Smart Grid Task Force
Expert Group 2

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

Final Report
December 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

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 of technical rules for electricity via a Network Code on cybersecurity.

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

As a result, 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 market. This report is the result of the group working on energy-specific cybersecurity.

1.2 1st Interim Report

In December 2017, the SGTF EG2 published a first interim report[2] 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 set the objectives for a Network Code on cybersecurity and has identified four key areas recommended to be addressed.

1.3 2nd Interim Report

In July 2018, the SGTF EG2 published a second interim report[3] that gave insight into the recommended structure and components of the network code.

This report will summarize the results anticipated and further developed from the previous reports, but does not reiterate how these results have been derived.

1.4 Acknowledgements

The final 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 11.2, Annex A-2) and respective working groups (see chapter 11.3, Annex A-3) with contributions of the nominated experts of the SGTF EG2 (see chapter 11.1, Annex A-1).

[1] COM/2016/0861 final/2 - 2016/0379 (COD)
[2] https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf
[3] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf

1.5 Disclaimer

This document represents the expert opinion of all the contributors listed in chapter 11.3 - Annex A-3. It does not represent the opinion of the European Commission. Neither the European Commission, nor any person acting on the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.

2. Symbols and Abbreviations

The following symbols and abbreviations are used in the report:

- **AGC** Automatic Generation Control
- **CapEx** Capital Expenditures
- **CC** Common Criteria
- **CERT** Computer Emergency Response Team
- **CRITs** Collaborative Research Into Threats
- **CSIRT** Computer Security Incident Response Team
- **CVE** Common Vulnerabilities and Exposures
- **CVSS** Common Vulnerability Scoring System
- **DSO** Distribution System Operator
- **EAM** Enterprise Asset Management
- **EC** European Commission
- **ECCG** European Cybersecurity Certification Group
- **EECSP** Energy Expert Cyber Security Platform
- **EFTA** European Free Trade Association
- **EU** European Union
- **GDPR** General Data Protection Regulation
- **HEMS** Home Energy Management Systems
- **IACS** Industrial Automation and Control System
- **ICT** Information and Communication Technology
- **IEC** International Electrotechnical Commission
- **IECEE** IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
- **IoA** Indicator of Attack
- **IoC** Indicator of Compromise
- **IoT** Internet of Things
- **IPCR** Integrated Political Crisis Response
- **ISMS** Information Security Management System
- **ISAC** Information Sharing and Analysis Centre
- **IT** Information Technology
- **ITRE** Industry, Research and Energy
- **LFC** Load Frequency Control
- **MISP** Malware Information Sharing Platform
- **NCA** National Competent Authority
- **NCIRC** NATO Computer Incident Response Capability
- **NIS** Network Information Security
- **NIST** National Insititute of Standard and Technology
- **NLF** New Legislative Framework
- **NRA** National Regulatory Authority
- **NVD** National Vulnerability Database

- **OES** Operator of Essential Services
- **OpEx** Operational Expenditures
- **OSI** Open Systems Interconnection
- **OT** Operational Technology
- **RTU** Remote Terminal Unit
- **SCADA** Supervisory Control And Data Acquisition
- **SGAM** Smart Grid Architecture Model
- **SGTF EG2** Smart Grid Task Force Expert Group 2
- **SL** Security Level
- **SOP** Standard Operating Procedures
- **STIX** Structured Threat Information Expression
- **TAXII** Trusted Automated eXchange of Intelligence Information
- **TLP** Traffic Light Protocol
- **TSO** Transmission System Operator
- **TTP** Tactics Techniques and Procedures
- **TYNDP** Ten year network development plan
- **ZCR** Zone and conduit requirement
- **ZVEI** Zentralverband Elektrotechnik- und Elektronikindustrie (German Electrical & Electronic Industry)

3. Executive Summary

The energy systems are 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 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 legislations in this regard is the NIS Directive[4] and its implementation at Member State level is a key element. The NIS Directive and the GDPR[5] regulation provide a legislative basis for all sectors, including the energy sector. Specific obligations deriving from the NIS Directive that are already impacting the energy sector are:

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

2. The identification of operators of essential services (OES) includes also energy operators. Those 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 incidents to their relevant National Competent Authority.

If the adoption of the Clean Energy Package will allow to have a Network Code on cybersecurity rules in electricity, this Network Code may address the cybersecurity challenges and gaps of the electricity subsector which were identified in an analysis done for the European Commission[6]. The provisions of the network code are building up to what is already deemed compulsory under the NIS Directive and which would better be scoped by an energy specific secondary legislation.

The proposed scope for the Network Code on cybersecurity rules is synthetized in Figure 1. The Network Code on cybersecurity may address electricity transmission and distribution system operators, i.e. the network code needs to consider electricity system operators with different capabilities and capacities. All operators would be suggested to meet a baseline protection that includes the management of known security risks in respect to the essential services (e.g. ISO/IEC 27001:2013) and a prescriptive approach to implement minimum security requirements in the operational infrastructure that could make good use of the certification tools offered by the EU Cybersecurity Act[7] in its actual formulation. Operators which are providing services that are essential for the well-functioning of the economies and societies are identified by respective Member States as operators of essential services (OES). Those Operators may be subject to advanced cybersecurity requirements reflecting the criticality of the services provided that include the protection of the current infrastructure and specific care in the risk management of their supply chain.

[4] Directive (EU) 2016/1148
[5] Regulation (EU) 2016/679
[6] EECSP-Report: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[7] COM(2017) 477

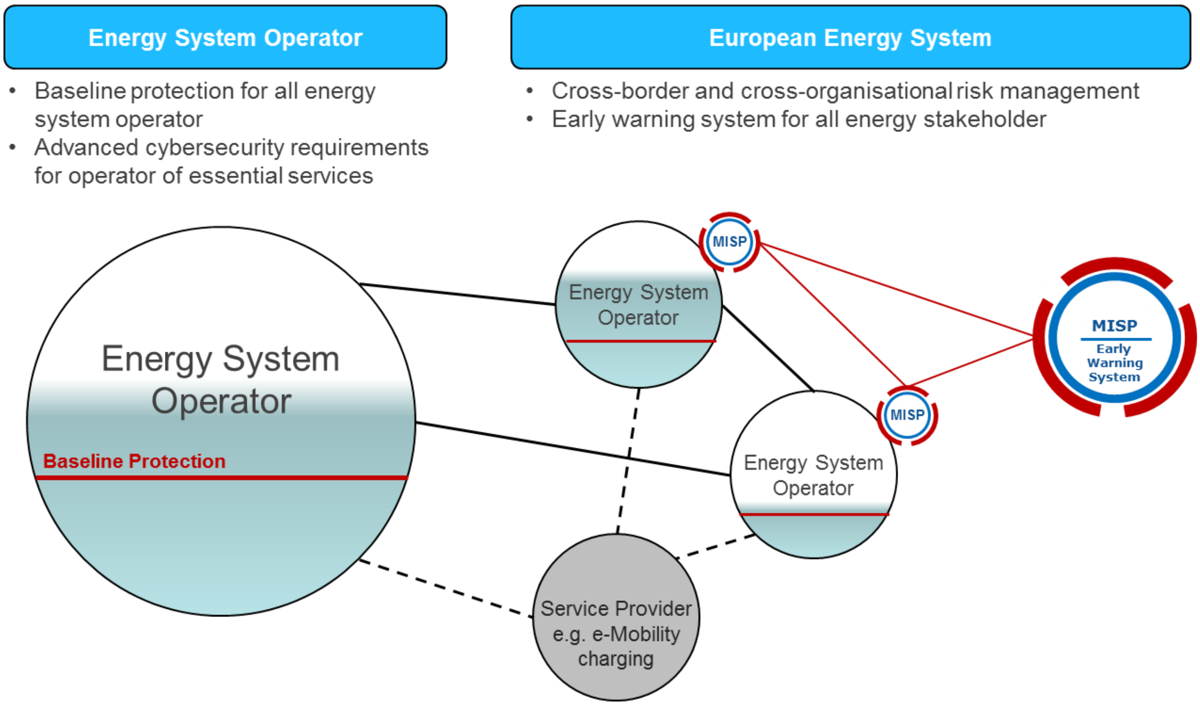


Figure 1: Scope of the Network Code on Cybersecurity

The European Energy System is interconnected and interdependent: as an example, energy system operators have the need to interact directly or indirectly with other service providers such as e-mobility charging, photovoltaic or smart homes. Understanding and mitigating cyber risks that can cascade throughout this interconnected and interdependent network may go beyond the scope of individual energy system operators. Such cross-border and cross-organisational risks are recommended to be addressed by ENTSO-E and EU-DSO[8] as organisations which can encompass a broader range of expertise into the analysis. They may also offer the possibility to formulate cybersecurity recommendation to stakeholders that cannot directly be addressed by a Network Code.

The objective of the recommended Network Code on cybersecurity should not only address current cybersecurity risks, but support energy system operators in order to mitigate and protect their cyberspace against future risks and threats. Taking into consideration fast and unpredictable evolution of cyber threats, this can only be properly addressed with an early warning system. This may be built on the already existing infrastructure and communication systems provided by the implementation of the NIS Directive in Member States. A so-called Malware Information Sharing Platform (MISP[9]) is recommended to be established and supported by the EU Member States for collaboration and cooperation across public and private organisations, Member States and other international allies and partners. Operators of essential services are recommended to actively participate in such early warning system.

[8] 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

[9] https://www.misp-project.org/

Further supportive elements recommended are sector-specific guidance for operators on the implementation of crisis management and on the security of the supply chain and a tool to support mature organisations to steer cybersecurity implementation by assessing the actual status of implementation.

All the recommended actions are based on principles to address cybersecurity in a holistic and risk-based approach that offers operators freedom in the implementation in order to address organisation-specific operational needs. Additionally, harmonization requirements are provided that allows the achievement of a minimum protection level across Europe.

The recommendation outlined in this report can be summarized as following:

Baseline Protection for Energy System Operators

- Set-up of an Information Security Management System (ISO/IEC 27001:2013)
- Minimum security requirements protecting the EU Energy System (utilizing the proposed EU Cybersecurity Act)

Advanced Cybersecurity Implementation for Energy System Operators of Essential Services

- Active protection of current infrastructure
- Supply chain risk management process
- Protection against cross-border and cross organizational risks through proper analysis and risk treatment
- Active participation in an early warning system of all energy system stakeholders

Supportive Elements and Tools

- Sector-specific guidance on crisis management for operators
- Sector-specific guidance on supply chain security for operators
- Energy cybersecurity maturity framework (A tool to assess maturity and to steer cybersecurity implementation)

Cybersecurity is not a one-time implementation, but a continuous effort that requires different stakeholder to cooperate and collaborate to achieve a resilient energy infrastructure. The recommendations provided in this report support this effort by providing direction and guidance.

4. Scope and Analysis Approach of SGTF EG2

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

One guiding principle throughout is to follow a risk-based approach with the implementation of measures that are auditable by a third party. The recommendations contained in this report consider existing EU legislations such as the Directive on security of Network and Information Systems (NIS)[10] and the General Data Protection Regulation (GDPR)[11] and their ongoing implementations as the baseline for building pillars of a Network Code.

The analysis approach taken as agreed with the SGTF EG2 has been performed by the editorial team with the working groups as shown in Figure 2.

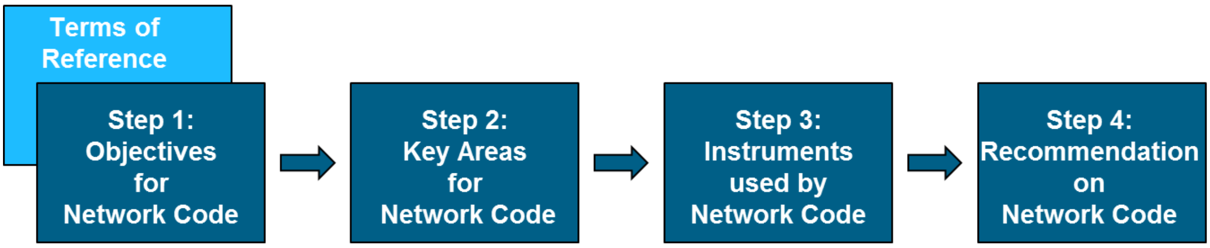


Figure 2: Overview of the analysis and implementation approach

The work was initiated in Step 1 with the analysis of the SGTF EG2 Terms of Reference in the context of identified strategic areas for action, gaps in existing legislation and recommendations on actions published in the report[12] ("Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector") by the Energy Expert Cyber Security Platform (EECSP). This analysis led to the identification of four objectives to be targeted and addressed as candidate topics for the Network Code on cybersecurity by the SGTF EG2. In Step 2, the objectives derived has been further analysed which led to four proposed key areas for the network code on cybersecurity. A detailed explanation about the approach and the results of step 1 and step 2 can be found in the 1st interim report[13].

