SMART GRIDS TASK FORCE - EXPERT GROUP 2 - CYBERSECURITY

Interim Report

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

December 2017

The mission of the Smart Grid Task Force Expert Group 2 on cybersecurity is to prepare the ground for a network code on energy-specific cybersecurity.

1. Contents

1. Introduction

1.1 Context

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. The advantage of digitalization of the energy infrastructure has led to an increase in efficiency of network operation and new business models and market players in the energy value chain. The other side of that coin is that modern energy infrastructures are increasingly exposed to cyber risk and threats.

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.

1.2 Acknowledgements

This intermediate report has been prepared by the Smart Grid Task Force - Expert Group 2 (SGTF EG2) and is a product of intensive work, discussions and bi-weekly conference calls of the editorial team (see chapter 8.2, Annex A-2) with contributions of the nominated experts (see chapter 8.1, Annex A-1) from May 2017 until December 2017.

1.3 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
- **cPPP** Contractual Public Private Partnership
- **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
- **ICT** Information and Communication Technology
- **IEC** International Electrotechnical Commission
- **IoA** Indicators of Attack
- **IoC** Indicators of Compromise
- **ISAC** Information Sharing and Analysis Center
- **IT** Information Technology
- **MSIP** Malware Information Sharing Platform
- **NCA** National Cybersecurity Authority
- **NIS** Network Information Security
- **OT** Operational Technology
- **PLC** Programmable Logic Controller
- **RSC** Regional Security Coordinator
- **RTU** Remote Terminal Unit
- **SCADA** Supervisory Control And Data Acquisition
- **SPOC** Single Point of Contact
- **SGTF EG2** Smart Grid Task Force Expert Group 2
- **TLP** Traffic Light Protocol
- **TSO** Transmission System Operator

3. Executive Summary

Energy systems provide an essential service that underpins the smooth functioning of a modern society and serve as the backbone for the economic activities within the European Union. In the way the digitalization of energy grids is taking place, the energy systems are increasingly exposed to cyber risks and threats. The network code on cybersecurity rules targets to continuously improve the resilience of the inarguably most complex and critical infrastructure of a modern digital society using a risk-based approach.

The Smart Grid Task Force Expert Group 2 (SGTF EG2) has derived four objectives that need to be addressed by a potential network code on cybersecurity for electricity system operators:

- Protect the energy system based on current and future threats and risks.
- Have effective plans in place to ensure that an energy crisis is managed, to limit the effect upon the European society and economy.
- Create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector.
- Harmonized maturity and resilience for cybersecurity across EU with defined minimum level while favouring higher maturity using a risk based approach.

Based on these objectives, four key areas on cybersecurity have been defined that address cybersecurity in organisations as well as the cybersecurity challenges of an interconnected European energy system.

With the key area on a **European Cybersecurity Maturity Framework** the SGTF EG2 targets to provide an instrument to the energy sytem operators in order to steer the cybersecurity implementation in a structured and risk-based approach. Additionally, it is an instrument that can be used to harmonize the implementation in defining a minimum security level on cybersecurity across the EU.

The key area on **Supply Chain Management** will help energy system operators to have more transparency and build more trust in the products, systems and services provided by vendors and service providers. Additionally, it helps energy system operators with the implementation of protection concepts by getting transparency in the functionality and lifecycle support provided with products to be deployed.

A **European 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 within the CSIRT network and with other energy system operators and stakeholders in the EU.

The energy grid in the EU is interconnected with an increasing number of market players participating in the energy value chain. The key area **Cross-Border and Cross-Organisational Risk Management** takes into account the changing environment of the energy infrastructure by providing a systematic approach on managing the threats and risks associated with the nature of the energy infrastructure in a cross-border and cross-organizational environment.

In order to prioritize the specific cybersecurity measures to be defined for the network code, the SGTF EG2 has prepared risk scenarios to be considered and rated concerning the risks by respective energy system operators. The rating will be used in the work planned in preparing the ground for a network code on cybersecurity rules.

Chapter 4 provides more detail on the key areas and chapter 5 explains the risk scenarios prepared by the SGTF EG2 in detail. The approach on addressing the key areas and to prepare the ground for the network code on cybersecurity is described in detail in chapter 6.

4. Key Areas in Cybersecurity

The mission of the Smart Grid Task Force Expert Group 2 (SGTF EG2) is to prepare the ground for a network code on energy-specific cybersecurity, 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, please reference chapter 6.4 for more details.

As a guiding principle, the 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 legislation such as the Directive on security of Network and Information Systems (NIS)[2] and the General Data Protection Regulation (GDPR)[3] and their ongoing implementations as a baseline for building all pillars of the network code.

The following section describes in more detail the approach used for the analysis.

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.

