Smart Grids Task Force

Documents for input to define the Terms of Reference

For the Working Group on

Cybersecurity

1) Scope & Objectives

This working group stems 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 will establish in 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. The Commission will report on the structure, scope and planning of the groups in spring 2017 and final results by the end of 2018." This working group is dedicated to energy-specific cybersecurity.

2) Context

The energy infrastructure is inarguably one of the most complex and most critical infrastructures of a modern society and serves as the backbone for its economic activities and for its security. Digital technologies play an increasingly important role in the energy sector in many ways, making the energy system smart and providing the ground for a new energy market design.

But the new efficiency in energy services comes at a price: increased exposure to cyber-attacks and a higher risk for personal data. Therefore, ensuring resilience of the EU energy supply system against cyber-threats is becoming increasingly important as wide-spread use of IT and data traffic becomes the foundation for the functioning of infrastructures underlying the energy system.

3) Relevant policy basis and background

Energy:

In December 2006, the Commission adopted the Communication on a European Program for Critical Infrastructure Protection (EPCIP), which set out an overall framework for critical infrastructure protection activities at EU level. The threats to which the program aims to respond are not confined to cyber security or terrorism alone, but also include criminal activities, natural disasters and other causes of accidents. The program thus seeks to provide an all-hazard, cross-sectoral approach to the protection of critical infrastructures. A key pillar of this program is the 2008 Directive on European Critical Infrastructures (2008/114/EC), which established a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. This Directive has a sectoral scope and applies only to the energy and transport sectors.

The creation of Energy Union is a priority of the Junker's Commission. Launched in February 2015, it covers five dimensions: energy security, solidarity and trust; a fully integrated European energy market; energy efficiency contributing to moderation of demand; decarbonizing the economy; and research, innovation and competitiveness. The aim of the Energy Union is to lead to a sustainable, low carbon and environmentally friendly economy, putting Europe at the forefront of renewable energy production and the fight against global warming. In light of the increasing digitalization of the energy sector, the Commission intends to develop the Energy Union in synergy with the creation of the Digital Single Market agenda. This includes taking measures to ensure privacy protection and cyber-security.

The "Clean Energy for all Europeans" package of 30 November 2016 acknowledges the importance of cyber security 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] and draft Risk preparedness Regulation[2] propose the adoption of measures to prevent and mitigate the risks identified, as well as the adoption of technical rules for electricity (i.e. a Network Code) on cyber-security.

As dedicated expert group, the EECSP-Expert Group[3] gave guidance to the Commission from December 2015 until February 2017 on policy and regulatory directions on energy sector key points at European level under the framework of the Directive on security of network and information systems (the NIS Directive). The expert group identified the strategic challenges and specific needs of the whole energy sector regarding cyber security from four key angles: threat and risk management, cyber defence, cyber resilience and required capacity and competences needed. They further analysed to which extent existing legislation at EU and national level is sufficient to tackle the specific needs of the energy sector and proposed a roadmap of ten action lines as a way forward, such as the identification of providers of essential services in energy, definition of the rules for a regional cooperation, set up the response framework and coordination. The work of this new working group should be based on the outcome of the EECSP-Expert Group and take all other current activities on energy and cyber security into account. The focus is not to reinvent the wheel, but to acknowledge and use work already done and to focus on the proposed network code on cyber security.

Security of Network and Information Systems:

The EU Cybersecurity Strategy from 2013, and the 2016 adopted Directive on Security of Network and Information Systems (NIS directive), form part of the core policy response on cybersecurity challenges. The Strategy focuses on identifying high-risk areas, working with the private sector to close loopholes, providing specialised training and cyber-security capacity building, and promoting better cooperation between law enforcement and cybersecurity authorities. The NIS Directive currently provides the legal instrument at European level to boost the overall level of cybersecurity in the energy sector. It focuses on essential service providers, including electricity, oil and gas. The NIS

[1] COM/2016/0861 final/2 – 2016/0379 (COD)
[2] COM/2016/0862 final – 2016/0377 (COD)
[3] Energy Expert Cyber Security Platform (EECSP):
https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

Directive entered into force on 8 August 2016. Member States will have 21 months to implement the directive into their national laws and 6 months more to identify operators of essential services.