In Step 3, SGTF EG2 set-up separate sub-working groups for each of the four key areas in order to derive the instruments, i.e. the building blocks recommended to be used by a Network Code on cybersecurity. This has been complemented with recommendation on the usage and realization in Step 4. The 2nd interim report[14] published in July 2018 provides a glimpse into the work on the

[10] Directive (EU) 2016/1148
[11] Regulation (EU) 2016/679
[12] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[13] https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf
[14] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf

instruments that have been further developed and finalized within the context of this final report. Instruments may be further refined in the future.

5. Objectives and Key Areas for the Network Code on Cybersecurity

The objectives are high-level strategic targets that are defining what could be potentially achieved by a Network Code on cybersecurity. The key areas are identified by the SGTF EG2 as the areas addressing the four objectives. The following Figure 3 shows the four objectives and key areas identified.

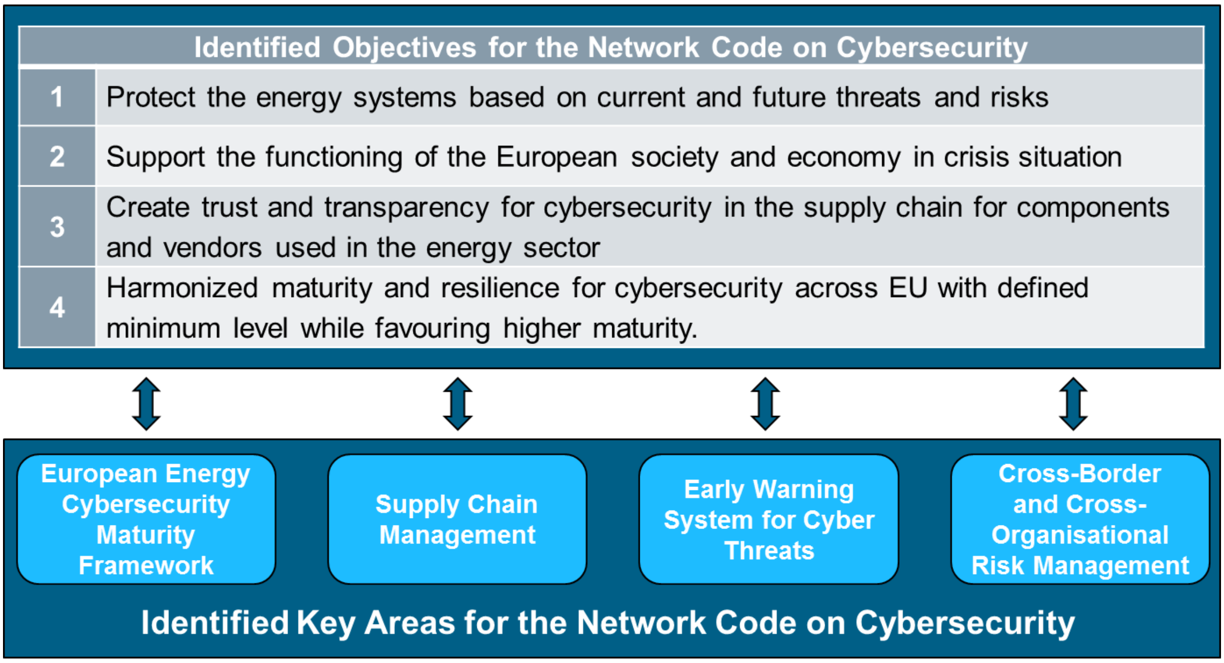


Figure 3: Objectives and Key Areas for the Network Code on Cybersecurity

The key area '**European Energy Cybersecurity Maturity Framework'** aims to provide an instrument for electricity system operators that can be used to steer cybersecurity implementation. It is a very powerful tool that addresses all four objectives as it may eventually embed metrics capable of measuring the resilience level of an organization in an objective and independent way, e.g. by highlighting vulnerabilities in energy systems and their organizational set-up.

The key area '**Supply Chain Management'** aims to create trust and transparency in products, systems, and services provided by vendors and service providers which addresses in particular objectives (1), (3) and (4).

A '**Early Warning System for Cyber Threats'** is a key area that aims to evolve existing incident reporting mechanisms and all related obligations as defined in the NIS Directive towards an information sharing system that may reduce the response time on cyber threats and may strongly mitigate the risks by providing early indicators of threats, attacks, and compromises. This key area addresses the objectives (1) and (2).

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'** aims to provide a methodology that helps to analyse, evaluate and mitigate risks related to the interconnectivity and interdependency in a changing environment. A key part of any risk management framework is the consideration of risk thresholds and the evaluation of extreme risk scenarios that can have a severe impact on the correct functioning of the European electricity system[15]. This key area addresses in particular objectives (1) and (4).

The recommended building blocks for the Network Code on cybersecurity are described in detail in chapter 6.

[15] https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf

6. Recommended Structure for the Network Code on Cybersecurity

A Network Code on cybersecurity as secondary legislation will eventually address all operators of transmission and distribution networks. This is different to the existing obligations set and adopted under the NIS Directive. The NIS Directive targets operators of essential services (OES), i.e. Member States are obliged to identify these operators who are essential for the functioning of the economy and society: only these identified operators of essential services are subject to the obligations of the NIS Directive. Operators of essential services are identified as critical by their respective Member State for the functioning of the economy and society, a more detailed definition is provided in chapter 8. Naturally, for a potential Network Code on cybersecurity rules, a differentiation between operators of essential services and operators who are not identified as OES must be taken into consideration. Particularly for operators of distribution networks, many operators cover only small municipalities while others cover a vast portion of a single Member State or of a bigger geographical region. Small and medium-sized operators typically do not have the resources and capabilities to address cybersecurity the same way as the operators of essential services, who manage energy systems typically covering a large region and a considerable number of consumers. A Network Code on cybersecurity rules may eventually take the capabilities of different operators into consideration by applying a stringent security baseline for operators not considered critical, while operators of essential services will need to follow a more structured approach that focusses and addresses current risks and threats. Another difference is that the NIS Directive addresses information systems that support essential services of the operators, but does not necessarily cover the overall infrastructure of the operators.

Figure 4 shows the recommended structure of the Network Code that has been agreed within SGTF EG2.

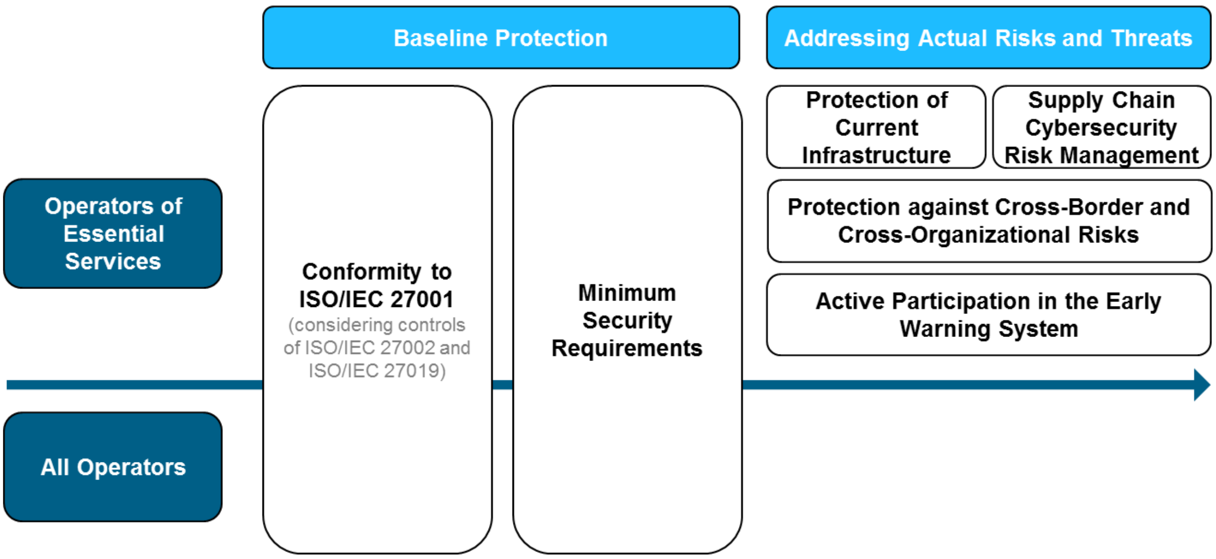


Figure 4: Recommended Structure for the Network Code on Cybersecurity

The recommended building blocks to be used for the Network Code on cybersecurity rules are divided into two sections: the first is defining a common baseline applicable to all operators, see chapter 6.1, and the second is defining additional measures in respect to the existing legal obligations, to be implemented by operators of essential services, see chapter 6.2. In order to reflect the different capabilities of operators, chapter 7.1.4 will propose a proportionality to be considered for this baseline protection. Furthermore, supportive elements are recommended to support the cybersecurity implementation and objectives for the Network Code that are described in chapter 6.3

6.1 Harmonized Cybersecurity Baseline across the European Union

A baseline protection is defined by the following building blocks:

Conformity to ISO/IEC 27001

All operators are expected to have an Information Security Management System (ISMS) according ISO/IEC 27001:2013[16] implemented, i.e. cybersecurity processes and practices are integrated into the respective organizations and cybersecurity risks are generally managed based on a methodology and in a consistent and standardized way. Controls of ISO/IEC 27002 and ISO/IEC 27019 standards are considered to be included in the risk management.

Minimum Security Requirements

The protection of energy systems is based on defined security levels that have to be derived from European reference architectures. Components used in the energy network have to be conform to these minimum security requirements. Minimum security requirements are those following the objectives as proposed in the EU Cybersecurity Act[17] proposal.

These two recommended building blocks for a Network Code on cybersecurity will contribute to the harmonization of cybersecurity implementations across the EU. They are based on ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 and minimum security requirements for the infrastructure that set an entry point for all operators, eventually allowing them to achieve a higher protection for their infrastructures depending on their respective risk appetite.

All building blocks will be described in detail in chapter 7.

6.2 Advanced Cybersecurity Implementation for Operator of Essential Services

Operators of essential services are identified by their respective Member State as those critical for the functioning of the economy and society. Consequently, a cybersecurity implementation is recommended that goes beyond a security baseline. The following building blocks are recommended:

Protection of Current Infrastructure

The minimum security requirements defined in the protection baseline is based on a European reference architecture. It neither reflects the current architecture and components used in a grid of an operator, nor addresses changes applied to the infrastructure. The protection requirement requests operators of essential services to protect the existing infrastructure. The protection concept based on an existing infrastructure might differ to the one derived in the protection baseline.

Supply Chain Cybersecurity Risk Management

[16] https://www.iso.org/isoiec-27001-information-security.html - Applicable version is ISO/IEC 27001:2013
[17] COM(2017) 477

The minimum security requirements of the baseline protection address key requirements for supply chain management that will be sufficient for a majority of products and services. For a consistent approach, additional management of cyber-risks in the supply chain applicable to critical components in an energy grid should be addressed where the disruption could have a significant impact on system resilience and the continuity of the essential services.

Protection against Cross-Border and Cross-organizational Risks

The energy systems are interconnected physically and virtually. In energy grids, cascading effects can be caused directly within a grid of one operator, across operators or indirectly by third-party stakeholders that provide services that are interlinked with the grid. Consequently, cross-border, cross-organizational risks including dependencies from other services (e.g. smart home, e-mobility, photovoltaic, etc.) should be managed.

Active Participation in an Early Warning System

Operators of essential services are obliged by the NIS Directive to report major cybersecurity incidents (as defined by Nations) to their Single Point of Contact (SPoC), e.g. a National CSIRT. The reporting of cybersecurity incidents is not sufficient to actively protect critical energy systems from current risks and threats. The sharing of relevant information within a trust-based network in a timely manner can support the objective to protect the critical infrastructure from current risks and threats.