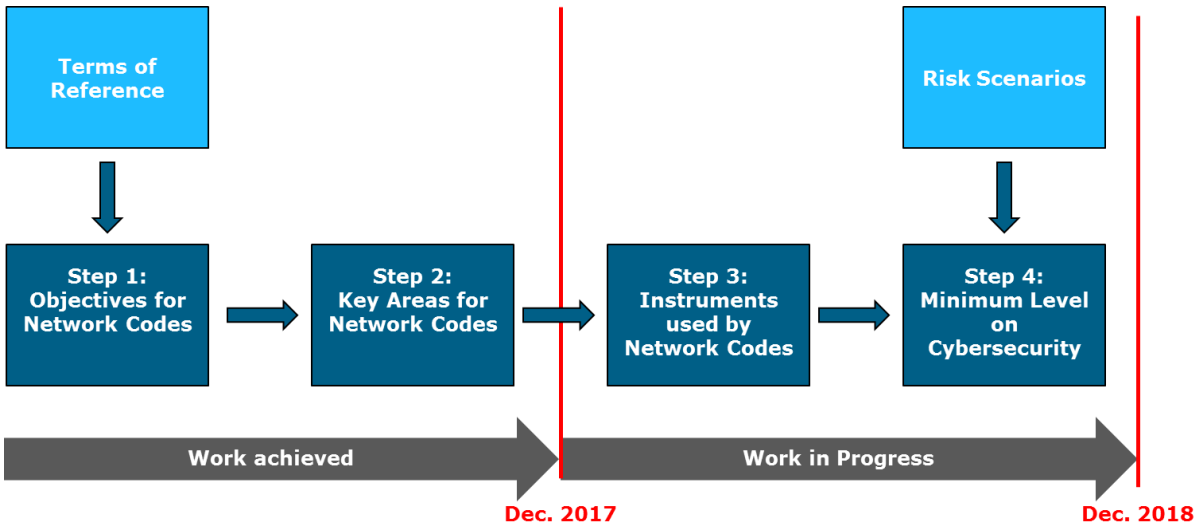

Figure 1: Overview of the analysis and implementation approach

The starting point of the analysis is the Terms of Reference (ToR) that have been agreed by the SGTF EG2. In Step 1, the agreed ToR has been analysed in detail by the editorial team in order to derive the objectives and the key areas to be addressed by the network code. In 2017, the Energy Expert Cyber Security Platform (EECSP) published a report[4] 'Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector' that identified a number of strategic areas for action, together with gaps in existing legislation and recommendations on actions which provides context to the potential network code

[2] Directive (EU) 2016/1148
[3] Regulation (EU) 2016/679

on cybersecurity. In a structured exchange, the editorial team has mapped the ToR with the areas of actions, the strategic areas and the gaps in legislation as identified by EECSP in order to derive the objectives for the network code, see chapter 4.2.

In Step 2, the objectives derived in Step 1 of the analysis work have been further analysed which has led into four key areas for the network code on cybersecurity that has been agreed by the SGTF EG2. In extensive discussions by the editorial team, the scope and approach of these key areas has been further outlined. Chapter 4.3 describes the key areas identified in more detail and chapter 6 presents the approach chosen by the Expert Group to prepare the ground work for the network code.

The work in progress covers Step 3 that is going to define the instruments used by the network code and Step 4 that is going to define a minimum level on cybersecurity to be fulfilled by electricity system operators. In order to follow the guiding principle on a risk-based approach and to be able to prioritize on cybersecurity measure for electricity system operators, a risk analysis on potential threats has been initiated. The risk analysis is based on publicly available data such as incidents reported and the ENISA threat-taxonomy that are described and referenced in more detail in chapter 5. It should be noted that the risk analysis done here is determined to be used only by SGTF EG2.

Furthermore, following the developments of late 2017 regarding the EU Cybersecurity Act[5], in 2018 the SGTF EG2 will also reconsider part of the existing deliverables in light of the ongoing negotiations on the new proposed regulation.

4.2 Objectives for the Network Code on Cybersecurity

In the agreed Terms of Reference, seven main topics are to be covered, see chapter 8.3, Annex A-3 for more details:

1. Work towards a cybersecurity maturity framework.
2. Work towards a cyber defence framework.
3. Clear definition of a methodology to assess value of data in the electricity sector.
4. Certification of IT and OT devices prior to 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 harmonized 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.

[4] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

[5] COM(2017) 477 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'').

These initial topics have been further elaborated and refined within the editorial team and were well matched against the strategic areas as defined in chapter 6 of the EECSP report:

No.	Identified Strategic Areas	Addressed by ToR
1	European threat and risk landscape and treatment	X
2	Identification of operators of essential services	X
3	Cyber response framework	X
4	Crisis management	X
5	European cybersecurity maturity framework	X
6	Supply chain integrity framework for components	X
7	Capacity & competence build-up	
8	Best practice and information exchange	
9	Foster international collaboration	
10	Awareness campaign from top level EU institutions	

Table 1: Mapping of ToR to EECSP Strategic Areas

While the scope of the work of EECSP has been much wider to the overall energy sector representing a European Union view on the topic of cybersecurity, it can still be used for the purpose of a network code on cybersecurity with a narrower view on electricity transmission and distribution system operators whilst keeping in mind that all system operators have to play their part in the overall concept of a cyber-resilient European infrastructure.

In the following, the respective content of the ToR, see chapter 8.3 Annex A-3 has been analysed together with the EECSP areas of action and related gaps in legislation (EECSP report, chapter 8 and 9; see chapter 8.4 Annex A-4 for an overview) in order to derive the objectives for the network code on cybersecurity for electricity network operators:

No.	Identified Objectives for the Network Code on Cybersecurity	Addressed ToR
1	Protect the energy systems based on current and future threats and risks	1.f 2.a,b 3 5
2	Have effective plans in place to ensure that an energy crisis is managed, to limit the effect upon the European society and economy.	2.c
3	Create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector	1.b 4
4	Harmonized maturity and resilience for cybersecurity across EU with defined minimum level while favouring higher maturity using a risk based approach. (Possibility to define maturity level by profiles depending on criticality and relevance as provider of essential services to be considered)	1.a,c,d,e 6

Table 2: Identified Objectives for a Network Code on Cybersecurity

In the following chapter 4.3 the scope related to the objectives is defined and four key areas for the network code on cybersecurity are derived.