The NIS Directive is based on four cornerstones – improving national cyber security capabilities, improving cooperation, Security and Notification Requirements for Operators of Essential Services and Security and notification requirements for digital service providers.

Data Protection:

The General Data Protection Regulation (GDPR) was adapted by the European Parliament and of the Council of 27 April 2016. This regulation specifies rules relating to the protection of individuals with regard to the processing of personal data by automated means and rules relating to the free movement of personal data. The regulation updates and modernizes the principles of the 1995 Data Protection Directive to guarantee privacy rights. It focuses on: reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards.

The GDPR foresees the DPIA as a key instrument to enhance data controllers' accountability and renders it mandatory when type of data processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Operating smart grids and smart metering systems might be classified as one of such operations. Therefore, the GDPR provisions are of vital importance to the energy sector. The DPIA Template, currently under development of the SGTF, will be the first sectorial template of its kind under GDPR.

The NIS directive and the GDPR create a new framework for handling cyber security and data protection in the EU and should thus be considered as the key legislations for the work of this group. Additionally the working group shall build up on the key findings of the EECSP -Expert Group[4], as well as the other initiatives mentioned above.

4) Topics to address

The work of the SGTF working group shall focus on energy networks and prepare the ground for a possible network code on cyber security. The work should be based on the outcome of the EECSP - Expert Group and take all other relevant activities on energy and cyber security into account. The focus is not to reinvent the wheel, but to acknowledge and use work already done and to focus on the proposed network code on cyber security.

As a first activity, the group has to identify the tasks as well as a roadmap. The experts in the working group will decide how to handle the tasks and also provide a realistic timetable keeping the reporting obligations in mind. The group will focus on cyber security as well as data protection requirements, taking into account the above mentioned legal basis and background documents.

The group will work towards:

1. **Work towards a cyber security maturity framework**

[4] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341

a. **Identify the minimum cyber security requirements** – This includes the definition of the basic driving principles, such as the duty of care and due diligence which are commonly accepted and understood by the security community.

This area relates to the EECSP action #7 "Establish a European cyber security maturity framework for energy". A risk landscape can be the input to define which maturity level would be recommended in different areas and would therefore allow a risk based approach to drive cyber security in Europe.

b. Independent testing of the supply chain products used in the electricity grid

This included the definition of minimum security requirements to be tested against the equipment before they are deployed on the field, in isolation or within a complex and integrated system.

This relates to the EECSP action #2 "Risk analyses and Framework" and EECSP action #7 "Cyber security maturity framework" as the organisational level of a grid operator is addressed.

c. **Definition of Protection Profiles and Acceptance Evaluation Levels**, by analogy with what is common practice for example from Common Criteria, or using existing efforts from the European Commission to establish similar frameworks in Europe.

d. Human Resources

- Minimum requirements for taking up duty, definition of baseline for a code of conduct applicable to all the sector
- Define rules to deal with privileged work force – background check, type of authentication, vetting for critical posts
- Enforce strong access control policies as an effective mitigation measure

e. Definition of minimum requirements for maintenance of the existing and future equipment connected to the Grid

f. Define minimum security baseline to ensure an acceptable level of security appropriate to the acceptable risks*

g. Set the need for a common threat landscape analysis shared among all operators

2. Work towards a cyber defence framework

a. Address what is an acceptable time frame to address any issue related to cyber security.

The scope lies on the organisational level and is linked to EECSP report action #5 " Define and implement cyber response framework and coordination."

b. Establish a structured and shared incident classification schema in order to boost in time and effective communication*

c. **Crisis Management** – Definition of organizational infrastructure and ad-hoc processes to enable cooperation at operational level among all actors. This relates to the EECSP Action #4 "EU framework for vulnerabilities disclosure in the energy sector.

3. Clear definition of a methodology to assess value of Data in the electricity sector

This includes also analysing the relationships and contradictions of existing network codes, as well as analysing the common grid model.

