat and actively support the cooperation among the CSIRTs. This network lays down its own rules of procedure.

These two transnational institutions do not have any power to set compulsive measures for Member States. They can only prepare proposals in their report to the Commission. So these groups rep. networks only have exchanging character and may only make suggestions to compulsive institutions.

Incident Notification

One main aspect of the NIS- Directive is the compulsory notification of Cyber incidents. Both Operators of Essential Services and Digital Service Providers have to ensure the security of their networks and systems to promote a culture of risk management and ensure that serious incidents are reported to Competent Authority or CSIRT, but Digital Service Providers have less strict provisions.

For Operators of Essential Services

Operators of Essential Services will have to notify National Competent Authorities or CSIRT whenever there is a "significant" impact on the provision of the operator's service. The "significance" is not defined precisely in the Directive, but there are a few parameters that can be used for determining the incident. For the decision whether

³² European Commission - Fact Sheet "Directive on Security of Network and Information Systems" Brussels, 6 July 2016

³³ the Computer Emergency Response Team for the EU institutions, agencies and bodies

an incident is significant or not an Operator of Essential Services has to take into account the number of users that are affected by the disruption of the service, the duration of the incident and the geographical spread with regard to the area affected by the incident. Furthermore they have to balance how critical the incident is for society and economy.

If the incident has significant impact on the continuity of the essential service other affected Member States are to be informed without undue delay. The Decision whether the other Member State is to be informed or not is to be taken by the Competent Authority of the respective national CSIRT³⁴. The operator's security, commercial interest and confidentiality of the provided information shall be preserved. Informing the public on individual incidents by the notified authority is set as an option as it may be decided where public awareness is necessary to prevent an incident or to deal with ongoing incident. Despite that public is to be informed only after consultation of the concerned Operator of Essential Services.

For Digital Service Providers

Digital service providers will be required to notify incidents that have a "substantial" impact on the provision of a service they offer in the EU without undue delay. The "substantiality" of an incident will be determined by relevant factors which are quite the same criteria as for Operators of Essential Services. In addition to those factors the extent of the disruption of the functioning of the service and the extent of the impact on economic and societal activities are taken into account. However, the duty to notify incidents will only apply to digital service providers if they have access to the information needed to assess the impact of an incident against the parameters referred to.³⁵

Notification to other Member States by Competent Authority or CSIRT is particularly deemed appropriate where the incident concerns two or more Member States.

In any case, security and commercial interests of the Digital Service Provider and the confidentiality of the information provided should be preserved. An obligation to inform the public is foreseen as well where public awareness is necessary to prevent an incident or to deal with an ongoing incident. What differs from requirements applicable to operators of essential services is that informing the public may be decided where disclosure of the incident is otherwise in the public interest. Information can be done not only by the national Competent Authority or CSIRT but also, where appropriate, by the authorities or CSIRTs of other Member States concerned and even by the Digital Service Provider itself if so required. Before informing the public, Digital Service Providers have to be consulted.

Under the Directive, Member States will also be required to implement and enforce penalties against critical infrastructure providers that fail to comply with the Directive's requirement

The scope of such a contractual notification obligation and the mentioned parameters need to be further defined by each Member State in order to be practically usable. A number of questions rise up in context of incident notification, especially for the energy sector: each Member State will have to determine what is a significant impact on a smart grid? What is the preferred format of the information? When is criticality of an incident justifying information of the public – in case of a blackout, data theft or technical failure? What is the difference between a significant³⁶ or a substantial³⁷ impact? Furthermore, what is a significant impact on a smart grid with impact on the continuity of essential services of another Member State? Where to draw the line between commercial interest and confidentiality of an operator and the interest of public in being informed? When is public awareness necessary to prevent an incident? How can the state of the art be ensured, validated and maintained?

³⁴ the one who receives the notification

³⁵ cf. 15 (4) NIS-Directive

³⁶ For Operators of Essential Services

³⁷ For Digital Service Providers

Conclusions

The NIS Directive introduces provisions to achieve an improved level of harmonisation across Member States, but it is not yet clear how it will be implemented into national laws of the Member States. It will be seen if Member States introduce new laws dealing especially with the requirements of the NIS Directive or if Member States will include the required security regulations into existing laws.

Based on many unanswered questions around the NIS Directive, Member States have to take important decisions when implementing the Directive into national law. There have to be found appropriate regulations for the different sectors and established different sector-based institutions in each Member State. According to different advancement in several Member States differing legal provisions are required in each Member State. Those provisions should be able to set the same security standard in all Member States to finally reach the goal of harmonisation within the European Union.

Literature

European Commission (2016): Commission Staff Working Document - Impact Assessment, Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council concerning measures to safeguard security of gas supply and repealing Council Regulation 994/2010". SWD(2016) 25.

European Commission (2013): Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union. COM(2013), 48 final

European Commission (2016): Fact Sheet "Directive on Security of Network and Information Systems".

Schmidthaler, M., Reichl, J. (2016): Assessing the socio-economic effects of power outages ad hoc. Computer Science-Research and Development, 31, 157.