The recommended building blocks require operators of essential services to address cybersecurity with much more profound concepts and detailed actions than the more prescriptive approach defined for the baseline. Additionally, it requires operators of essential services to strengthen their resilience capabilities.

All building blocks will be described in detail in chapter 8.

6.3 Supportive Elements for the Network Code on Cybersecurity

In order to achieve a consistent implementation of a potential Network Code on cybersecurity across the EU, supportive elements for operators are recommended that support the objectives of the Network Code. One supportive element is the sharing of best practice within the electricity subsector on the implementation of the objectives of the Network Code. Those domain-specific best practices can provide guidance on the implementation of cybersecurity measures. The other potentially supportive element is a tool that enables operators to measure and steer cybersecurity implementation, i.e. an energy cybersecurity maturity framework. An energy cybersecurity maturity framework answers the need for a progression model that allows incremental progress in order to achieve the objectives of a Network Code on cybersecurity. Figure 5 shows the supportive elements recommended by the experts of SGTF EG2.

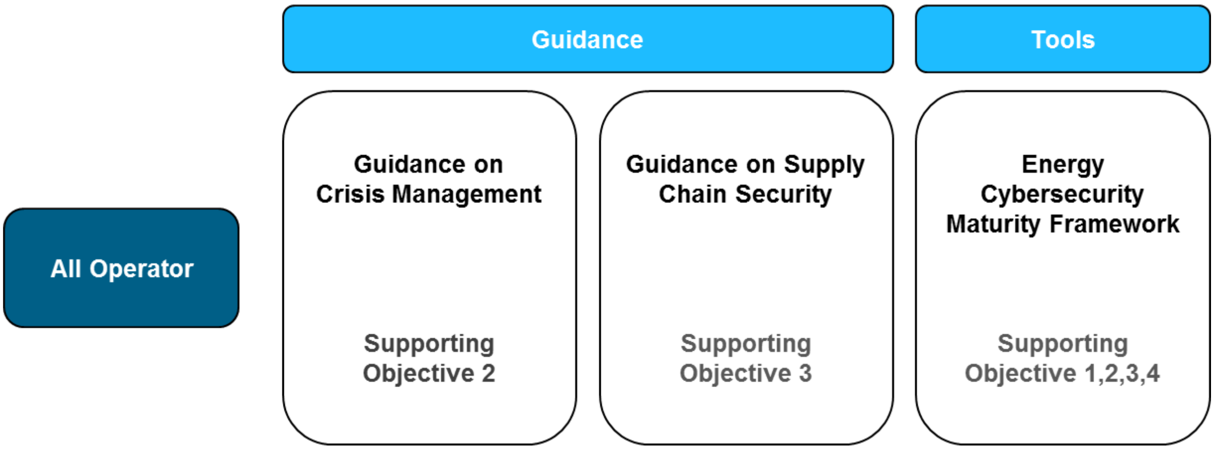


Figure 5: Supportive Elements for the Network Code on Cybersecurity

Following supportive elements are recommended:

Guidance on Crisis Management

The main purpose of a Network Code on cybersecurity rules is to secure the energy value chain in order to safeguard the legitimate financial interests of the EU financial actors operating in the market, and to safeguard the European Union society. One key capability to be developed in this context is to foster the ability to handle cyber crisis situations caused by cybersecurity incidents, i.e. to recover from a disaster in order to re-establish the supply of energy in case of a major disruption. This supplements the Network Code on Emergency and Restoration[18]. Guidance is recommended by sharing best practice on the implementation of the controls described in ISO/IEC 27001:2013, further elaborated in the ISO/IEC 27002[19] and ISO/IEC 27019[20]. Crisis management is one objective of the Network Code, see chapter 5.

Guidance on Supply Chain Security

One item of the security baseline, see chapter 6.1, are minimum security requirements for products, services and processes used in energy systems. Minimum security requirements are partly addressed by the controls of the ISO/IEC 27001:2013 concerning supplier relationships. SGTF EG2 recommends to provide domain-specific guidance for operators on the various aspects of supply chain security. Guidance is recommended by sharing existing or newly developed implementation best practice on controls of the ISO/IEC 27002[21] and ISO/IEC 27019[22] that addresses the respective objective (3) of the Network Code, see chapter 5.

Energy Cybersecurity Maturity Framework

Implementing cybersecurity and maintaining a specific protection level within an organization requires not only the definition of common practices and measures relevant for cybersecurity, but also how to measure the actual status of their implementation and to align the approach within the entire set of relevant stakeholders and of the respective organization. An energy cybersecurity maturity framework contributes to this by providing a tool for the implementation of cybersecurity.

[18] Network Code Emergency and Restoration (EU) 2017/2196, https://www.entsoe.eu/network_codes/er/
[19] https://www.iso.org/standard/54533.html - Applicable version is ISO/IEC 27002:2013
[20] https://www.iso.org/standard/68091.html - Applicable version is ISO/IEC 27019:2017
[21] https://www.iso.org/standard/54533.html - Applicable version is ISO/IEC 27002:2013
[22] https://www.iso.org/standard/68091.html - Applicable version is ISO/IEC 27019:2017

SGTF EG2 recommends that such a tool is provided and used. The use of such a tool shall be left voluntary to the judgement of each energy operator.

These recommended supportive elements will provide operators with domain-specific implementation guidance and a tool to help operators measure and steer their cybersecurity implementation.

All building blocks will be described in detail in chapter 9.

7. Baseline Cybersecurity Requirements for All Operators

In order to achieve a common cybersecurity baseline across the EU, two conditions needs to be met.

First, all stakeholders need to share the same common language, using internationally recognised standards. With regards to information security, the international standard ISO/IEC 27001:2013 can build such a foundation for the electricity subsector. Chapter 7.1 will describe the recommendation for conformity of ISO/IEC 27001 for transmission and distribution system operators that considers controls of ISO/IEC 27002 and ISO/IEC 27019.

Second, minimum security requirements need to be defined. Minimum security requirements that address the energy infrastructures are described in chapter 7.2 with a recommendation on a methodology on how these requirements can be defined for systems, components and services for the energy grid and a recommendation on a conformity scheme aligned to the proposed EU Cybersecurity Act.

7.1 Conformity to ISO/IEC 27001

The key for the harmonization of the cybersecurity landscape in the European Union lies in internationally recognised standards. As stated in chapter 6.1, conformity to ISO/IEC 27001:2013 (considering controls of ISO/IEC 27002 and ISO/IEC 27019) can provide common ground for energy system operators by guaranteeing proper management of cybersecurity through the implementation of an Information Security Management System (ISMS). The elements of an Information Security Management System (ISMS) are well defined in the ISO/IEC 27001:2013 standard. However, some key elements as outlined in the following chapters are particular important to achieve a harmonized approach across the European Union.

7.1.1 Scope of the Information Security Management System

It is important to set a common definition of the scope where an ISMS should operate. The scope definition is illustrated in the Figure 6. In the centre is the asset security model with the assets that needs to be protected; assets includes infrastructure and information. The SGTF EG2 experts have used the architecture model of IEC/TR 62351-10:2012 as the base for definition of the scope recommended to be covered by ISO/IEC 27001:2013. The architecture model links logical security domains to logical power system domains. Table 1 shows the defined security domains.

Security Domain	Required Protection Level	Applies to	In Scope
Public	Low	Assets, supporting the communication over public networks.	-
Corporate	Medium	Assets, supporting the business operation with baseline security not essential to the power system reliability and availability.	-
Business Critical	High	Assets, supporting the critical operation, which are not critical to power system reliability and availability.	-
System Operation Critical	Very High	Assets directly related to the availability and reliability of power generation and distribution infrastructure.	X

Table 1: Logical Security Domains (Source: IEC/TR 62351-10:2012)

The recommended scope of a Network Code on cybersecurity is the ‘System Operation Critical’ security domain that links assets that are directly related to the availability and reliability of energy transmission and distribution infrastructures. As such, it particularly defines the productive environment of an energy system operator, i.e. the Operational Technology (OT) domain.

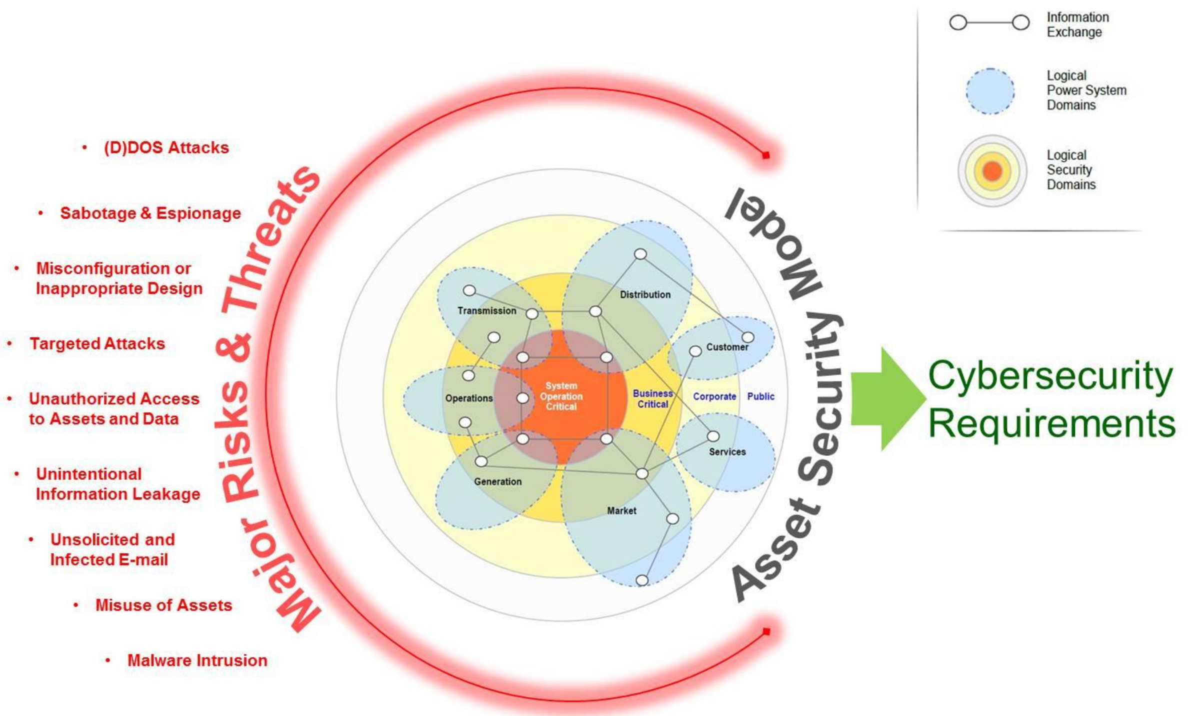


Figure 6: Cybersecurity Model for an Information Security Management System (ISMS)[23]

In order to derive cybersecurity requirements, risks and threats have to be evaluated. This is illustrated in Figure 6, where major cyber risks & threats in 2018 for energy transmission and distribution operators are listed, derived from a SGTF EG2 threat mind map tailored according to ENISA’s threat landscape 2017:

Major Risk & Threat	Description
(D)DOS attacks	These attacks attempt to make smart grid resources unavailable to its intended users (internal and external).
Sabotage & espionage	Intentional actions aimed to cause disruption or damage to assets. Threat of unauthorised manipulation of hardware and software, including web based and web application attacks. Stealing information or physical assets.
Misconfiguration or inappropriate design	Damage caused by improperly configured IT or OT assets or business processes design (inadequate specifications of IT or OT products, inadequate usability, insecure interfaces, policy/procedure flaws and design errors).
Targeted attacks	A diverse set of stealthy processes such as Advanced Persistent Threats (APTs) targeting a specific entity and performed by threat agents with high capabilities.
Unauthorized access to assets and data	Unapproved access to a facility or unauthorized logical access to the information system / network from different locations.
Unintentional information leakage	Sharing information with unauthorised entities. Loss of information confidentiality due to unintentional human actions.

[23] Asset security model is based on IEC/TR 62351-10:2012; major risks & threats for transmission and distribution operator in 2018 are based on a SGTF EG2 threat mind map tailored according to ENISA’s threat landscape 2017

Unsolicited and infected e-mail	Threat of wrong handling of received unsolicited or infected email which affects information security and efficiency (e.g. spam, fishing).
Misuse of assets	Damage caused by misuse of assets (lack of awareness of application features) or wrong / improper assets configuration or management or unintentional change of data.
Malware intrusion	This threat affects any IT or OT system that has software in it which can be updated, modified or configured. It encompasses a large number of variants (e.g. virus, worm, Trojan, rootkit, botnet, ransomware), depending on the type of attack and the ultimate goal of the attacker (compromise system, corrupt data, and steal data).

