SMART GRIDS TASK FORCE - EXPERT GROUP 2 - CYBERSECURITY

2nd Interim Report

Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity.

July 2018

The mission of the Smart Grid Task Force Expert Group 2 on cybersecurity is to prepare the ground for a Network Code on cybersecurity for the electricity subsector.

1. Contents

1. Introduction 3
1.1 Context 3
1.2 1st Interim Report 3
1.3 Acknowledgements 3
1.4 Disclaimer 3
2. Symbols and Abbreviations 4
3. Executive Summary 5
4. Brief Summary of the First Interim Report 8
4.1 Analysis and Implementation Approach 8
4.2 Objectives and Key Areas for the Network Code on Cybersecurity 8
5.1 Recommended Structure for the Network Code 10
5.2 Proposed Components of the Network Code for Cybersecurity 11
6. Conclusion & Outlook 13
7. Annex 14
7.1 Annex A-1: Smart Grids Task Force – Expert Group – Working Group on Cybersecurity 14
7.2 Annex A-2: Editorial Team 15
7.3 Annex A-3: Working Groups on Key Areas Identified 16

1. Introduction

1.1 Context

The Commission Proposal "Clean Energy for all Europeans" of 30th November 2016 (currently under negotiations with the Council and the Parliament) acknowledges the importance of cybersecurity for the energy sector, and the need to duly assess cyber-risks and their possible impact on the security of supply. In particular, the draft 'Electricity Regulation' (recast)[1] proposes the adoption to technical rules for electricity via a Network Code on cybersecurity rules.

The working group on cybersecurity originated from the Commission Communication 'Clean Energy for All Europeans' (COM/2016/0860 final) announcing the set-up of such a group in spring 2017 and the delivery of final results by end 2018. This Communication emphasizes that ensuring resilience of the energy supply systems against cyber risk and threats becomes increasingly important as wide-spread use of information and communications technology and data traffic is becoming the foundation for the functioning of infrastructures underlying the energy systems.

Thus as a direct action, the European Commission established in spring 2017 stakeholder working groups under the Smart Grids Task Force to prepare the ground for Network Codes on demand response, energy-specific cybersecurity and common consumer's data format with the focus on the electricity subsector.

1.2 1st Interim Report

In December 2017, the SGTF EG2 has published the first interim report that gave insight into the approach to prepare the ground for a Network Code on cybersecurity for the electricity subsector. The 1st interim report has provided the objectives for a Network Code on cybersecurity and has identified four key areas recommended to be addressed.

This report will not reiterate the content of the 1st interim report but will provide further context on the work in progress.

1.3 Acknowledgements

This interim report has been prepared by the Smart Grid Task Force - Expert Group 2 (SGTF EG2) and is a product of intensive work and discussions of the editorial team (see chapter 7.2, Annex A-2) and respective working groups (see chapter 7.3, Annex A-3) with contributions of the nominated experts of the SGTF EG2 (see chapter 7.1, Annex A-1).

1.4 Disclaimer

[1] COM/2016/0861 final/2 - 2016/0379 (COD)

2. Symbols and Abbreviations

The following symbols and abbreviations are used in the report:

- **CERT** Computer Emergency Response Team
- **CSIRT** Computer Security Incident Response Team
- **DSO** Distribution System Operator
- **EC** European Commission
- **EECSP** Energy Expert Cyber Security Platform
- **EU** European Union
- **GDPR** General Data Protection Regulation
- **IEC** International Electrotechnical Commission
- **IT** Information Technology
- **NIS** Network Information Security
- **OT** Operational Technology
- **SCRM** Supply Chain Risk Management
- **SGTF EG2** Smart Grid Task Force Expert Group 2
- **TSO** Transmission System Operator

3. Executive Summary

The energy infrastructure is inarguably one of the most complex and most critical infrastructures of a modern digital society that serves as the backbone for its economic activities and for its security. It is therefore in the interest of the European Union and its Member States to secure the energy infrastructure against cyber risks and threats.