4.3 Outline of the Key Areas for a Network Code on Cybersecurity

In order to identify the key areas in cybersecurity with the respective scope, the EECSP areas of action (EECSP report, chapter 9; see chapter 8.4 Annex A-4 for an overview) has been considered

together with the Terms of Reference topics (see chapter 8.3 Annex A-3) that have eventually resulted in four key areas in cybersecurity to be addressed in the network code on cybersecurity:

i. European Cybersecurity Maturity Framework
ii. Supply Chain Management
iii. European Early Warning System for Cyber Threats
iv. Cross-Border and Cross-Organisational Risk Management

As can be seen in Figure 2 the key area (i.) and (ii.) address the transmission and distribution system operator as an organization, while the key area (iii.) and (iv.) address the interconnected European Union energy system, see Figure 3.

On an organizational level, see Figure 2, a transmission or distribution system operator is considered to work conform to ISO/IEC 27001 for his operational infrastructure and the related IT/OT environment necessary for the business operations. Please note that in some Member States such as Germany, ISO/IEC 27001 conformity must be certified by an accredited 3rd party. The objective (4) on a harmonized maturity and resilience across the EU with defined minimum level while favouring higher maturity using a risk based approach are reflected in the key area (i.) of a European cybersecurity maturity framework shall be based on the ISO/IEC 27000 series. The key area (ii.) on supply chain management will address objective (3) with the need to define minimum cybersecurity requirements that are defined as a baseline security for products or systems. Furthermore, a 'standardized' product declaration is foreseen in order to create transparency and trust in the supply chain. ISO/IEC 27001 conformity declaration by vendors and required capabilities on incident handling and vulnerability handling shall secure the lifecycle support of products, systems and services deployed.

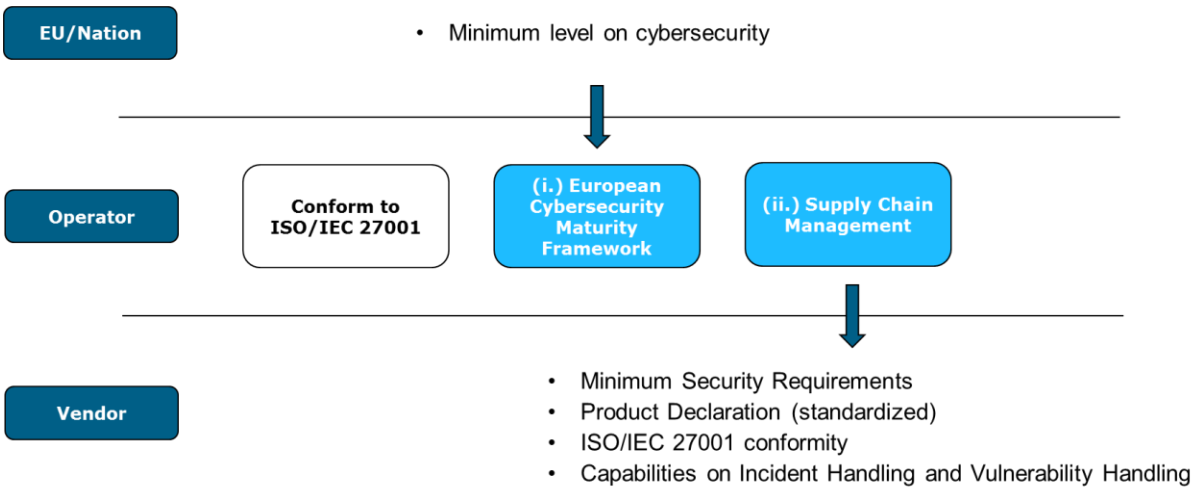

Figure 2: Overview of key areas in cybersecurity related to a TSO or DSO organization

On the level of interconnected EU energy systems, see Figure 3, the key area (iii.) with a European early warning system for cyber threats addressing objective (1) by implementation of an information sharing mechanism across organizations utilizing the set-up of CSIRTs[6] as provided by the NIS Directive. The CSIRT organization is taking an active role in sharing information as a single point of contact for each Member State. The key area (iv.) with a cross-border and cross-organisational risk

[6] Please note that in some Member States CSIRTs might be represented by a National Cybersecurity Authority or another competent authority (NCA)

management is addressing objective (1) and (2) by executing a respective threat and risk analysis and by defining appropriate mitigation measures.

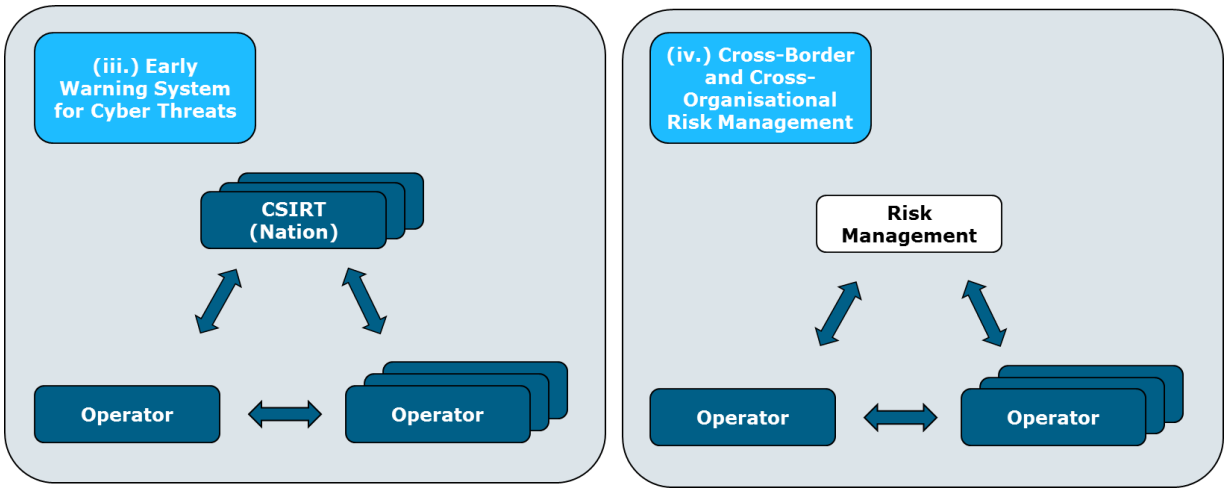

Figure 3: Overview of key areas in cybersecurity addressing the interconnected EU energy system

The key areas in cybersecurity are described in more detail below.

