NIS-Directive and Smart Grids

Workshop on European Smart Grid Cybersecurity: Emerging Threats and Countermeasures

Marie Holzleitner

EU FP7 Programme Contract No. 608224

Table of Content

SMART GRID PROTECTION AGAINST CYBER ATTACKS

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*

EU FP7 Programme Contract No. 608224

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?

EU FP7 Programme Contract No. 608224

AIM
of NIS-DIRECTIVE

EU FP7 Programme Contract No. 608224

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

EU FP7 Programme Contract No. 608224

OBJECTIVES

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

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

EU FP7 Programme Contract No. 608224

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

EU FP7 Programme Contract No. 608224

AFFECTED PARTIES

EU FP7 Programme Contract No. 608224

For whom does the NIS Directive apply?

- Operator of essential services
- Digital Service Provider

→ no application if “certain” provisions (with at least equivalent requirements) apply instead of the respective NIS Directive Directive not applicable:

→ not for Micro and Small Enterprises

→ not for sectors which are regulated separately (with at least equivalent requirements)

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Operator of essential services

- 6 months after implementation of MS to identify operators of essential services
- public or private entity with an important role for the society and economy
- have to take appropriate security measures and to notify serious incidents to the relevant national authority

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Operator of essential services

- applies to operators of essential services in the following critical sectors:

  - → **Energy: electricity, oil and gas**
  - → Transport: air, rail, water and road
  - → Banking: credit institutions
  - → Financial market infrastructures: trading venues, central counterparties
  - → Health: healthcare settings
  - → Water: drinking water supply and distribution
  - → Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries

EU FP7 Programme Contract No. 608224

Operator of essential services

- Requirement
  - National Measures
    - Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
    - Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
    - Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Operator of essential services

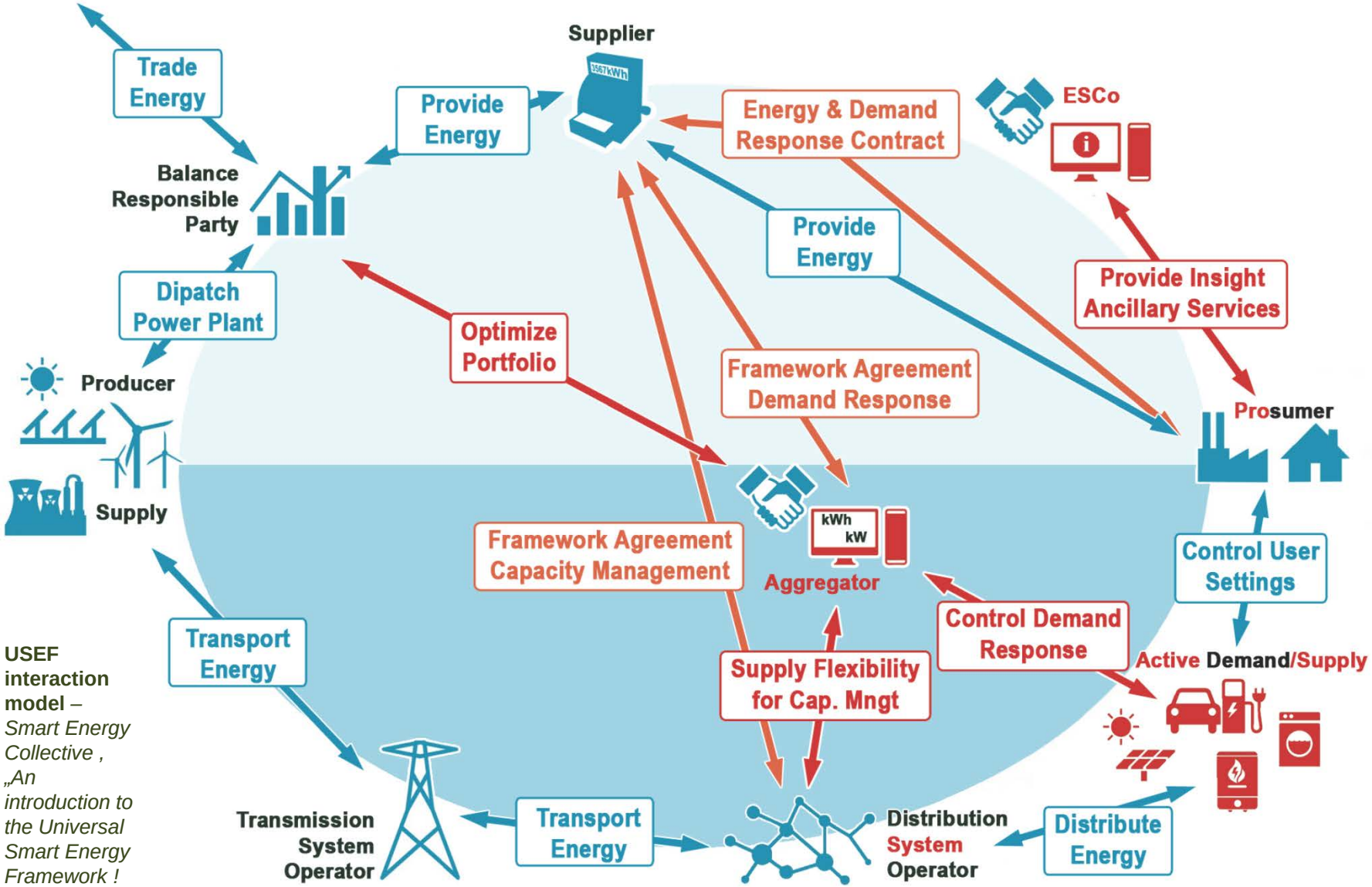
- Identification of OoES
  - Entities providing service which is essential for the maintance of critical societal/economic activities
  - provision of that service depends on network and information systems
  - security incident would have significant disruptive effects on the provision of the essential service

Which entities in the Smart Grid Environment need to be considered ?