In the European Union, one of the key legislation in this regards is the NIS Directive[2] and its implementation at Member State level is a key element. The NIS Directive and the GDPR[3] regulation as a baseline for all sectors, including the energy sector. The intent of this Network Code is to address energy sector specific challenges and gaps as identified in the analysis done at the European Commission[4] by holistically addressing cybersecurity covering people, practices and infrastructure. A risk-based approach must be, as in other sectors, a guiding principle also for the energy sector. Consequently, cybersecurity is not going to be addressed with ad-hoc recommendations, but with a recommendation on legislative targets aiming to help in managing cybersecurity in a sectorial context, but still at European level, and which can assure a smooth and coherent implementation.

Specific obligations are already impacting the energy sector by the NIS Directive such as:

1. The NIS Directive addresses a number of general needs in regard to cybersecurity for the energy sector and will allow the establishment of specific Computer Security Incident Response Team (CSIRT) at Member State level;

2. The identification of operators of essential services that includes energy operators. Energy operators will have to implement appropriate security measures with principles that are general to all sectors;

3. The operators of essential services will have the obligation to notify serious incidents to the relevant National Competent Authority.

The Network Code, in addition to what is already set as compulsory under the NIS Directive, could add the following topics not specified in the NIS Directive and which would better be scoped by an energy specific secondary legislation:

- The definition of a minimum and more ambitious level of cybersecurity for the energy sector with specific measures that will cover aspects of operational technology for energy infrastructures and operation of energy systems those are typical for the energy sector. Furthermore, it will address the need for close cooperation among energy operators and energy sector specific methodologies.

- It will require specific energy expert subgroup(s) which, under the NIS-transnational CSIRTs, will allow to foster the communication among operators, and to prevent the rapid propagation of threats in such critical sector. Furthermore, it allows to effectively providing rapid report back to the network of CSIRTs.

[2] Directive (EU) 2016/1148
[3] Regulation (EU) 2016/679
[4] EECSP-Report: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

- It will further specify the responsibilities and specific information/notification flows regarding anomalies linked to potential cybersecurity threats among operators of essential services within the energy sector, which would eventually allow a fast detection and response of unknown threats.

- It will introduce a methodology to analyse risks in large scale interconnected and interdependent energy networks and infrastructures, which, in this context, will allow to assess and to mitigate risks, as well as to prepare up front response scenarios on the potential impact of complex and rapidly spreading threats to the existing interconnections and of the possible cascading effects.

Finally, the implementation of a network code on cybersecurity could provide the following unique components specifically tailored for the essential and specific cybersecurity needs of the energy sector:

Set-up of an early warning system in Europe for the energy sector
Following the already existing implementation of the NIS Directive in the Member States, respective set-up could be extended to have an operational function in supporting operators of energy infrastructure protecting energy systems by implementing a multiplier and competence center that provides information on potential cyber-attacks and threats.

Cross-border and cross-organizational risk management in the EU
Respectively ENTSO-E together with EU-DSO[5] will be managing cross-border and cross-organizational risk of interconnected, interdependent energy systems, infrastructures and applications.

Minimum Security Requirements for critical infrastructure components
Respectively ENTSO-E together with EU-DSO will orchestrate within the group of selected stakeholders minimum security requirements for infrastructure components and services that are critical to secure the energy infrastructure. The methodology will be aligned with the proposed EU Cybersecurity Act[6].

Minimum Protection Level for energy system operators
A methodology to define a minimum protection level for energy system including requirements for organization, practices and infrastructure will be recommended in order to set a baseline security level within the EU. The recommendation will include minimum requirements in regards of supply chain management.