4. Certification of IT and OT devices prior their connection to the grid

5. **Incident notification and dissemination to prevent and minimize the impact of medium-large incidents on the IT systems that provide essential and critical services to the grid** *

6. Identification of harmonised selection criteria of operators of essential services in the electricity sector*

7. Define minimum security baseline to ensure an acceptable level of security appropriate to the acceptable risks*

* These topics should be developed in track with the NISD cooperation group that is working horizontally for all sectors.

Editorial Team:

1. Wolfgang Loew, EVN, representing EDSO
2. Armin Selhofer, Austrian Electricity Association, representing GEODE
3. Keith Buzzard, ENTSO-E
4. Volker Distelrath, Siemens, representing Orgalime/T&D Europe

5) Deliverables and Milestones

The Group will have to conclude its work and deliver the final results by the end of 2018. The findings will be summarised in two deliverables (reports) which will be submitted for approval to the Steering Committee of the Smart Grids Task Force at the end of 2017 and 2018, respectively. The following milestones and deliverables in order to keep the programme of work in schedule are defined:

1. Milestone 1 – Terms of Reference: Decision on approach and roadmap: within 1 month of launch of Working Group
2. Deliverable 1 – 1st Interim Report: by 12/2017
3. Milestone 2 – 2nd Interim Report: by 06/2018
4. Deliverable 2 – Final Report: by 12/2018

6) Composition of the working group

The Group will consist of 12 nominated experts designated by the participating associations and will undertake its work by means of its own resources. The Commission will chair the Group and organise the necessary meetings.

In its first meeting, the Group will designate an Editorial Team which will consist of 4 members of the Group. The Editorial Team will be responsible for providing the deliverables as lined out in section 5 on time based on input and comments by the Group. The members of the Editorial Team may decide on any further working arrangements and allocation of work upon formation of the Team. They shall be in close contact to the chair of the working group.

It is foreseen that the Group will meet on average once every quarter (4 meetings per annum), while the Editorial Team should arrange separate meetings. Besides physical meetings, the Editorial Team and the Working Group are encouraged to exchange information via telephone conferences.

The Group members should be experts in the field at a high level in their organisation and market domain, and should be in a position to influence stakeholders, to foster partnerships and to leverage resources, as well as to demonstrate a high degree of commitment to the Group and ability to devote sufficient time to its activities. The Commission will inform the Smart Grids Task Force Steering Committee on the progress of the work as well as the composition and structure of the group and of any subsequent changes.

Working Group on Cybersecurity
(as a subgroup of the Smart Grids Task Force)
Chaired by the European Commission

1) no alternate; 2) Multiple functional player; 3) Covering the role of supplier; 4) 2 experts and 2 alternates; 5) EC ask BEUC case by case, according with the issue to discuss

EC	DG ENER:	Michaela Kollau, Manuel Sánchez Jiménez, Yolanda Garcia Mezquita, Remy Denos Adam Szolyak
	DG JRC:	Igor Nai Fovino Nikoleta Andreadou Ioulia Papaioannou
	DG CNECT:	Domenico Ferrara
	ACER:	Stefano Bracco
	ENISA	Konstantinos Moulinos Paraskevi Kasse

	Expert	Alternate
CEER	**Roman Picard**, French NRA	**Carolin Wagner**, BNetzA
CEDEC (1) (2)	**Joy Ruymaekers**, Eandis	No alternate
EDSO (1)	**Wolfgang Löw**, EVN	No alternate
Eurelectric (1)	**Gitte Bergknut**, Uniper	No alternate
GEODE (1)	**Armin Selhofer**, Austrian Elect. Assoc.	No alternate
ENTSO-E (4)	**Alina Neagu**, ENTSO-E **Sonya Twohig**, ENTSO-E	**Keith Buzzard**, ENTSO-E **David Willacy**, National Grid
Orgalime/T&D	**Volker Distelrath**, Siemens	**Laure Duliere**, T&D Europe
ANEC/BEUC (5)	**Katrin Behnke** , ANEC	
SEDC	**Thomas Weisshaupt**, Director Smart Energy and IoT, Gemalto SA	**Frauke Thies**, SEDC
ENCS	**Anjos Nijk**, ENCS	**Maarten Hoeve**, ENCS
EUTC	**Guillermo Manent**, Iberdrola	No alternate