Table 2: Cyber Risks & Threats 2018 for Transmission and Distribution Operator (Source: ENISA)

A methodology on how to derive cybersecurity requirements from known risks and threats are described in chapter 7.2 in detail.

7.1.2 Risk Management

The main focus of an ISMS is risk management. A key part of risk management is the risk assessment, e.g. by using the risk assessment methodology of ISO/IEC 27005. The most important part for a risk assessment is to have a common understanding of the current risks and threats. Besides risks specific to an organization, there are common risks and threats for all operators of transmission and distribution energy systems. Some have been outlined in previous chapter as provided by ENISA, see Table 2, some are known within the industry from actual security incidents and attacks. As pointed out in chapter 7.2.4, too, it is recommended to include actual industry specific risks and threats in the analysis, see Figure 7.

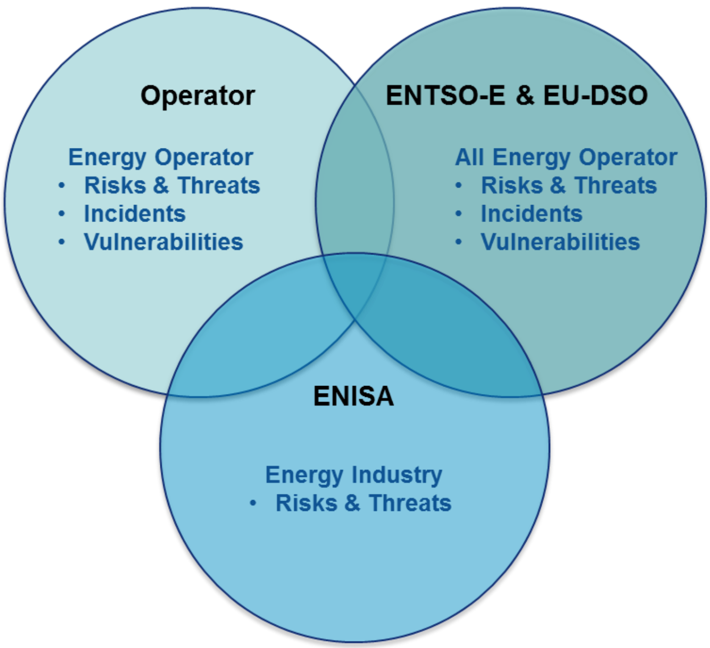


Figure 7: Specific Risks and Threats within the Industry

It is recommended that operators must keep records of known incidents, attacks and vulnerabilities, while ENTSO-E and EU-DSO must keep a record of known basic risks for cyber incidents and cyber attacks. ENISA is recommended to provide a yearly update on major risks and threats for transmission and distribution system operators:

- Operator – Specific to an organization
  Known incidents, attacks and vulnerabilities within an organization.
- ENTSO-E and EU-DSO[24] – Specific for energy transmission and distribution operator
  Known basic risks for cyber incidents and cyber attacks that are known from transmission and distribution system operators.
- ENISA – Specific within the energy industry
  Major risks and threats identified for transmission and distribution system operators.

7.1.3 Asset Management

In order to link risk and threats to assets, it is important for operators to know and to properly manage their own assets. SGTF EG2 recommends that energy system operators implement asset management controls as specified in ISO 27002 (chapter 8). This is required to verify where minimum security requirements are already deployed to assets and where minimum security requirements are applicable for a possible deployment; see chapter 7.1.4 for more details on the recommended approach on application of minimum security requirements in an existing infrastructure.

A useful tool for asset management is the infrastructure network plan and the categorization of assets; an approach that has been already applied in Germany by the German regulator[25]. This approach requests operators to categorize assets in the areas as recommended in the BDEW-OE-Whitepaper[26], see Table 3.

Technology Category	Description and Examples
Operations management / control systems and system operations	This relates to all centralised systems used for process control and monitoring; process control operations management and associated / required supporting central IT systems; applications and related central infrastructure. Examples: - Central grid control and management systems - Power plant control systems - Central systems used for monitoring and control of distributed generation and loads, e. g. virtual power plants, storage management, central control room systems for hydroelectric plants or photovoltaic / wind power installations - Systems for fault management and work force management - Central metering and measurement management systems - Data archiving systems - Central parameterisation, configuration and programming systems - Supporting systems required for operations of the above-mentioned systems, e. g. programming and parameterisation devices
Transmission technology / voice communications	The transmission, telecommunications and network technology deployed in process technology for voice and data communications.

[24] 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

[25] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1

[26] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

	Examples: - Routers, switches and firewalls - Transmission technology-related network components - Voice communication devices - Phone installations, VoIP systems and associated servers - Wireless digital system - Central management and monitoring systems of the transmission, telecommunication and network technology
Secondary, automation and telecontrol technologies	This relates to process-oriented control and automation technology as well as associated protection and safety systems and telecontrol components. In particular, these include the technology in substations as well as the automation technology in generation and storage facilities. Examples: - Control and automation components - Control and field devices - Telecontrol devices - Programmable logic controllers, including digital sensor and actor elements - Protection devices - Safety components - Digital measurement and metering installations - Synchronisation devices - Excitation systems

Table 3: Technology Categorization (Source: BDEW-OE-Whitepaper)

In order to have a harmonized approach for energy system operators, the SGTF EG2 recommends all operators to categorize assets and to have an infrastructure network plan available. SGTF EG2 recommends ACER to align the categorization approach of assets with the respective regulators, ENTSO-E and EU-DSO in order to derive a common approach on asset management that supports the final objectives of the Network Code on cybersecurity.

7.1.4 Application of Minimum Security Requirements

A key building block for baseline protection is the minimum security requirements as described in detail in chapter 7.2. Taking into consideration the life-time of components and systems installed at energy system operators, the application of a European cybersecurity certification scheme under the EU Cybersecurity Act proposal in the area of the electricity subsector needs to consider that systems needs to be supported over a long period of time in order to protect the investments of the operators, e.g. replacement of components within a legacy system that might not fulfil the minimum security requirements.

SGTF EG2 recommends operators to use products, systems and services conform to EU cybersecurity certification schemes as soon as respective schemes and components are available. A respective provision for operators of essential services is stated in article 48a of the Draft European Parliament Legislative Resolution on the EU Cybersecurity Act.

Furthermore, operators should have a migration plan for existing infrastructure based on criticality in alignment with their local regulatory regime and with EU policy objectives. SGTF EG2 recommends to have migration plans for systems and not single assets for a consistent implementation of a baseline protection. Operators are recommended to use an infrastructure network plan, see chapter 7.1.3, and to classify systems using a risk-impact matrix while considering guidance from respective national regulatory authority (NRA) if available. SGTF EG2 recommends ENTSO-E and EU-DSO to provide a risk-impact matrix as the template for operators; a template example is provided in Annex A-4 (chapter 11.4).

The Outcome should be a migration plan to implement a baseline security depending upon an agreed level of CapEx and OpEx. SGTF EG2 recommends the National Regulatory Authorities (NRA) to agree with respective stakeholders on the amount that should be used for CapEx and OpEx with the objective to migrate existing infrastructure towards a baseline protection over time.

7.2 Minimum Security Requirements

Another overall goal of a Network Code on cybersecurity is to work as a baseline for the protection across the European Union. A key element is to have a defined level of cybersecurity implementation in the critical infrastructures itself. As pointed out in chapter 6, baseline protection requires a prescriptive approach that considers international standards, common practices among stakeholders and existing and proposed regulation, i.e. NIS Directive, GDPR and EU Cybersecurity Act proposal.

Chapter 7.2.1 provides an overview on cybersecurity standards in the electricity subsector. Defining a baseline protection requires an aligned and complementary approach to existing and proposed regulation. Chapter 7.2.2 will describe the proposed EU Cybersecurity Act[27] and how the minimum cybersecurity requirements can be translated into international standards, which can then build the basis for deriving a EU cybersecurity certification scheme for the electricity subsector.

In order to understand the methodology and implementation of recommendations, it is important to understand common practices in the electricity subsector. A respective industry perspective will provide a categorization of products, systems and services in domains that can be used to derived minimum security requirements; the categorization is described in chapter 7.2.3. This will lead directly to the methodology to be applied for the definition of minimum cybersecurity requirements in chapter 7.2.4. A best practice implementation with the IECEE[28] conformity assessment scheme is described in chapter 7.2.5.

An existing conformity assessment framework is contained in the so-called New Legislative Framework[29] (NLF) for the marketing of products within the EU. The approach of the NLF will be discussed in more detail in chapter 7.2.6. Furthermore, this chapter will briefly discuss the Common Criteria that is frequently discussed, too, in the context of the EU Cybersecurity Act.

Chapter 7.2.7 further looks into smart metering, explaining a strategy already included in proposed regulation, which may be specific for smart metering solutions.

Recommendations towards a baseline cybersecurity for the Network Code on cybersecurity are summarized in chapter 7.3.

[27] COM(2017) 477
[28] IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
[29] Decision no. 768/2008/EC

7.2.1 International Standards used in the Electricity Subsector

A variety of international standards exist that are relevant for the electricity subsector. Each standard typically covers a specific area. An overview from work of the Smart Grid – Coordination Group, Smart Grid Information Security (SGIS) under the mandate M/490 is provided in Figure 8 which indicates four dimensions covered by standards towards:

- Completeness with governance and policies aspects
- Design details with focus on technical aspects
- Details for operations
- Relevance for Products.

The overview shows well known standards such as ISO/IEC 27001:2013 with a focus on completeness and details for operations and specific standards that are covering specific aspects of cybersecurity.

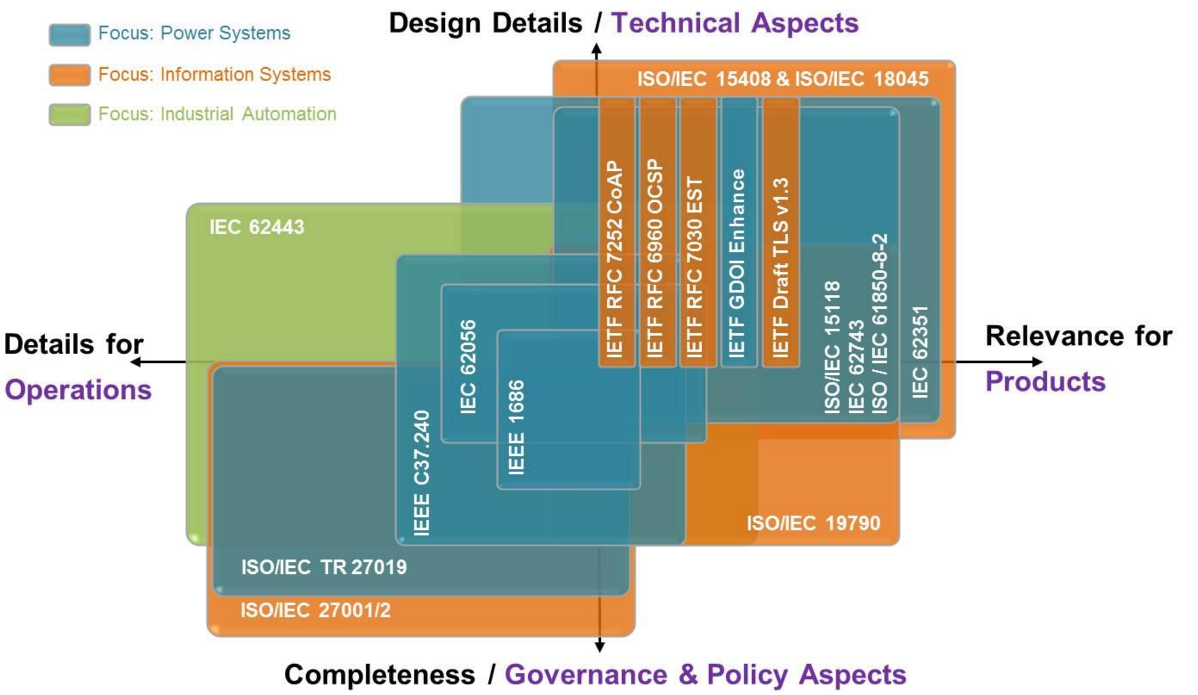
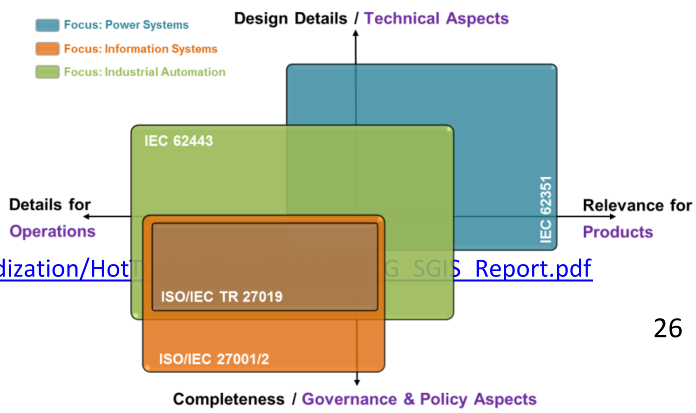


Figure 8: International Cybersecurity Standards - Area of Applicability[30]

Furthermore, the listed standards in the figure are indicating, too, that some standards are addressing cybersecurity in a more generic way while other are focussing on specific domains such as energy power systems or industrial automation.