European Energy Cybersecurity Maturity Framework for Operator of Essential Services
Recommendation towards and a European energy cybersecurity maturity framework will be provided in order to have a metric for energy system operators and Member States available to measure and steer the protection and resilience of critical infrastructure in the energy sector. The

[5] Depending on the outcome of the negotiations of the "Clean Energy for all Europeans" package, and once established, the EU-DSO entity shall take over for the DSOs. See the Commission proposal: Article 49 ff, http://eur-lex.europa.eu/resource.html?uri=cellar:9b9d9035-fa9e-11e6-8a35-01aa75ed71a1.0012.02/DOC_1&format=PDF
[6] COM(2017) 477

recommendation will consider security measures[7] that has been provided as guidance by the NIS Cooperation Group.

Supply Chain Risk Management for Operator of Essential Services

Recommendation towards a supply chain risk management process specific for the energy sector will be provided in order to have a methodology available for operator of essential services in order to address supply chain risk.

Please note that all components presented are subject to change due to ongoing discussions in the working groups of the SGTF EG2 and will be concluded in the final report in end of 2018.

[7] http://ec.europa.eu/information_society/newsroom/image/document/2018-24/reference_document_security_measures_oes_1B549F1B-9144-40B4-AFC2A5441E087584_52944.pdf

4. Brief Summary of the First Interim Report

The mission of the Smart Grid Task Force Expert Group 2 (SGTF EG2) is to prepare the ground for a network code on cybersecurity for the electricity subsector, i.e. for electricity system operators of transmission (TSO) and distribution (DSO) networks. Generation is not included, but connected infrastructure and service providers might be indirectly affected by requirements derived when the Network Code is implemented. The subsector oil and gas is not explicitly excluded, i.e. recommendation provided to the electricity subsector might be considered for oil and gas, too.

The guiding principle remains unchanged, i.e. the recommendation on a Network Code shall follow a risk-based approach and the implementation of measures shall be auditable. The recommendations in this report will consider existing EU legislations such as the Directive on security of Network and Information Systems (NIS)[8] and the General Data Protection Regulation (GDPR)[9] and their ongoing implementations as a baseline for building all pillars of the Network Code.

The following section gives an update on the approach.

4.1 Analysis and Implementation Approach

The analysis approach agreed with the SGTF EG2 and performed by the editorial team is shown in Figure 1. The figure shows the work that has been achieved and the work that is in progress in order to complete the mission of the SGTF EG2 by end of 2018.

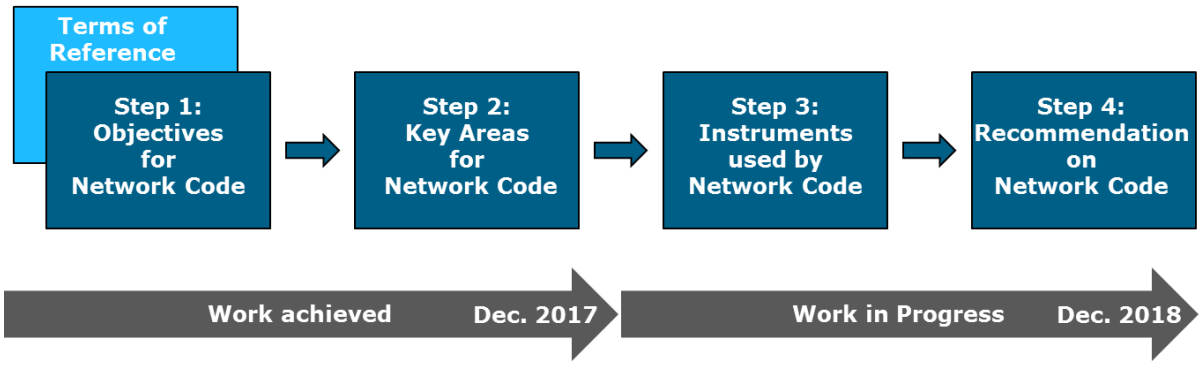

Figure 1: Overview of the analysis and implementation approach

A detailed explanation about the approach and the results of step 1 and step 2 can be found in the 1st interim report[10]. Current focus of the SGTF EG2 is on step 3 and 4; a status update on the work in progress will be provided in his report.

The risk scenarios explicitly listed in the 1st interim report are now part of the risk methodology discussion, see chapter 5.2, and not listed separately anymore.