4.3.1 European Cybersecurity Maturity Framework

The maturity framework addresses the need for a harmonised approach in cybersecurity. Due to the interconnected nature of the power grid, the weakest link-problem must be considered; an interconnected system is just as robust as the weakest part of it. Hence, the proposal is to bring all system operators to a minimum security level with a commitment on continuous improvement. This improvement should be matched against a maturity framework that needs to be developed and kept up to date by relevant stakeholders. A European cybersecurity maturity framework should follow international standards such as ISO/IEC 27000 series and IEC 62443, existing maturity frameworks such as C-SET[7] might be used but it requires a mapping to the European cybersecurity maturity framework (to be developed) if applied.

The objective of a maturity framework is to:

- Contribute to an organisation risk management and decision-making process.
- Steer and justify investments and roadmaps concerning cybersecurity implementation.
- Highlight vulnerabilities in energy systems and organizational set-up with the target to provide recommendations on ways to address respective vulnerabilities.
- Provide a method or metric to systematically compare and monitor improvement in the resilience of an organization and of their related critical infrastructure.
- Raise awareness and facilitates discussion on cybersecurity.
- Provide a common industry-wide tool for assessing organisations and cyber systems.
- Support benchmarking against an industry-wide maturity.

[7] https://cset.inl.gov - The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) by cybersecurity experts and with assistance from the National Institute of Standards and Technology (NIST). C-SET covers various cybersecurity maturity frameworks such as ES-C2M2 or framework based on NIST standards.

- Support operational training and assurance programs.
- Convince decision makers of organizations with improvements and concrete goals to be achieved in specific domains.

Please note that existing cybersecurity maturity frameworks provided with C-SET are valid options to be applied. However, the experts has agreed that for Europe, a cybersecurity maturity framework based on ISO and IEC standards to be the preferred option as deployments in Europe are commonly based on such standards rather than NERC CIP or NIST.

4.3.2 Supply Chain Management

The scope of supply chain management targets to create transparency and trust in the use of products, systems and services that are deployed in an electricity grid. There are two main aspects contributing to this target:

1. A 'standardized' product declaration that covers conformance aspects of ISO/IEC 27001, ISO/IEC 27019, IEC 62443 and IEC 62351 that includes capabilities on incident handling and vulnerability handling.
2. Minimum cybersecurity requirements that are defined as a baseline security for products, systems and services.

A 'standardized' product declaration (1.) could provide a statement about processes implemented for respective products and functions supported by respective products. Furthermore, the product declaration should include a statement if the minimum cybersecurity requirements (2.) are met.

Minimum cybersecurity requirements (2.) should define minimum cybersecurity requirements for products, systems and services. These minimum requirements shall consider respective requirements according to article 45 of the EU Cybersecurity Act[8] that could be independently certified.

4.3.3 European Early Warning System for Cyber Threats

The EU has set the baseline for information sharing by implementing the NIS Directive[9] with the regulatory requirement to report relevant incidents towards respective CSIRT by provider of essential services. In order to protect energy systems against current and future threats, an early warning system has to be implemented that allows sharing of sensitive information on attacks and vulnerabilities in order to decrease the response time of operators and allows mitigation and preparedness on current threats and risks. By utilizing the existing set-up of the CSIRT network, early warnings could be communicated to the CSIRT and further processed by the CSIRT network in order to provide early warnings to energy system operators utilizing the set-up provided by the Member States within implementation of the NIS-Directive. This system will act as a multiplier for information sharing between energy system operators, but shall not block established communication between operators as indicated in Figure 3 with the arrow between operators.

[8] COM(2017) 477 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'').
[9] Directive (EU) 2016/1148

4.3.4 Cross-Border and Cross-Organisational Risk Management

The risk management of cross-border and cross-organisational risk of an interconnected energy system has not yet been systematically addressed. As the scope is beyond a single organization, risk management has to be treated by an entity that has the span and competence to cover or involve the various stakeholders in analysis of the threats and risks and in defining appropriate measures to be implemented in order to mitigate these threats and risks.

5. Risk Scenarios

One of the guiding principles in defining the network code on cybersecurity, see chapter 4, is the risk-based approach. The risk scenarios analysed here are used only for the purpose of the SGTF EG2 mission. However, risk management approaches such as ISO/IEC 27005 provides a risk management methodology that can be used to evaluate risks by organizations. Here, in the context of the network code on cybersecurity, addressing risks means to define a minimum level on cybersecurity and to prioritize cybersecurity measures proposed based on the risk analysis performed, see Figure 1.

Cyber risks in the context of energy systems can be assessed by the use of risk scenarios with the respective evaluation of the potential impact and likelihood. The risk scenarios that are going to be evaluated by respective TSO and DSOs[10] will be used to identify risk profiles to be addressed by the minimum level on cybersecurity defined in the network code.

5.1 Methodology and Approach on Risk Scenarios

The approach used for identifying key risk scenarios for energy specific grid systems has been to map the latest ENISA threat taxonomy[11] onto the ANSI/ISA-95 level[12] for enterprise and control systems as already applied to SCADA type architecture in an ENISA report[13].