In the electricity subsector following standards can be considered as basis standards:



[30] ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Hot ... G_SGIS_Report.pdf

- **ISO/IEC 27001/2/19**
  targeting cybersecurity management

- **IEC 62443**
  targeting the industrial automation

- **IEC 62351**
  targeting the communication security

Figure 9: Basis Standards in Electricity Subsector

These basis standards provide coverage from cybersecurity management over system security down to technical implementation details relevant for product manufacturers. The interdependency of these standards is described in chapter 7.2.3 in more detail.

Additional standards such as ISO/IEC 15118 for road vehicles with a grid communication interface or IEEE 1686 on intelligent electronic devices can be applied on a need basis, i.e. depending on application or use case.

7.2.2 EU Cybersecurity Act Proposal and Minimum Cybersecurity Requirements

On $19^{th}/20^{th}$ October 2017, the European Council asked for the adoption of the EU Cybersecurity Act as proposed[31] by the European Commission in the context of a Digital Europe[32]. The general approach was agreed on 8^{th} June 2018 by the EU Council[33] with the Council general approach[34]. Besides the EU Council general approach, recommendation from the ITRE committee[35] on the EU Cybersecurity Act proposal have been provided with ‘Draft Compromise Amendments’ from 2^{nd} July 2018. Since September 2018, the EU Cybersecurity Act is in trilogue negotiation, i.e. this report is based on existing documentation from the EU Council and ITRE committee, but does not include results from the trilogue discussions. Adjustments to the recommendations made in this report for requirements and assurance might be needed to be adjusted in regards to the output of the trilogue when available. The requirements and requested assurance level of the EU Council approach and of the ITRE committee draft compromise amendments are used in this report and compared in detail in chapter 7.2.5.

In Figure 10, the interplay of the requirements on a harmonized protection level across the EU by the Network Code on cybersecurity with the conformance and certification schemes of the EU cybersecurity certification framework is shown. The Network Code on cybersecurity should have as a target to support a baseline protection across EU with minimum security requirements that do not limit operators in achieving a higher protection level or to implement individual and specific protection needs.

---

[31] COM(2017) 477

[32] http://www.consilium.europa.eu/en/meetings/european-council/2017/10/19-20/

[33] http://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/

[34] http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

[35] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bREPORT%2bA8-2018-0264%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN

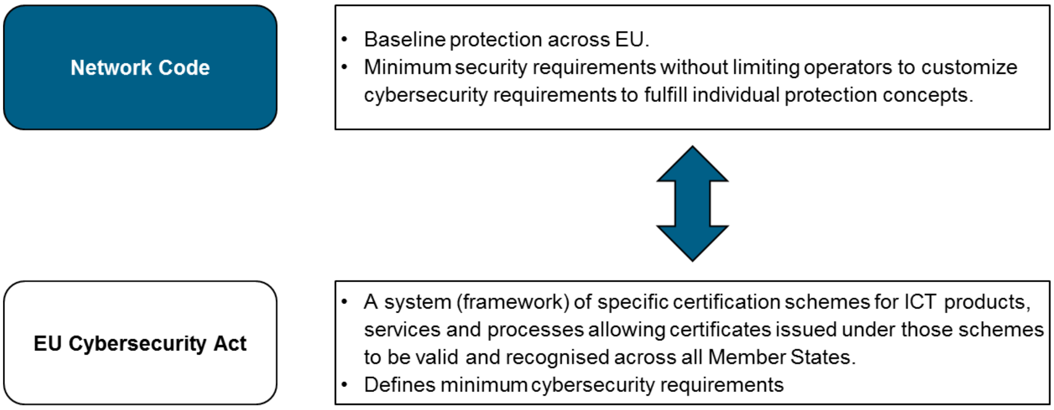


Figure 10: Interplay of Network Code on Cybersecurity and EU Cybersecurity Act

The EU cybersecurity certification framework is going to provide EU-wide certification schemes with a comprehensive set of rules, technical requirements, standards and procedures. These will be based on an agreement at EU level for the evaluation of the security properties of specific ICT-based products, services or processes. The certification framework will attest that ICT products, services and processes that have been certified in accordance with such a scheme comply with specified cybersecurity requirements. The resulting certificate will be recognized in all Member States. The conformance and certification scheme will define minimum security requirements with three assurance level: basic, substantial and high.

In the scope of the EU cybersecurity certification framework are ICT products, services and processes that are defined as following:

- **ICT products**
  'ICT product' means any element or group of elements of network and information systems
- **ICT services**
  'ICT service' means any service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems
- **ICT processes**
  'ICT process' means any set of activities performed to design, develop, deliver and maintain an ICT product or service

ICT products includes 'group of elements of network and information systems' that can be considered as a definition of a system. In IEC 62443-1-1, a system is defined as an 'interacting, interrelated, or interdependent elements forming a complex whole'.

Minimum security requirements are recommended for the Network Code on cybersecurity that addresses the same objectives as defined within the objectives of an EU cybersecurity certification scheme.

The international standard IEC 62443-3-3 defines 4 security levels (SL) that can be used to translate the assurance level of the EU Cybersecurity Act to an international standard:

- Security level 1 (SL 1) – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

- Security Level 2 (SL 2) – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- Security Level 3 (SL 3) – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- Security Level 4 (SL 4) – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

The security level (SL) of IEC 62443 can be mapped to the security level as defined in the assurance level basic, substantial and high of the EU Cybersecurity Act as defined in the EU Council and ITRE committee amendments, see Table 4.

Assurance	EU Cybersecurity Act – Security Level		IEC 62243 Security Level
	EU Council Approach	ITRE Committee Amendments	
Basic	known basic risks for cyber incidents and cyber attacks	known basic risks of cyber incidents are resisted	1-2
Substantial	known cyber risks, cyber incidents and cyber attacks carried out by actors with limited skills and resources	known risks of cyber incidents are prevented and there is also capability to resist cyber-attacks with limited resources	2-3
high	risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources	risks of cyber incidents are prevented and there is also ability to resist state-of-the-art cyber-attacks with significant resources	3-4

Table 4: Mapping of Assurance Level to IEC 62443 Security Level

With a mapping to IEC 62443, the security objectives as defined in the article 45 of the EU Cybersecurity Act can be translated into functional and process related requirements of an international standard, see Figure 11.

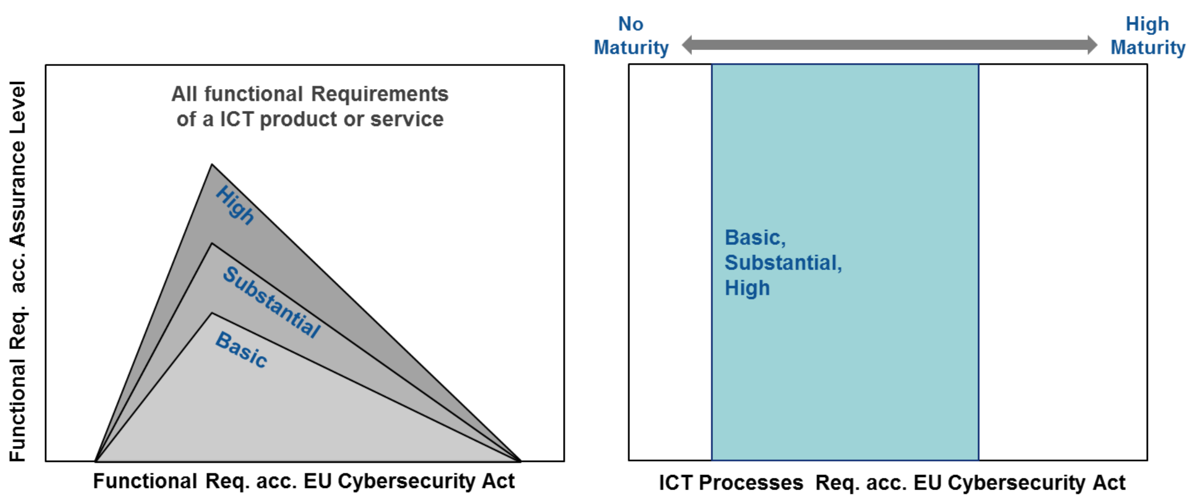


Figure 11: Functional and Process related Objectives of the EU Cybersecurity Act

Functional requirements can differ for each of the different assurance levels - basic, substantial and high. An example can be taken from IEC 62443-4-2. The requirement CR 2.1 of IEC 62443-4-2 asks for authorization enforcement as a basic security requirement, i.e. security level SL-1. For a higher protection need, the international standard requires authorization enforcement of all users (CR 2.1 RE 1; SL-2) and permission mapping to roles (CR 2.1 RE 2; SL-2). On the other side, for ICT processes, such differentiation does not apply. Here, the 1 to 1 mapping of the EU cybersecurity certification framework objectives to process requirements does not differentiate between different assurance levels. Differences are presented in the maturity of an organization. The EU cybersecurity certification scheme does not address maturity. However, functional and process requirements can be mapped to the objectives of a candidate EU cybersecurity certification scheme; this is described in detail in chapter 7.2.5 for IEC 62443 and ISO/IEC 27001 controls.

Furthermore, the EU cybersecurity certification framework sets out the criteria that must be met for each assurance level:

EU Cybersecurity Certification Framework – Assurance Level		
Assurance	**EU Council Approach**	**ITRE Committee Amendments**
Basic	At least review of technical documentation	No requirement for third party conformity assessment – self-assessment by manufacturer
Substantial	Third party conformity assessment of non-applicability of publicity known vulnerabilities and security testing	Third party conformity assessment of technical documentation
high	Third party conformity assessment of non-applicability of publicity known vulnerabilities, security testing and penetration testing	Third party conformity assessment through penetration testing (resisting of security functionalities)

Table 5: Minimum Evidence Requirements of the EU Cybersecurity Act

For the purposes of discussion and recommendation of a Network Code on cybersecurity, the outline of the EU cybersecurity certification framework under the EU Cybersecurity Act of the EU Council approach and of the ITRE committee amendments are used accordingly.

7.2.3 Categorization of Products, Systems and Services

Transmission and distribution system operator are managing complex distributed systems. Consequently, the business perspective as well as protection concepts of energy grids are mainly focussed on systems. The relevant stakeholders are the supplier, integrator and operator with international standards as a common base for defining requirements. The interplay of the international 'basis' standards and relevant stakeholder in the value chain are illustrated in Figure 12.