4.2 Objectives and Key Areas for the Network Code on Cybersecurity

The objectives and key areas identified for the Network Code on cybersecurity are listed in Figure 2. The key areas for the network code are addressing these objectives.

[8] Directive (EU) 2016/1148
[9] Regulation (EU) 2016/679
[10] https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf

The key area '**European Energy Cybersecurity Maturity Framework'** targets to provide an instrument to the electricity system operators in order to steer the cybersecurity implementation.

The key area '**Supply Chain Management'** targets to create trust and transparency in products, systems and services provided by vendors and service providers.

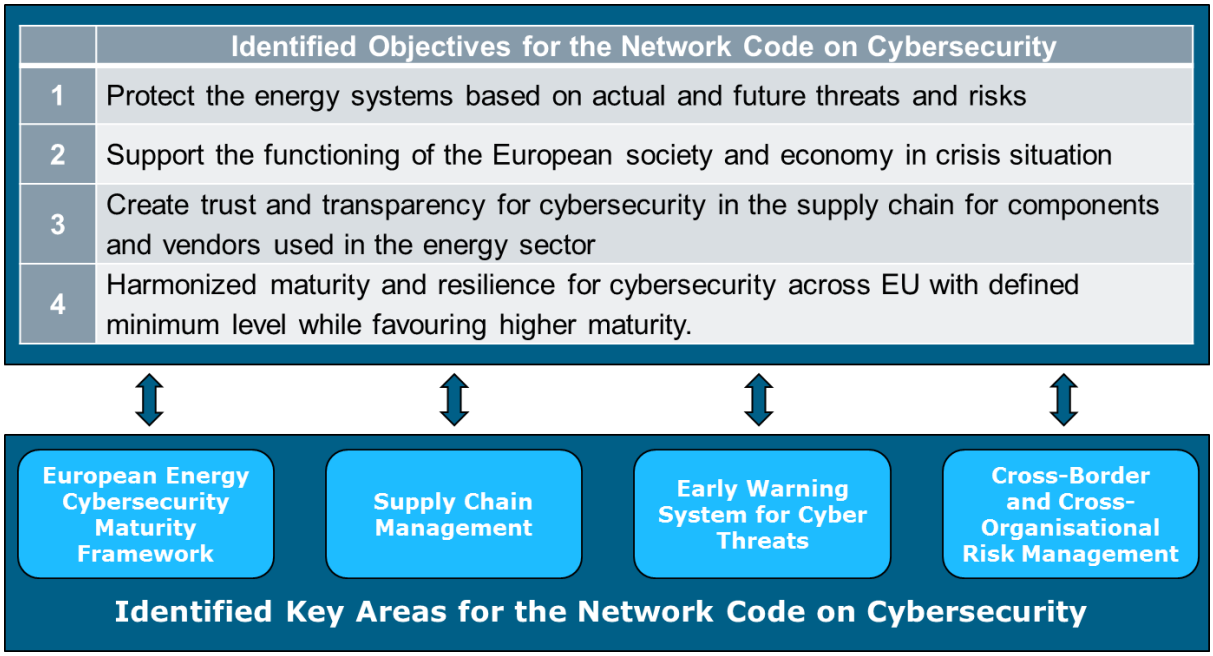

Figure 2: Objectives and Key Areas for the Network Code on Cybersecurity

A '**Early Warning System for Cyber Threats'** is a key area that targets to extend the existing incident reporting mechanism as defined in the NIS Directive towards an information sharing system that dramatically reduces the response times on cyber threats and risks by providing early indicators of attacks and compromises.

The energy grid in the EU is interconnected and interdependent with an increasing number of market players participating in the energy value chain. The key area '**Cross-Border and Cross-Organisational Risk Management'** targets to provide a methodology that helps understanding and mitigating risks in a changing environment of the electricity infrastructures. A key part of risk management will be the definition of risk thresholds and extreme risk scenarios that can, when occur, cause emergency incident situations for the European grid[11].