ANSI/ISA-95 has identified four distinct levels of activities:

- Level 4 – Business planning and logistics systems
- Level 3 – Business operations management systems
- Level 2 – Monitoring and supervisory control systems
- Level 1 – Production and control processes

The editorial team has mapped identified ENISA threats to these four levels of activities. Although the same threat could occur at different levels, most threats logically apply at only one level. An overview on the risk scenarios can be found in Table 4 provided in chapter 8.5 Annex A-5.

For each identified threat, functional areas are stated that would be impacted if the risk were to materialize:

- Identity and Access management
- System availability
- Secure system acquisition, development and maintenance
- Data confidentiality

[10] TSO entity : ENTSO-E ; Depending on the outcome of the negotiations of the "Clean Energy for all Euorpeans" 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

[11] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[12] See 9. Annex – ISA95 levels overview: https://www.enisa.europa.eu/publications/ics-scada-dependencies: Communication network dependencies for ICS/SCADA Systems, December 2016

[13] See , Page 17, Figure 2: ISA95 levels applied to a SCADA architecture. https://www.enisa.europa.eu/publications/ics-scada-dependencies: Communication network dependencies for ICS/SCADA Systems, December 2016

- Data integrity

Editorial comments on the threats have been provided and publicly reported energy specific cyber related incidents, see chapter 8.5 Annex A-5 Table 5, have been cross referenced against these threats in order to create a common understanding of the threat.

The rating will be based on the likelihood that the threat could materialize, together with the expected impact should the threat materialize. The impact rating is based upon the CEN/CENELEC Smart Grid Risk Impact Levels[14] and the likelihood is expressed as the condition of being likely that the event could happen within the next three year horizon.

The following rating will be used for the analysis for impact as an interpretation of the consequences should the event occurs, in terms of, for example: financial impact, reputation, and most importantly the operational resilience of the energy grid:

- Rating 1 – Neglectable
- Rating 2 – Low impact
- Rating 3 – Medium impact
- Rating 4 – High impact
- Rating 5 – Critical or Highly Critical impact

The following rating will be used for the analysis of likelihood which can be expressed as the condition of being likely or probable that the event could happen within the next five years:

- Rating 1 – Very Low 0% to 20%
- Rating 2 – Low 20% to 40%
- Rating 3 – Medium 40% to 60%
- Rating 4 – High 60% to 80%
- Rating 5 – Very High 80% to 100%

The overall risk rating will be calculated per threat by multiplying the likelihood and impact rating resulting in:

- High risk: risk rating ≥ 15
- Medium risk: 15 > risk rating > 4
- Low risk: risk rating ≤ 4

The prepared risk scenarios, see Table 4 provided in chapter 8.5 Annex A-5, will be rated by transmission and distribution system operators, in order to prioritize cybersecurity measures proposed by SGTF EG2.

[14] SG-CG/M490/H_Smart Grid Information Security (Date: 2014-12), Page 57, Figure 34: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

6. Preparing the ground for the Network Code on Cybersecurity

In chapter 4, the approach and key areas that are going to be addressed in the network code on cybersecurity are described. This chapter will focus on the implementation of the necessary content required for the network code. In the final report at the end of 2018, the SGTF EG2 will provide the instruments, the processes and roles needed to define the policy of the respective network code.

Instruments are for example the European cybersecurity maturity framework or processes defining the way how for example minimum security requirements for product, systems and services are defined with roles identified that are responsible for implementing the policy in an organization or entity.

The following sections provide an outlook for the key areas identified for the work and approach planned by SGTF EG2.

6.1 European Cybersecurity Maturity Framework

As stated in chapter 4.3.1, no cybersecurity maturity framework for the electricity subsector[15] based on ISO/IEC 27000 series and IEC 62443 could be identified[16]. A major task will be to develop such a cybersecurity maturity framework and to define the process of how the cybersecurity maturity framework will be used in an organization.

As the cybersecurity maturity framework will be the instrument for the EU and Member States to define the minimum security level for a resilient energy grid in Europe, see Figure 2, one key focus for the policy implementation will be the possibility to define industry benchmarks and to ensure a harmonized implementation across organisations. This includes having an auditable maturity framework available.

The editorial team will work on such a maturity framework and take into account opinions and input from experts within their organisations (with background on maturity framework, ISO/IEC 27000 series and IEC 62443) and discuss the progress regularly with the SGTF EG2. Due to its experience, ENISA will take a leading role in this deliverable.

6.2 Supply Chain Management

As pointed out in chapter 4.3.2, two topics need to be prepared in detail:

1. A ‘standardized’ product declaration that covers conformance aspects of ISO/IEC 27001, ISO/IEC 27019, IEC 62443 and IEC 62351 that includes capabilities on incident handling and vulnerability handling.
2. Minimum cybersecurity requirements that are defined as a baseline security for products, systems and services.

[15] See Annex II, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.

[16] However, various cybersecurity frameworks exist than can be referred to:

- https://www.certsi.es/sites/default/files/paginas/publicaciones/ensi/ensi_c4v_01_value_chain_cyber_security_capability_building_model_draft.pdf; https://www.certsi.es/en/blog/how-evaluate-my-cybersecurity-capacities-according-c4v
- https://www.weforum.org/projects/partnering-for-cyber-resilience
- https://cset.inl.gov
- http://cmmiinstitute.com/capability-maturity-model-integration

The product declaration (1.) template with guidance on usage is going to be prepared and proposed by the editorial team that will cover statements on:

- Intended use and operational environment for the product.
- Processes used in the context of the product development such as IEC 62443 4-1 or ISO/IEC 27001
- Scope covered by processes such as ISO/IEC 27001.
- Functions supported by the products based on international standards such as IEC 62443 4-2, IEC 62351 or ISO/IEC 27019.
- Minimum cybersecurity requirements if defined, see point (2.).