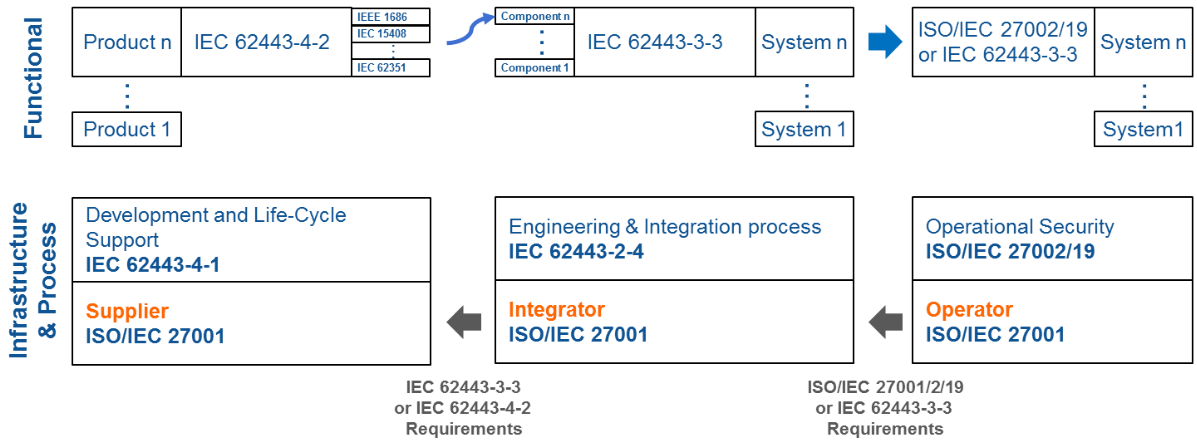


Figure 12: Interplay of International Standards and Relevant Stakeholders

Operators must conform to ISO/IEC 27001:2013, see chapter 7.1, i.e. the operational security is built on cybersecurity controls further specified in ISO/IEC 27002 and the domain specific controls of ISO/IEC 27019. Consequently, requirements for energy transmission or distribution systems are based on controls of ISO/IEC 27002 and ISO/IEC 27019. In recent years, operators have started to increasingly use the industrial automation standard IEC 62443-3-3 as an alternative to define cybersecurity requirements.

The standard ISO/IEC 27001:2013 also applies to an Integrator as it defines how the operational environment of the integrator is protected itself. Concerning the systems to be engineered and integrated into the operator's energy grid, the international standard IEC 62443-2-4 defines controls and practices to be used to address cybersecurity adequately for the engineering and commissioning of systems. While IEC 62443-2-4 defines the processes, the standard IEC 62443-3-3 defines the functional requirements of a system. These requirements reflect the requirements received from an operator. A system can consist of several hundreds of components. Part of the engineering process is to define the protection concept and to map it to requirements of the components. By applying a defence-in-depth concept, not all components will require the same level of security resulting in a cost-efficient protection concept.

The supplier should also comply to the ISO/IEC 27001:2013 as a base standard to secure his operational environment. For development and life-cycle, the standard IEC 62443-4-1 provide the controls and practices to be applied in order to produce components that follow a security-by-design principle. Each component has to meet requirements defined by IEC 62443-4-2. For suppliers, additional implementation standards such as IEC 62351 are used that outline in detail how specific security requirements are to be implemented. IEC 62351 is one of the key standards in the electricity subsector defining the communication security implementation, see chapter 7.2.1, and relevant to providing interoperability among components of different vendors. As stated in chapter 7.2.1, other standards may apply depending on the application or use case.

The outline of this chapter is to prepare the ground for the discussion in following chapters as it describes:

- The nature of the electricity subsector to be system oriented.
- Outline why there are basis standards for the electricity subsector, see chapter 7.2.1.

- The importance of having standards addressing systems and products as a whole.

In the case of IT services, the key standard ISO/IEC 27002 is used while additional standards may apply depending on the application and use case. An internet-of-things based cloud service for example is commonly based on security measures defined in the machine-to-machine communication standard IEC/TR 62541-2 or ISO/IEC 27017. Additionally, also commonly used by industry players are security controls and practices as outlined by the Cloud Security Alliance (CSA)[36] for Cloud environments.

In order to take this into account, the SGTF EG2 has categorized products, systems and services in different domains see Table 6.

Categorization	OT Products incl. Life-Cycle Support	OT Systems incl. Services	IT Services
Examples	RTU Protection Relay Industrial Router …	Control Centre Primary Substation Asset-Monitoring Smart Metering Micro-Grid Industrial Router …	Cloud (on-/off-premise) …

Table 6: Categorization of Products, Systems and Services

The SGTF EG2 recommends following such a categorization in order to define minimum cybersecurity requirements. In case of uncertainty, the mutual consent of all stakeholders, see chapter 7.2.4, should be achieved. There are cases, where an application or a single use case needs to be addressed in both areas, e.g. an asset management system can be an OT system with a Cloud Service included. In such cases the application has to be split into respective domains.

7.2.4 Recommended Methodology for the Definition of Minimum Cybersecurity Requirements

The recommended methodology used to derive minimum cybersecurity requirements is following the security risk management process of ISO/IEC 27005 enriched with additional requirements from IEC 62443-3-2[37], see Figure 13.

[36] https://cloudsecurityalliance.org/
[37] IEC CDV 62443-3-2

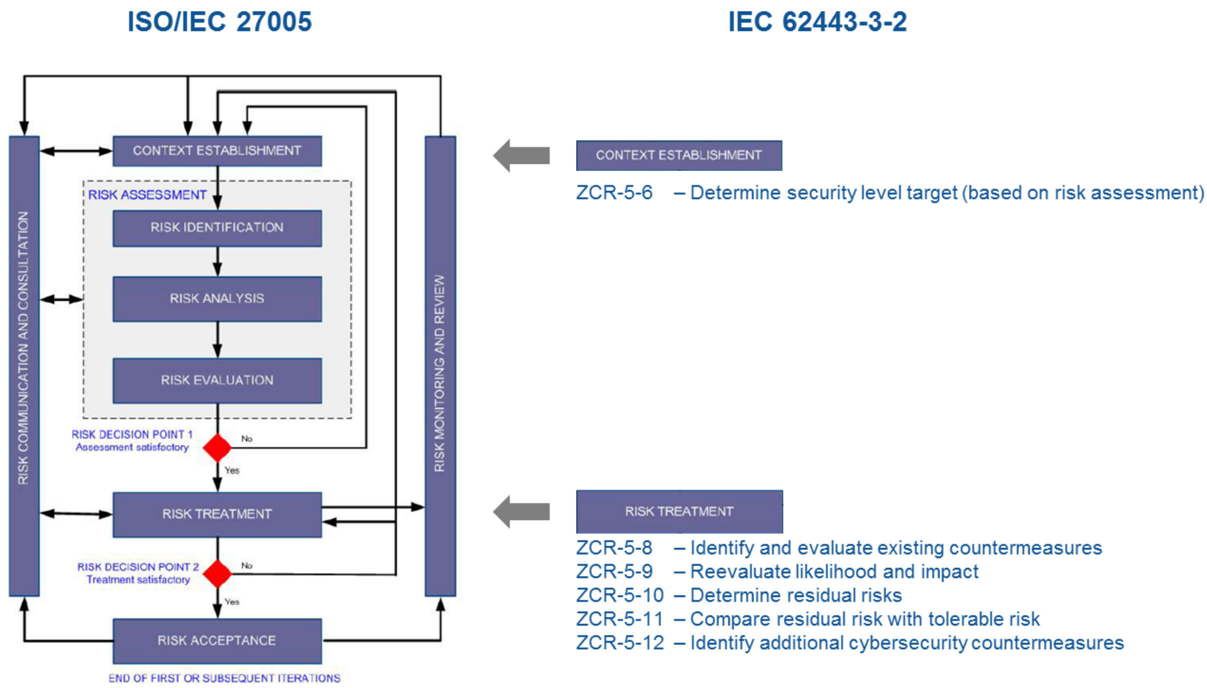


Figure 13: Security Risk Management Process (Source: ISO/IEC 27005:2011) Enriched with IEC 62443-3-2 Requirements

The key building blocks of the methodology with the selected zone and conduit requirements (ZCR) of IEC 62443-3-2 are described in the following in more detail.

Context Establishment

Context establishment is defining the environment in which the risk assessment will be performed. The key building blocks for context establishment recommended to be used are:

- System outline
- Categorization of products, systems and services
- Risk-impact matrix
- Target protection level (ZCR-5-6 - IEC 62443-3-2, security target level)

A system outline is defining the architecture, functional blocks and components considered in the risk assessment including the interfaces to the outside. The SGTF EG2 recommends using the system level for the analysis even for single products or components as systems do encompass most business processes they support and are defining the operational environment of a component. Additionally, they are comparable between grid operators and allow having security controls in that part of the system where they are most cost-effective. Furthermore, minimum security requirements are recommended to be based on European reference architectures (e.g. SGAM or IEC 62351-10) for specific systems. It is recommended to agree upon a reference architecture on the system level under consideration of existing architectures defined in international standards, e.g. the reference architecture for substation automation in IEC 62351-10.

A categorization of products, systems and services, see chapter 7.2.3, is used to identify the right standards to be used for risk treatment, e.g. IEC 62443 for OT based products, systems and related services.

A risk-impact matrix should be prepared as the instrument to evaluate risks in the risk assessment module based on a template provided by ENTSO-E and EU-DSO, see chapter 7.1.2.

A target protection level (IEC 62443-3-2; ZCR-5-6 – security target level) should be defined for a system, i.e. against what kind of risk and threat the system should be protected. The EU Cybersecurity Act provides three possible target levels against which a system could be protected, see Table 4. The risk protection target is used in the risk assessment to identify risks based on a specific attacker profile.

Risk Assessment

The risk assessment includes three steps: risk identification, risk analysis and risk evaluation, see Figure 13. In the risk identification, SGTF EG2 recommends to include risks as described in chapter 7.1.2 for the analysis.

The risk analysis and evaluation should use the risk-impact matrix and target protection level identified in the context establishment in order to identify risks based on a specific attacker profile.

Risk Treatment

All identified and assessed risks need to be treated. There are multiple options to treat a risk typically falling into the response strategies of avoid, reduce, transfer or accept. The most important response in risk treatment in the context of minimum security requirements is the strategy to reduce the risk by selecting appropriate security controls. SGTF EG2 recommends consulting with industry stakeholders when choosing controls and implementation recommendations in order to consider technical and financial constraints appropriately, i.e. to target cost-effective and technically feasible implementations. Minimum requirements should be selected from broadly supported international standards. The following standards are recommended, see Table 7.

Area	Functional Requirements	Process Requirements
OT Products	IEC 62443-4-2 or ISO/IEC 27002 and ISO/IEC 27019	IEC 62443-4-1 or ISO/IEC 27002 and ISO/IEC 27019
OT Systems	IEC 62443-3-3 or ISO/IEC 27002 and ISO/IEC 27019	IEC 62443-2-4 or ISO/IEC 27002 and ISO/IEC 27019
IT Services	ISO/IEC 27002 and ISO/IEC 27019 Domain specific, no general standard applicable	ISO/IEC 27001, controls from ISO/IEC 27002 and ISO/IEC 27019

Table 7: Recommended International Standards for Selecting Minimum Security Requirements

The use of IEC 62443 or ISO/IEC 27002 and ISO/IEC 27019 for products and systems allows the requirements to be well aligned across stakeholders, see previous chapter 7.2.3.

As outlined above in the section 'Context Establishment', the starting point to classify the assurance level for components is the system itself, see Figure 14.

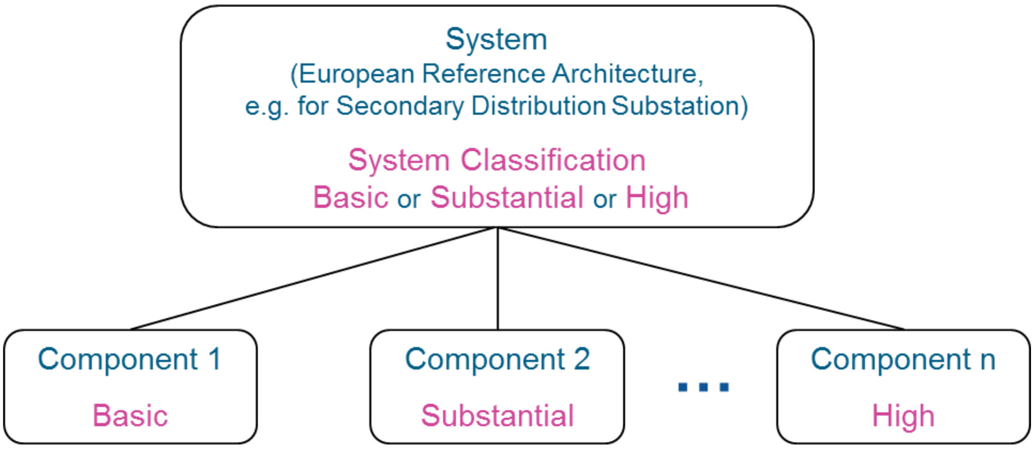


Figure 14: Classification of Systems and Products

As outlined earlier, a system might have a different classification than the individual components, when a defence-in-depth approach is applied, e.g. not all components in a system classified as 'high' need to follow the same classification. The target protection level defined in the 'Context Establishment' is used subsequently for the risk treatment plan. Additional requirements of IEC 62443-3-2 should be applied in the analysis work of the risk treatment, see Figure 13:

- ZCR-5-8 – Identify and evaluate existing countermeasures
- ZCR-5-9 – Re-evaluate likelihood and impact
- ZCR-5-10 – Determine residual risks
- ZCR-5-11 – Compare residual risk with tolerable risk
- ZCR-5-12 – Identify additional cybersecurity countermeasures

When evaluating security requirements to address identified risks, existing countermeasures should also be evaluated (ZCR-5-8). The security controls of IEC 62443-3-3 for systems or IEC 62443-4-2 for products should follow the identified assurance level, i.e. security level as defined by IEC 62443, for respective system or component, see mapping of assurance level to IEC 62443 security level in Table 4 in context of Figure 14. With this approach, minimum security requirements can be defined.