[11] https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/2014_ICS_Methodology.pdf

5. Proposal for a Network Code on Cybersecurity

In order to further elaborate on the identified key areas, the SGTF EG2 has set-up expert working groups for each key area; nominated experts are listed in chapter 7.3, Annex A.3.

The following sections provide first results of the discussions in the working groups. Please note that the presented results are still subject to change due to ongoing discussions in the working groups of the SGTF EG2 and will be concluded in the final report scheduled for end of 2018.

5.1 Recommended Structure for the Network Code

Recommendation for the Network Code follows the guiding principles, see chapter 4, i.e. it follows a risk-based approach. As a Network Code will apply to all operators, it requires a differentiation between operators and operators that are identified as operators of essential services (OES). Figure 3 shows the recommended structure of the Network Code that is in discussion with the experts in the working stream.

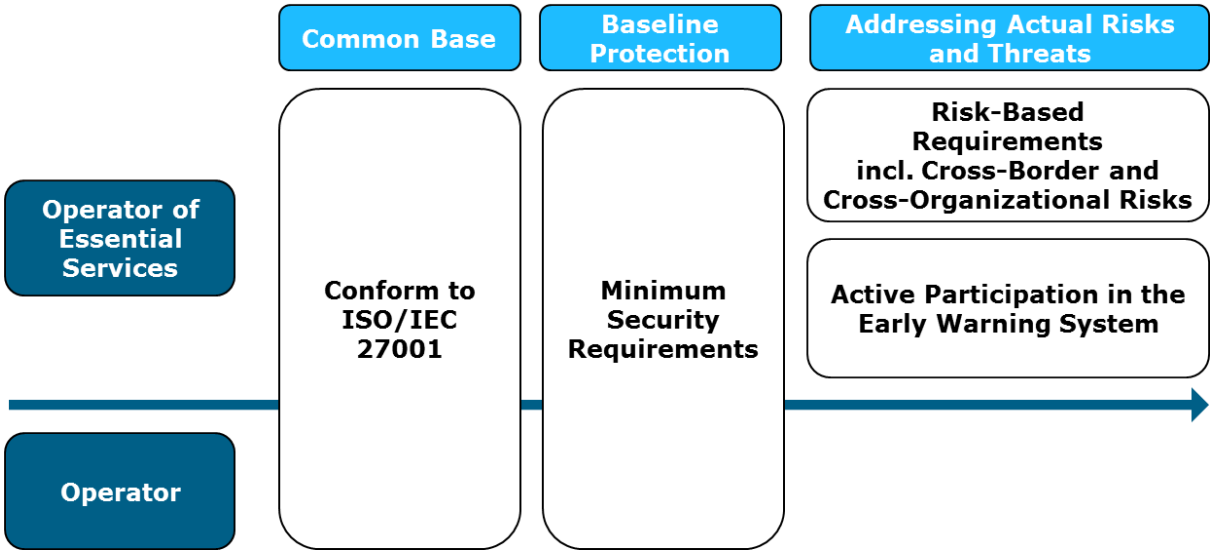

Figure 3: Recommended Structure for the Network Code on Cybersecurity

One of the key building blocks is a common baseline for all operators, which is to work conform to ISO/IEC 27001; this common baseline has been already stated in the 1st interim report[12] of the SGTF EG2. A baseline protection is going to be introduced that defines minimum security requirements for operators that includes measures for people, practices and infrastructure. Additional Requirements are going to be introduced for operators that are identified as operators of essential services that targets a risk-based protection addressing actual risks and threats which includes mitigation measures that are derived by a methodology currently in preparation by the working group of the key area 'Cross-Border and Cross–Organizational Risk Management'. Furthermore, the active participation in an 'Early Warning System for Cyber Threats' will be recommended.

Minimum security requirements are derived with methodology following a risk-based approach in order to reflect cybersecurity needs to address risks and threats that are continuously evolving. This implies that minimum security requirements are not static but are subject to a regular change, too.