The minimum cybersecurity requirements (2.) will cover the process on how such requirements for products, systems and services are defined and which stakeholders will be involved. The proposal of SGTF EG2 is that ENTSO-E and the respective DSOs[17] are responsible in their area in defining the minimum cybersecurity requirements jointly with T&D Europe and ENISA. The process defined shall be aligned to the proceedings as defined in the EU Cybersecurity Act[18]. T&D Europe will have the role to supervise that the requirements defined are based and properly proposed on international standards such as ISO and IEC. The role of ENISA will be to provide guidance on best practices and to avoid cybersecurity requirements that have previously been known to fail in real-life deployments.

6.3 European Early Warning System for Cyber Threats

Sharing of security related information and especially of early warning information (like indicators of compromise (IoC) or indicators of attacks (IoA) has been identified as one of the key topics for the network code on cybersecurity, see chapter 4.3.3.

To improve the resilience and security of the European energy infrastructures, it is necessary to share cybersecurity related information within and across the Member States and the affected organizations of the energy infrastructure. The following key topics should be covered:

- Sharing of energy related security information within and across the Member States
- Mandatory Code of Conduct for all the involved parties
- Means for sharing
- Structure of the data shared

Sharing of energy related security information within and across the Member States

In the NIS Directive[19] measures concerning computer security incident response teams (CSIRTs) (article 9), CSIRTs network (article 12) and Security requirements and incident notification (article 14) are defined. A Network Code for Cybersecurity should use these measures as the basis for information sharing.

[17] 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

[18] COM(2017) 477 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'').

[19] Directive (EU) 2016/1148

To improve the resiliency and security of the European energy infrastructure it is crucial to have cybersecurity related information available as earliest as possible. Therefore, the requirements of sharing incident notification should be extended and voluntary sharing of cybersecurity related information should be added. This voluntary information should include information such as IoC, IoA, other technical indicators and tactical information. The network code should include rules for sharing this voluntary information. To share this information between the energy related organizations and the Member State existing information sharing architectures such as the CSIRT network should be used that should provide compatible information sharing with platforms commonly used by CERT organizations such as MISP[20] – Malware Information Sharing Platform. The network code of cybersecurity should therefore define which security related information should be shared between the energy related organizations and the CSIRT network. Furthermore, the sharing process and handling of sensitive information in case the information will be classified by a Member State has to be addressed.

While only identified operators of essentials services will be affected by the NIS Directive, the network code will apply to all transmission and distribution system operators. Therefore, the network code on cybersecurity will have to take into account the handling of organisations that are not directly considered by the Member States following the NIS Directive or do not have the necessary CERT capabilities[21].

Mandatory Code of Conduct for all the involved parties

As part of the network code on cybersecurity a Code of Conduct for all the involved parties should be mandatory that defines the rules of communication as one important building block to build-up trust among the involved parties:

- Definition of an information classification scheme such as Traffic Light Protocol (TLP).
- Single Point of Contact (SPoC) based on the requirements of the NIS Directive.
- Role definition and respective requirements for the roles.
- Rules for sharing information.

Means of sharing

Because of the sensitivity of security related information, it will be necessary to define means of sharing information in the network code. These means of sharing should reflect minimum security requirements for sharing the related information. This includes security measures for protecting the confidentiality, integrity and availability of the shared information.

Structure of the data shared

To enhance the processing capabilities of the shared security related information, the SGTF EG2 will define the structure of the data itself and the use of existing data formats as part of the instruments used for the network code for cybersecurity in alignment with NIS cooperation group.

[20] http://www.misp-project.org/

[21] One possibility could be the handling by an accrediated service provider. Such model with a 'Common Superior Notification Site' has been implemented in Germany (GÜAS – Gemeinsame übergeordnete Ansprechstelle gemäß BSI-Gesetz)

6.4 Cross-Border and Cross-Organisational Risk Management

The key area of cross-border and cross-organisational risk management, see chapter 4.3.4, is an area that cannot be handled by one organization due to the nature of the subject. A main topic to be prepared by SGTF EG2 is the definition of the methodology for a threat and risk analysis to be performed in order to address the key area appropriately. Furthermore, the process on how agreed mitigation measures are implemented needs to be covered.

The SGTF EG2 proposes that ENTSO-E and the EU-DSO[22] entity should jointly take the responsibility for this key area and work together with relevant stakeholders like the Regional Security Coordinators (RSCs) in order to address respective risks., SGTF EG2 proposes to work together with ENTSO-E on this topic in order to prepare the instrument of a threat and risk analysis methodology for the network code.

[22] Depending on the outcome of the negotiations of the "Clean Energy for all Euorpeans" 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

7. Conclusion & Outlook

The SGTF EG2 is confident that the key areas identified for the network code on cybersecurity will improve the resiliency of the electricity infrastructure in Europe. The risk scenarios will help to prioritize the proposed measures based on the risk foreseen by electricity system operators. The required instruments such as the maturity framework, the threat and risk analysis methodology or the methodology on sharing information are not defined yet and it should be noted that it will be a challenge for the SGTF EG2 to get it prepared on time for the network code on cybersecurity.