Once the minimum security requirements have been selected, the residual risks, assuming implementation of security controls that have been considered appropriate, must be documented.

Risk Acceptance

ENTSO-E and the EU-DSO[38] are recommended to align with involved stakeholders on the classification, the minimum security requirements and the residual risks for systems and components evaluated.

In the following, further recommendations on the process of defining minimum security requirements are provided.

[38] 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

Procedural Recommendation

ENSTO-E and EU-DSO are recommended to align on respective European reference architectures (e.g. SGAM or IEC 62351-10) and on defined minimum security requirements for the systems in scope and the classification concerning assurance level of such systems. Furthermore, ENTSO-E and EU-DSO are recommended to involve experts from ENISA and relevant stakeholders in the analysis work including a final review by respective stakeholders.

When a EU cybersecurity conformance scheme is in place, it must be regularly reviewed concerning developments in technology, threats and risks (at least every 3 years). ENISA is recommended to provide a yearly update on threats and risks relevant for the transmission and distribution system operators, see chapter 7.1.2.

Further recommendation to the minimum security requirements and certification scheme are provided in chapter 7.2.5.

7.2.5 Recommended for a Certification Scheme

In chapter 7.2.4, the methodology on how to derive minimum security requirements has been described. This chapter is providing recommendations for a candidate EU certification scheme that addresses the following points:

- Mapping of EU cybersecurity certification schemes security objectives to the 'basis' standards in the electricity subsector (see chapter 7.2.1)
- Recommendation on a candidate EU cybersecurity certification scheme
- Recommendation on assessment criteria
- Recommendation on conformity assessment procedures

Mapping of EU Cybersecurity Act Objectives to Key Standards

As described in detail in chapter 7.2.2, the trilogue discussion between EU Council, EU Parliament and the European Commission on the EU Cybersecurity Act is ongoing. Consequently, the mapping provided in this chapter cannot be final and would need an adjustment based on the outcome of the trilogue discussion later on. Nevertheless, the SGTF EG2 has prepared a mapping to international standards (basis standard, see chapter 7.2.1) based on the categorization as defined in chapter 7.2.3 towards both, the EU Council approach and the ITRE committee draft compromise amendments.

Mapping of requirements towards the objective of the EU Council approach:

EU Council Draft - Requirements			OT Product IEC 62443-4-1/-4-2		System / OT Service IEC 62243-2-4/-3-3		IT Service ISO/IEC 27001
Art. 45 - Security Objectives		Type	-4-1	-4-2	-2-4	-3-3	Annex A
(a)	protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure during the entire process, product or service lifecycle;	functional		CR 4.1 CR 4.2		SR 4.1 SR 4.2	A.6.2.1 A.6.2.2 A.8.2.1 A.8.2.3 A.10.1.1 A.11.1.1 A.11.2.3 A.11.2.5 A.11.2.7 A.11.2.9 A.12.3.1 A.12.4.2 A.13.2.1 A.13.2.3 A.17.2.1 A.18.1.4
(b)	protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration or lack of availability during the entire process, product or service lifecycle;	functional		CR 2.1 CR 3.1 SAR 3.2 EDR 3.2 HDR 3.2 NDR 3.2 CR 3.4 CR 3.8 CR 3.9 CR 7.3		SR 3.1 SR 3.2 SR 3.4 SR 3.8 SR 3.9 SR 7.3	A.6.2.1 A.6.2.2 A.8.2.1 A.8.2.3 A.10.1.1 A.11.1.1 A.11.2.3 A.11.2.5 A.11.2.7 A.11.2.9 A.12.3.1 A.12.4.2 A.13.2.1 A.13.2.3 A.17.2.1 A.18.1.4
(c)	ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;	functional		CR 1.1 CR 1.2 CR 1.3 CR 1.4 CR 1.5 NDR 1.6 CR 2.1		SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.6 SR 2.1	A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.2 A.11.1.2

EU Council Draft - Requirements			OT Product IEC 62443-4-1/-4-2		System / OT Service IEC 62243-2-4/-3-3		IT Service ISO/IEC 27001
Art. 45 - Security Objectives		**Type**	**-4-1**	**-4-2**	**-2-4**	**-3-3**	**Annex A**
(d)	record which data, functions or services have been communicated accessed, used or otherwise processed, at what times and by whom;	functional		CR 1.1 CR 1.2 CR 1.3 CR 2.8 CR 2.11		SR 1.1 SR 1.2 SR 1.3 SR 2.8 SR 2.11	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4
(e)	ensure that it is possible to check which data, services or functions have been accessed, or used or otherwise processed, at what times and by whom;	functional		CR 6.1		SR 6.1	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4
(f)	restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;	functional		CR 7.3 CR 7.4 CR 7.5		SR 7.3 SR 7.4 SR 7.5	A.12.3.1 A.16.1.1 A.16.1.4 A.16.1.5
(g)	(g) ensure that ICT processes, products and services are provided with up to date software and hardware that does do not contain publicly known vulnerabilities, and are provided mechanisms for secure software updates;	process	DM-1 DM-2 DM-3 DM-4 DM-5 SVV-3 SUM-1 SUM-2 SUM-3 SUM-4 SUM-5		SP.03.03 SP.11.03 SP.11.04		A.12.5.1 A.12.6.1
(ga)	ICT processes, products and services are developed, manufactured and supplied according to the security requirements stated in the particular scheme.	process	SM-1 SI-1 SVV-1		SP.01.02 SP.02.01		A.14.1.1 A.14.2.1 A.14.2.5 A.14.2.7 A.14.2.8 A.14.2.9 A.15.1.2 A.18.1.1 A.18.2.3

Table 8: Mapping of Requirements to the Objectives of EU Council Approach

Mapping of requirements towards the objective of the ITRE committee draft compromise amendments:

ITRE Committee Amendments - Requirements			OT Product IEC 62443-4-1/-4-2		System / OT Service IEC 62443-2-4/-3-3		IT Service ISO/IEC 27001
Art. 45 - Security Objectives		Type	-4-1	-4-2	-2-4	-3-3	Annex A
(a)	the confidentiality, integrity, availability and privacy of services, functions and data;	functional		CR 2.1 SAR 3.2 EDR 3.2 HDR 3.2 NDR .32 CR 3.4 CR. 3.8 CR 3.9 CR 4.1 CR 4.2 CR 7.1 CR 7.2 CR 7.3 CR 7.4		SR 2.1 SR 3.2 SR 3.4 SR 3.8 SR 3.9 SR 4.1 SR 4.2 SR 7.1 SR 7.2 SR 7.3 SR 7.4	A.8.2.1 A.8.2.3 A.10.1.1 A.11.1.1 A.11.2.3 A.11.2.5 A.11.2.7 A.11.2.9 A.12.3.1 A.12.4.2 A.13.2.1 A.13.2.3 A.17.2.1 A.18.1.4
(b)	that services, functions and data can be accessed and used only by authorised persons and/or authorised systems and programmes;	functional		CR 1.1 CR 1.2 CR 1.3 CR 1.4 CR 1.5 SR 1.6 CR 2.1		SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 2.1	A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.2 A.11.1.2
(c)	that a process is in place to identify and document all dependencies and known vulnerabilities in ICT products, processes and services;	process	SR-1 SR-2 SD-1 SVV-3 SVV-4		SP.03.01 SP.03.03 SP.03.03 RE1 SP.06.02		A.12.6.1 A.15.1.3
(d)	that ICT products, processes and services do not contain vulnerabilities;	process	SI-1 SVV-3 SVV-4		SP.02.01 SP.03.03 SP.03.03 RE1		A.12.6.1 A.14.2.8 A.14.2.9
(e)	that a process is in place to deal with newly discovered vulnerabilities in ICT products, processes and services;	process	DM-1 DM-2 DM-3 DM-4		SP.03.03		A.12.6.1
(f)	ensure that ICT products, processes and services are secure by default and by design	process	SM-1 SD-1 SD-2 SD-3 SD-4		SP.02.01 SP.03.01 SP.03.05		A.14.1.1 A.14.2.1 A.14.2.5 A.14.2.6 A.15.1.2 A.15.1.3

ITRE Committee Amendments - Requirements			OT Product IEC 62443-4-1/-4-2		System / OT Service IEC 62443-2-4/-3-3		IT Service ISO/IEC 27001
Art. 45 - Security Objectives		Type	-4-1	-4-2	-2-4	-3-3	Annex A
(g)	that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.	process	DM-1 DM-2 DM-3 DM-4 DM-5 SUM-1 SUM-2 SUM-3 SUM-4 SUM-5 SVV-3		SP.03.03 SP.11.03 SP.11.04		A.12.5.1 A.12.6.1
(h)	that other risks linked to cyber-incidents, such as risks to life, health, the environment and other significant legal interests are minimised.	functional, process	-	CR 5.1	SP.03.01 SP.05.02 SP.12.01 SP.12.02 SP.12.09	SR 5.1 SR 5.4	A.11.1.5 A.16.1.5 A.17.1.1 A.17.1.2 A.17.2.1 A.18.1.1

Table 9: Mapping of Requirements to the Objectives of ITRE Committee Amendments

SGTF EG2 recommends using this mapping as a general profile for the EU Cybersecurity Act for the electricity subsector with the caveat that the mapping will need to be adjusted depending on the outcome of the trilogue discussion for the EU Cybersecurity Act. Additionally, the profiles needs to be updated in case of new releases of the standard or changes in the objectives of the regulation. It is recommended that ENTSO-E and EU-DSO use this mapping to make sure that security requirements defined independently from the EU Cybersecurity Act approach meet the same objectives as defined in the EU Cybersecurity Act. SGTF EG2 endorses the provisions of Article 44 on the preparation and adoption of a European cybersecurity certification scheme, where ENISA is asked to consult all relevant stakeholders by transparent consultation processes and in close collaboration with European Cybersecurity Certification Group (ECCG).

Furthermore, objective (h) of the ITRE Committee Amendment is recommended to be addressed by considering the impact to life, health, the environment and other significant legal interest within the risk assessment and respective topics should be reflected with an appropriate risk-impact matrix, see chapter 7.2.4.

Recommendation on a certification scheme

Based on the categorization, see chapter 7.2.3, the recommended certification scheme differs depending on OT products and OT systems or IT services.

For OT products and OT systems, SGTF EG2 recommends using the existing IECEE scheme as the basis for a certification scheme, see Figure 15.