[12] https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf

The methodology for minimum security requirements is currently in discussion in the working groups for the key areas: 'Supply Chain Management' and 'European Energy Cybersecurity Maturity Framework'.

5.2 Proposed Components of the Network Code for Cybersecurity

Following the recommended structure of the Network Code on cybersecurity, the four key areas are going to result in components for the Network Code that can be recapitulated as following:

Early warning system in Europe for the energy sector.
An information sharing platform that enables operator to share actual information on compromises and attacks.

Cross-border and cross-organizational risk management in the EU
A risk management methodology that provides mitigation measures for risks and threats that are substantiated by the interconnection and interdependency of energy systems, infrastructures and applications.

Minimum Security Requirements for critical infrastructure components
A methodology, aligned with the proposed EU Cybersecurity Act[13], to define minimum security requirements for infrastructure components and services that are critical to secure the energy infrastructure.

Minimum Protection Level for energy system operators
A methodology to define a minimum protection level for energy systems including requirements for organization, practices and infrastructure. The minimum protection level will include minimum security requirements for the supply chain management.

European Energy Cybersecurity Maturity Framework for Operators of Essential Services
Recommendation towards a European energy cybersecurity maturity framework in order to have a metric available for energy system operators and Member States that allows to measure and steer the protection and resilience of critical infrastructure in the energy sector.

Supply Chain Risk Management for Operators of Essential Services
Recommendation towards a supply chain risk management process specific for the energy sector in order to address supply chain risk appropriately.

The final report of the SGTF EG2 will describe the components in more detail, i.e. it will define

- A risk-based methodology to derive minimum security requirements for products and services used in and for energy systems. This includes recommendation for a certification scheme in alignment with the EU Cybersecurity Act.
- A risk-based methodology to derive minimum security requirements for operators. This includes recommended measures for people, practices and infrastructure.
- A risk-based methodology to derive mitigation measures for cross-border and cross-organizational risks.
- Recommendation for a European Energy Cybersecurity Maturity Framework.

[13] COM(2017) 477

- Minimum Security Requirements for Supply Chain Management.
- Recommendation for a Supply Chain Risk Management (SCRM) Process.
- Recommendation on an Early Warning System.

6. Conclusion & Outlook

The SGTF EG2 is detailing the recommendation in the working groups that will be concluded in the final report in end of 2018. The approach is generally following a risk-based approach in order to reflect the continuously changing risk and threat environment. This will result in a recommendation on components that supports a managed cybersecurity approach in Europe.

7. Annex

7.1 Annex A-1: Smart Grids Task Force – Expert Group – Working Group on Cybersecurity

The Working Group on Cybersecurity has members which are appointed as experts representing a common interest, i.e. organisation. The following table provides the list of experts of the group:

Experts representing a common interest:

Association	Experts	Alternate Experts
CEER	Roman Picard, French NRA	Carolin Wagner, German NRA
CEDEC	Joy Ruymaekers, Eandis	-
EDSO	Wolfgang Löw, EVN	-
Eurelectric	Nuno Medeiros, EDP	-
GEODE	Armin Selhofer, Austrian Elect. Assoc.	-
ENTSO-E	Alina Neagu, ENTSO-E Sonya Twohig, ENTSO-E	Keith Buzzard, ENTSO-E David Willacy, National Grid
Orgalime / T&D Europe	Volker Distelrath, Siemens	Laure Duliere, T&D Europe
Digital Europe / ESMIG	Willem Strabbing, ESMIG	-
ANEC/BEUC	Ieva Galkyte, ANEC	-
SEDC	Thomas Weisshaupt, Wirepas	Frauke Thies, SmartEn
ENCS	Anjos Nijk, ENCS	Maarten Hoeve, ENCS
EUTC	Guillermo Manent, Iberdrola	-
CECED **(Observer only)**	Felix Mailleux, Applia Mustafa Uğuz, Arçelik	-
CENELEC **(Observer only)**	Didier Giarratano, Schneider Electric	John Cowburn, Smart Energy Networks