8. Annex

8.1 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:

Name of Expert	Alternate Nomination
Roman Picard, French NRA CEER	Carolin Wagner, BNetzA CEER
Sanne Goossens, CECED (observer) CECED	No alternate
Joy Ruymaekers, Eandis CEDEC	No alternate
Wolfgang Löw, EVN EDSO	No alternate
Willem Strabbing, Digital Europe / ESMIG Digital Europe / ESMIG	Alternate tbd.
Gitte Bergknut, Uniper Eurelectric	No alternate
Armin Selhofer, Austrian Elect. Assoc. GEODE	No alternate
Alina Neagu, ENTSO-E Sonya Twohig, ENTSO-E ENTSO-E	Keith Buzzard, ENTSO-E David Willacy, National Grid ENTSO-E
Volker Distelrath, Siemens AG Orgalime/T&D Europe	Laure Duliere, Orgalime Orgalime/T&D Europe
Katrin Behnke , ANEC ANEC/BEUC	No alternate
Thomas Weisshaupt, Wirepas	Frauke Thies, SmartEn
Anjos Nijk, ENCS ENCS	Maarten Hoeve, ENCS ENCS
Guillermo Manent, Iberdrola EUTC	No alternate

8.2 Annex A-2: Editorial Team

The Editorial Team is listed in the following table:

Experts	
Volker Distelrath	Editor & Editorial Team
Keith Buzzard	Editorial Team
Wolfgang Löw	Editorial Team
Armin Selhofer	Editorial Team
European Commission & Agencies	
Manuel Sánchez-Jiménez	European Commission (DG ENER)
Michaela Kollau	European Commission (DG ENER)
Yolanda Garcia Mezquita	European Commission (DG ENER)
Remy Denos	European Commission (DG ENER)
Adam Szolyak	European Commission (DG ENER)
Igor Nai-Fovino	European Commission (DG JRC)
Nikoleta Andreadou	European Commission (DG JRC)
Ioulia Papaioannou	European Commission (DG JRC)
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)

8.3 Annex A-3: Terms of Reference

The SGTF EG2 has agreed to cover the following items in the work towards a cybersecurity network code:

1. **Work towards a cybersecurity maturity framework**
   a. **Identify the minimum cybersecurity 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.
   b. Supply Chain Management
   This included the definition of minimum security requirements and transparency in the supply chain.
   c. 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

   d. Definition of minimum requirements for maintenance of the existing and future equipment connected to the Grid
   e. Define minimum security baseline to ensure an acceptable level of security appropriate to the acceptable risks*
   f. 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 cybersecurity.
   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. **Define minimum security baseline to ensure an acceptable level of security appropriate to the acceptable risks***

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

8.4 Annex A-4: EECSP - Recommended Actions to the Identified Gaps

The following table provides an overview of the areas of actions and referenced gaps identified in the EECSP report[23] used in the analysis work in order to identify the objectives for a network code.

Strategic Priorities		Strategic Areas		Related Gaps	Areas of Actions
I	Set-up an effective threat and risk management system	1	European threat and risk landscape and treatment	1-13	(1) Identification of operators of essential services for the energy sector at EU level. (2) Risk analysis and treatment. (3) Framework of rules for a regional cooperation. (4) EU framework for vulnerabilities disclosure for the energy sector.
		2	Identification of operators of essential services	14-17	
		8	Best practice and information exchange	19	
		9	Foster international collaboration	20	
II	Set-up an effective cyber response framework	3	Cyber response framework	21-26	(5) Define and implement cyber response framework and coordination. (6) Implement and strengthen the regional cooperation for emergency handling
		4	Crisis management	27-30	
III	Continuously improve cyber resilience	5	European cybersecurity maturity framework	31-34	(7) Establish a European cybersecurity maturity framework for energy. (8) Establish a cPPP for supply chain integrity (9) Foster European and international collaboration
		6	Supply chain integrity framework for components	35	
		8	Best practice and information exchange	36	
		10	Awareness campaign from top level EU institutions	37	
IV	Build-up the required capacity and competences	7	Capacity & competence build-up	38-39	(10) Capacity and competence build-up.

Table 3: EECSP Report - Overview of the EECSP findings

[23] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

8.5 Annex A-5: Risk Scenarios

The following table provides an overview of the risk scenarios prepared for the risk analysis to be used in the work of SGTF EG2. The examples provided can be found in Table 5 below.

Risk Scenarios	ENISA Threat Taxonomy	Impacted Functional Areas	Editorial Comments on Threats	Examples
Level 4 – attacks from the Internet	**1. Identity theft/fraud**	Identity and access management		
Business Operations Management	**2. Denial of service**	System availability		ID 10
Business Planning & Logistics systems	**3. Generation and abuse of rogue certificates**	Identity and access management, Secure system acquisition, development and maintenance		
	4. Social engineering	Identity and access management; Data confidentiality	Spear phishing of user credentials leading to unauthorised access	ID 12
	5. Remote activity (execution)	Identity and access management	Complete or partial outsourcing of infrastructure and services	
	6. Targeted attacks (APTs)	Data confidentiality; Data integrity; System availability	Successful Advanced Persistent Threat (APT) attack, planned and executed over time	ID 3 ID 6 ID 13 ID 15
	7. Wardriving	Identity and access management		
	8. Interception/misuse of information	Data confidentiality	Confidentiality of common operational data exchanged between grid participants	
↑↓ exchange of information between supervisory and operation management systems and business operations management systems.				
Level 3 - attacks against Internet DMZ	**9. Unsolicited and infected email/attachments/URLs**	Data confidentiality; Data integrity; System availability	Introduction of Ransomware, Remote Backdoors, Rootkits and other forms of malicious code	ID 1 ID 11
Business Operations Management Systems	**10. Network reconnaissance, traffic monitoring and information gathering**	Data confidentiality	Unmaintained and unpatched infrastructure/no system hardening	ID 4
	11. Manipulation of hardware and software	Data confidentiality; Data integrity; System availability	Remote exploitation of infrastructure vulnerabilities from Internet or common TSO/DSO network	
Level 3 - attacks against Enterprise LAN	**12. Malicious code/software activity (indirect attack via the supply chain)**	Data confidentiality; Data integrity; System availability	Introduction of Ransomware, Remote Backdoors, Rootkits and other forms of malicious code	ID 5 ID 8 ID 9
Business Operations Management Systems	**11. Manipulation of hardware and software**	Data confidentiality; Data integrity; System availability	Local exploitation of infrastructure vulnerabilities	
	13. Misuse of audit tools	Data confidentiality		
	14. Unauthorised use of software	Data confidentiality; Data integrity; System availability; Secure system acquisition, development and maintenance		