EU FP7 Programme Contract No. 608224

Applicability of NIS-Directive

SMART GRID PROTECTION AGAINST CYBER ATTACKS



USEF interaction model – *Smart Energy Collective , „An introduction to the Universal Smart Energy Framework !*

Digital Service Provider (DSP)

- means any legal person that provides a digital service
- Types of DSPs for purposes of NIS-Directive
  - Online Marketplace
  - Online Search Engine
  - Cloud Computing Service

Is there any relevant Digital Service Provider in the Smart Grid Environment?

NATIONAL EFFORTS & INSTITUTIONS

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

NIS Strategy

Each MS has to adopt a National NIS Strategy

- 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

communicated to Commission within 3 months from their adoption

EU FP7 Programme Contract No. 608224

NIS Strategy

Each MS has to adopt a National NIS Strategy

- 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

What do we expect from the NIS-Strategies to promote security in the Energy Sector?

EU FP7 Programme Contract No. 608224

Which compulsory institutions does every Member State have to establish?

- Competent Authority
- Single Point of Contact
- Computer Security Incident Response Team (CSIRT)

Competent Authority

- **Monitors** application of NIS Directive **at national level**
- Is **to be notified in case of an incident** (or CSIRT)

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Single Point of Contact

- **liaison function to ensure cross-border cooperation** of MS authorities

- anonymized **summary report** to Cooperation Group about received notifications

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Computer Security Incident Response Team (CSIRT)

- **handling incidents and risks** according to a defined process - responding to incidents
- ensure **high availability of communications services** by avoiding single points of failure
- **Monitoring** incidents at a national level
- **Providing early warning, alerts, announcements and dissemination of information**

EU FP7 Programme Contract No. 608224

- Competent Authority
- Single Point of Contact
- Computer Security Incident Response Team (CSIRT)

How to ensure that the specific needs of the Energy Sector are covered?

TRANSNATIONAL NETWORKS

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Cooperation Group

Aim

- support and facilitate strategic cooperation among MS
- share information about best practices

Composition

- Members of Commission, ENISA and MS
- Biennial workprogramme

Output

- report assessing gained experience with strategic cooperation every 1,5 years

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

CSIRTs network

Aim

- confidence and trust between MS
- swift and effective operational cooperation

Composition

- National CSIRTs, CERT-EU, Commission (*observer*), ENISA (*support*)

Output

- report assessing gained experience with operational cooperation every 1,5 years

EU FP7 Programme Contract No. 608224

- Cooperation Group
- CSIRTs Network

What should be the specific tasks of these transnational networks?

EU FP7 Programme Contract No. 608224

INCIDENT NOTIFICATION *according to NIS-DIRECTIVE*

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Significant disruptive effect – cross-sectoral factors

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

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

EU FP7 Programme Contract No. 608224

Parameters which should be taken into consideration by OoES

- Number of users affected
- Duration of incident
- Geographic spread

These parameters may be further clarified by means of guidelines adopted by the national competent authorities acting together within the Cooperation Group.

EU FP7 Programme Contract No. 608224

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 sociatal activities

These parameters will be further specified by the Commission by means of implementing acts.

EU FP7 Programme Contract No. 608224

Notification to Public

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

EU FP7 Programme Contract No. 608224

INCIDENT NOTIFICATION according to *GENERAL DATA PROTECTION REGULATION (GDPR)*

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

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

EU FP7 Programme Contract No. 608224

INCIDENT NOTIFICATION

SUMMARY

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Focus:

NIS Directive: focused on **network security** to **improve security** of the Internet and private networks and information systems

GDPR: safeguard **personal data**

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Requirement:

NIS Directive: requires operators to appropriately **secure their networks** to **protect** the **provision** of the service

***GDPR*:** requires controllers to adopt **measures** that **secure personal data**

SMART GRID PROTECTION AGAINST CYBER ATTACKS

What incidents require notification?

NIS Directive: breach notification required **if significant disruption** to provision

GDPR: breach notification only where **personal data is jeopardized**

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Whom to notify?

NIS Directive: Notification to **competent authority**

GDPR: Notification to **data subjects**

EU FP7 Programme Contract No. 608224

INVITATION

- Workshop on **Security Requirements for Smart Grids:** Economic, legal and societal aspects
- On **19th of October 2016 in the European Parliament, Brussels**
- Attendees of EP, Comission, ENISA, ACER, …

THANK YOU FOR YOUR ATTENTION

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Energieinstitut an der Johannes Kepler Universität Linz

Altenberger Straße 69

4040 Linz, AUSTRIA

Tel: +43 723 2468 5675

Fax: + 43 723 2468 5651

e-mail: holzleitner@energieinstitut-linz.at

Marie-Theres Holzleitner

holzleitner@energieinstitut-linz.at

EU FP7 Programme Contract No. 608224