7.2 Annex A-2: Editorial Team

The Editorial Team is listed in the following table:

Expert	Role
Volker Distelrath, Siemens Orgalime / T&D Europe	Editor & Editorial Team
Keith Buzzard, ENTSO-E ENTSO-E	Editorial Team
Wolfgang Löw, EVN EDSO	Editorial Team
Armin Selhofer, Austrian Elect. Assoc. GEODE	Editorial Team

European Commission & Agencies	
Manuel Sánchez-Jiménez	European Commission DG ENER
Michaela Kollau	European Commission DG ENER
Beatriz Sinobas	European Commission DG ENER
Igor Nai-Fovino	European Commission DG JRC
Kyriakos Satlas	European Commission CERT-EU
Domenico Ferrara	European Commission DG CNECT
Stefano Bracco	Agency for the Cooperation of Energy Regulators ACER
Konstantinos Moulinos	Agency for Network and Information Security ENISA
Paraskevi Kasse	Agency for Network and Information Security ENISA

7.3 Annex A-3: Working Groups on Key Areas Identified

The Editorial Team is listed in the following tables:

Working Stream: European Energy Cybersecurity Maturity Framework		Working Stream: Supply Chain Management	
Participant	**Association**	**Participant**	**Association**
Volker Distelrath, Siemens (Team Lead)	Orgalime / T&D Europe	**Volker Distelrath, Siemens (Team Lead)**	Orgalime / T&D Europe
Lauri Haapamäki, Sectra	GEODE	Christoph Eberl, Wiener Netze	GEODE
Armin Selhofer, Österreich Energie	GEODE	Philip Westbroek, Enexis	EDSO
Philip Westbroek, Enexis	EDSO	Bart Luijkx, Alliander	EDSO
Anjos Nijk, ENCS Maarten Hoeve, ENCS	ENCS	Anjos Nijk, ENCS Maarten Hoeve, ENCS	ENCS
Guillermo Manet Alonso, Iberdrola	EUTC	Didier Giarratano, Schneider Electric	T&D
Eric Scheer, Siemens	T&D	Willem Strabbing, ESMIG	ESMIG
Joy Ruymaekers, EANDIS	CEDEC	Paraskevi Kasse, Enisa Konstantinos Moulinos, Enisa Prokopis Drograris, Enisa	ENISA
Paraskevi Kasse, Enisa Konstantinos Moulinos, Enisa Christina Skouloudi, Enisa	ENISA		
David Willacy, National Grid	ENTSO-E		
Andrea Foschini, Terna	ENTSO-E		
Guro Grøtterud, NVE	CEER		
Siegfried Sawinsky, Amprion	ENTSO-E		
Stefano Bracco, ACER	ACER		

Working Stream: Early Warning System for Cyber Threats		Working Stream: Cross-Border and Cross-Organizational Risk Management	
Participant	**Association**	**Participant**	**Association**
Wolfgang Loew, EVN (Team Lead)	EDSO	**Keith Buzzard, ENTSO-E (Team Lead)**	*ENTSO-E*
Lauri Haapamäki, Sectra	GEODE	Lauri Haapamäki, Sectra	GEODE
Marcel Kulicke, SIEMENS	T&D	Fredrik Torp, Vattenfall	GEODE
Paraskevi Kasse, Enisa Konstantinos Moulinos, Enisa	ENISA	Roman Tobler, Wiener Netze	GEODE
Kyriakos Satlas, European Commission	CERT-EU	Christophe Poirier-Galmiche, Enedis	EDSO
Nuno Medeiros, EDP	Eurelectric	Christiane Gabbe, Innogy	EDSO
Armin Selhofer, Österreich Energie	GEODE	Joy Ruymaekers, Eandis	CEDEC
		Artur Świętanowski, PSE	ENTSO-E
		Maarten Hoeve, ENCS	ENCS
		Ioannis Retsoulis, Eurelectric	Eurelectric