	15. Unauthorised installation of software	Data confidentiality; Data integrity; System availability; Secure system acquisition, development and maintenance	Use of software/hardware from suspect countries with known offensive capabilities/intentions	
	16. Unauthorised activities, unauthorised access to information systems and networks	Identity and access management; Secure system acquisition, development and maintenance	Escalation of user privileges through malware or vulnerability exploitation	
	17. Compromised confidential information	Data confidentiality		
	18. Abuse of authorisation	Identity and access management; Secure system acquisition, development and maintenance		
	19. Failed business process	Data confidentiality; Data integrity; System availability; Secure system acquisition, development and maintenance	Ineffective corporate security policies, ineffective governance	ID 14
Level 3 - attacks against Operational DMZ	**20. Abuse of information leakage**	Data confidentiality; Data integrity; System availability		
Business Operations Management Systems	**21. Falsification of records**	Data integrity	Cover up of a successful cyber attack through event log manipulation	
	22. Repudiation of actions	Data integrity		
	12. Malicious code/software activity (direct attack)	Data confidentiality; Data integrity; System availability	Compatibility issues between OT software and standard COTS security products	ID 2
↑↓ Exchange of information between systems in charge of interpreting and processing data from Level 1 devices and supervisory and operation management systems (SCADA).				
Level 2 - attacks against Supervisory LAN	**23. Unauthorised activities, unauthorised use of administration privileges**	Identity and access management		
Monitoring & Supervisory Control Systems	**24. Interception compromising emissions**	Data confidentiality		
	25. Replay of messages	Data integrity; System availability	Injection of malicious network traffic causing undesired actions	
	26. Man-in-the-middle/session hijacking	Data integrity; System availability		
Level 2 - attacks against Controller LAN	**27. Misuse and Manipulation of information**	Data integrity; System availability		
Monitoring & Supervisory Control Systems	**12. Malicious code/software activity (direct attack)**	Data integrity; System availability		
↑↓ Exchange of information between sensors/field devices (PLC, RTU, sensors) and the systems in charge of interpreting and processing the readings of these devices.				
Level 1 - attacks against Bus Network	**28. Interfering radiation**	Data confidentiality; Data integrity; System availability		
	11. Manipulation of hardware and software	Data confidentiality; Data integrity; System availability	Untested and uncertified devices (hidden functions, backdoors etc.)	

	11. Manipulation of hardware and software	Data confidentiality; Data integrity; System availability	Simultaneous exploitation of vulnerabilities shared by many devices on energy grid (causing n-1 problems)	ID 7

Table 4: Risk Scenarios overview

Examples on threats listed:

ID	Date	Examples on Open Source Reported Incidents
1	Dec 15	Ukraine. Compromise of corporate networks/SCADA using spear phishing emails with Black Energy malware. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
2	Dec 16	Ukraine. Crash Override malware used to target ICS protocols. https://www.us-cert.gov/ncas/alerts/TA17-163A
3	Oct 17	APT threat warning released by DHS/FBI, specifically targeting energy sector companies. https://www.us-cert.gov/ncas/alerts/TA17-293A
4	Apr 17	UK. EirGrid Vodafone router attacked via Vodafone's Direct Internet Access (DIA) service, leading to direct TSO network access. https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html
5	Jun 17	Ukraine. Updates to popular tax accountancy software (M.E.doc) contained Petya ransomware causing problem for grid operator. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine
6	Jun 17	APT threat warning released by DHS/FBI. Watering hole websites used to harvest user credentials specifically targeting energy sector companies. https://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group
7	Aug 17	Holland. Proof of concept exploitation of SMA PV Inverters through multiple device vulnerabilities, including CVE-2015-3964 hard coded passwords. https://www.theregister.co.uk/2017/08/07/solar_power_flaw/
8	Sep 17	Digitally signed version of CCleaner (V 5.33) distributed by anti-virus firm Avast, contained malicious backdoor code. https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleaner-cybersecurity-app-infected-with-backdoor/#24b551dd316a
9	Dec 15	Juniper VPN Concentrator - NSA backdoor. https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/
10	Oct 16	DDOS attack against DNS provider DYN https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
11	Nov 16	Ransomware attack locked San Francisco metro tram ticket machines. https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/
12	Mar 16	KWC Water Utility control system hacked, levels of chemical added to water changed, SQL injection & Phishing (AS/400) https://www.theregister.co.uk/2016/03/24/water_utility_hacked/
13	Dec 14	German steel mill furnace damaged via APT & Phishing attack. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
14	Jun 15	Swedish Police database administration outsourced to IBM with system administrators from other countries https://www.theguardian.com/technology/2017/aug/01/sweden-scrambles-to-tighten-data-security-as-scandal-claims-two-ministers
15	Jun 14	ICS focused malware "Havex" Remote Access Trojan (RAT) https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

Table 5: Examples on Open Source Reported Incidents