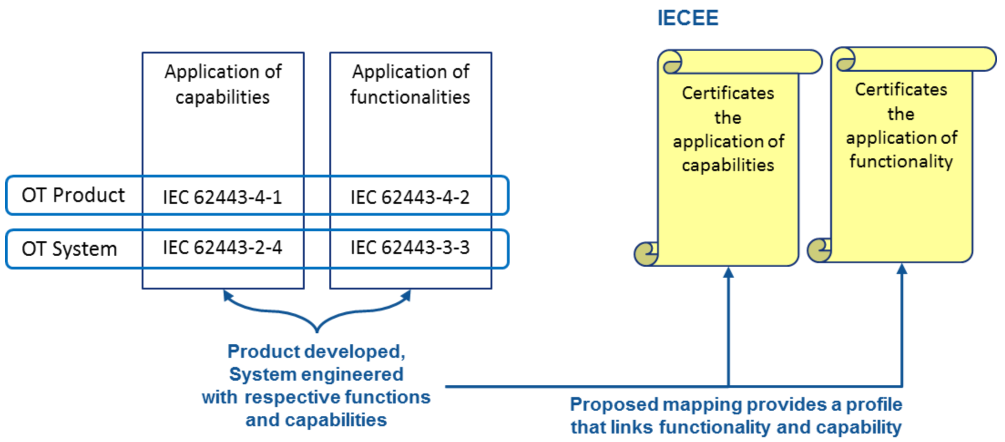


Figure 15: Certification of OT Products and OT Systems

IECEE differentiates between the applied capabilities, i.e. processes and practices, and provided functionalities within a product or system. Both can be assessed and certified independently. However, for a specific product or system, only a certificate that links the capability and functionality together is relevant. With this approach, it provides a profile as defined with the mapping of the EU Cybersecurity Act objectives, see previous chapter 7.2.4. It should be noted that the approach to define profiles for certification under the IECEE system is in line with the proposal to the IEC/TC 65 by the German standardization organization DKE (UK 931.1) to define profiles for conformance.

For IT services, SGTF EG2 recommends a domain specific certification, see Figure 16.

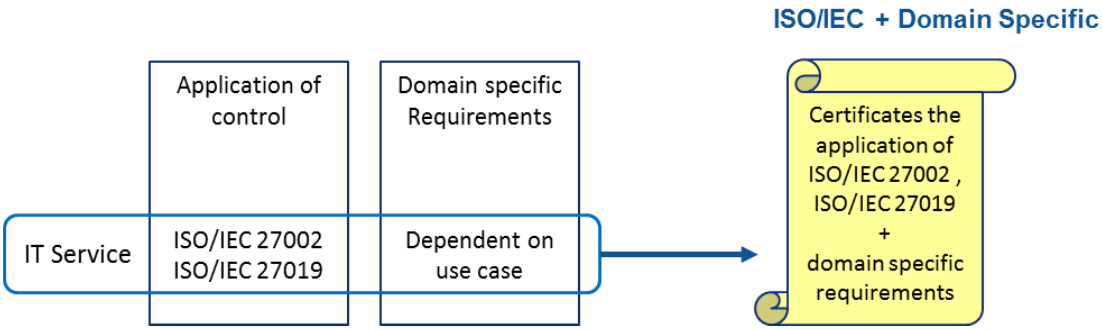


Figure 16: Certification of IT Services

The certification needs to cover ISO/IEC 27002 and ISO/IEC 27019 controls as provided in the mapping to IT services of the EU Cybersecurity Act objectives, see Table 8 and Table 9. The certification, however, can vary depending on the use case. For a cloud service as an example, this might be ISO/IEC 27017 or practices as outlined by the Cloud Security Alliance (CSA)[39]. SGTF EG2 recommends ENISA to provide guidance to the expert group that will be set-up by ENTSO-E and EU-DSO on selection of appropriate standards and frameworks related to IT services.

Recommendation on Assessment Criteria

In order to provide a harmonized and level playing field on the quality of respective certificates, SGTF EG2 recommends that the European Commission requests international and European standardization bodies to provide respective assessment criteria for IEC 62443 requirements that

[39] https://cloudsecurityalliance.org/

should be addressed by the EU Cybersecurity Act, see Table 8 and Table 9. ENTSO-E and EU-DSO should analyse if additional sector-specific assessment criteria are needed to assure relevant implementation of minimum security requirements. In such case, they should develop such criteria in alignment with industry stakeholders, ENISA and the standardization bodies. Until respective assessment criteria are available, assessments should be performed based on the practices and knowledge of accredited conformity assessment bodies.

The same recommendation applies to a certification of IT services if specific standards do not provide respective assessment criteria already.

Recommendation on Conformity Assessment Procedures

Industry has had long-standing experience with the conformity assessment procedures as defined in Annex II of decision no. 768/2008/EC, see Figure 17.

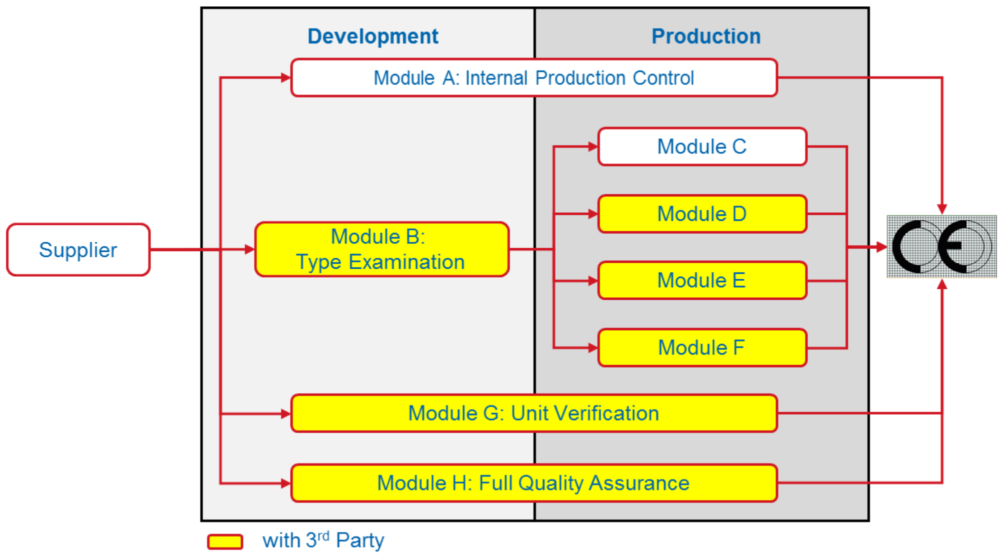


Figure 17: Conformity Assessment Procedures acc. Annex II of 768/2008/EC (Source: ZVEI)

These procedures are used or referred to by product-specific EU legislation in a variety of areas such as safety, public health, explosion protection, electromagnetic compatibility or eco-design (energy efficiency). Most industry products and systems have to comply with requirements set out in one or more pieces of legislation and therefore need to undergo the relevant conformity assessment chosen by the applicable legislation in order to be supplied or further marketed in the EU. The set of conformity assessment procedures of 768/2008/EC offers a variety of options reaching from self-declaration to certification of process and functional conformance, with different degrees of third party involvement which can be selected according to the specific risk potential involved with a product or its intended use. Moreover, these procedures provide for the possibility to demonstrate conformity with regulatory requirements through either product certification or management system certification (“quality assurance modules”). SGTF EG2 therefore recommends following Annex II of 768/2008/EC for the conformity assessment procedures. A detailed description of the modules can be found in the Annex II of respective decision and in the so-called ‘Blue Guide’[40] of the EU Commission. Regarding the management-system related procedures (modules D, E and H,

[40] http://ec.europa.eu/DocsRoom/documents/18027/attachments/1/translations

including variants), reference should preferably be made to ISO/IEC 27001 as the specific standard in the area of cybersecurity (instead of the general ISO 9001 quality management system standard). The conformity assessment procedures comprise an integral part of a candidate EU cybersecurity certification scheme and may vary depending on the envisioned level of assurance.

7.2.6 Common Criteria and New Legislative Framework

Alternative approaches also commonly discussed in the context of certification and EU Cybersecurity Act are Common Criteria[41] and New Legislative Framework[42]. These are not recommended by SGTF EG2 for minimum security requirements in the electricity subsector, a short discussion about the approaches is provided for completeness.

Common Criteria

The Common Criteria is an evaluation method based on an administrative agreement between several National administrative agreements. Common Criteria is based on ISO/IEC 15408. The approach is focusing on product certification and covers functional and assurance (processes) to be applied to respective products. In the electricity subsector, Common Criteria has been applied in Germany for the smart meter gateway with a protection profile. Common Criteria is an approach focused on products. To use Common Criteria for systems would require to have protection profiles for each component prepared and then aligned to each profile for a system while system related services as defined in IEC 62443-2-4 would not be covered. The application to systems is considered highly complex by SGTF EG2. An approach to use Common Criteria for the Network Code on cybersecurity has been extensively discussed, but not followed up as the holistic approach of starting from systems has been the preferred option by SGTF EG2.

New Legislative Framework

The New Legislative Framework (NLF) addresses the requirements for the marketing of products within the EU, and provides for the setting of product requirements that need to be complied with during both development and production. In particular, it covers requirement specification by reference to harmonized European standards, provisions on how conformity with requirements needs to assessed and demonstrated, rules for labelling and market surveillance. It also contains extensive requirements for the competence of conformity assessment bodies (so-called “notified bodies”) which may have to be involved in the certification depending on the specific procedure, to be assessed preferably by means of accreditation. The approach is considered as a horizontal approach for all EU product legislation for the purpose of free movement of goods in the Single Market.

The New Legislative Framework could be considered as an alternative approach, but would require special consideration to support the specific business needs of the electricity subsector such as the support of legacy products with systems and services typically operated for between 15 to 40 years. The New Legislative Framework would require immediate application after the adoption which might be impossible to be implemented for legacy systems of such longevity. Furthermore, as a horizontal regulation, it might be difficult to cover the same depth as provided by specific conformance and certification schemes within an EU Cybersecurity Act. On the other hand, it could be used to support a harmonization of requirements across business domains on a basic level.

[41] https://www.commoncriteriaportal.org/
[42] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

7.2.7 Smart Metering

Smart Metering has already been addressed by regulation with the proposal of a Directive on common rules for the internal market in electricity[43]. In article 20(b), cybersecurity is requested to follow best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the cost and principles of proportionality. With a primary legislation asking for the highest level of cybersecurity, it cannot be addressed by the Network Code on cybersecurity as secondary legislation in the context of defining minimum security requirements.

7.3 Summary of Recommendations

For the two building blocks Conformance to ISO/IEC 27001 and Minimum Security Requirements as defined in chapter 6.1 and described in detail in chapter 7.1 and chapter 7.2, the following requirements are recommended by SGTF EG2:

Building Block	Area	Requirements	Owner	Chapter
Conformity to ISO/IEC 27001	ISO/IEC 27001	Conformity to ISO/IEC 27001:2013 and any subsequent version applicable at the national level.	Operator	7.1
	Scope	System Operation Critical includes assets, which are directly related to the availability and reliability of power generation and distribution infrastructure. It defines the productive environment of an energy system operator, i.e. the Operational Technology (OT) domain.	Operator	7.1.1
	Risk Management	Record known incidents, attacks and vulnerabilities	Operator	7.1.2
	Risk Management	Known basic risks for cyber incidents and attacks should be record	ENTSO-E and EU-DSO	7.1.2
	Risk Management	Regular update on major risks and threats relevant for transmission and distribution operator	ENISA	7.1.2
	Risk Management	ENTSO-E and EU-DSO to provide a risk-impact matrix as template for operators.	ENTSO-E and EU-DSO	7.1.2
	Asset Management	ACER to align the approach on categorization of assets with the respective regulators, ENTSO-E and EU-DSO in order to derive a proper approach on asset management	ACER	7.1.3
	Asset Management	Categorize assets and to have an infrastructure network plan available	Operator	7.1.3
	Migration of legacy	Use of an infrastructure network plan to classify systems according to a risk-impact matrix in order to derive a migration plan depending on an agreed level of CapEx and OpEx.	Operator	7.1.4
	Migration of legacy	Agee with respective stakeholders on the level that should be used for CapEx and OpEx with the objective to migrate existing infrastructure towards a baseline protection	NRA	7.1.4

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0864R%2801%29

Minimum Security Requirements	Categorization	Split into domains of OT products, OT systems and IT Services	ENTSO-E and EU-DSO	7.2.3
	Methodology	Methodology based on ISO/IEC 27005 with additional requirements of IEC 62443-3-2: • ZCR-5-8 – Identify and evaluate existing countermeasures • ZCR-5-9 – Re-evaluate likelihood and impact • ZCR-5-10 – Determine residual risks • ZCR-5-11 – Compare residual risk with tolerable risk • ZCR-5-12 – Identify additional cybersecurity countermeasures	ENTSO-E and EU-DSO	7.2.4
	Methodology - Context establishment	Context establishment shall cover: - System outline - Categorization of products, systems and services - Risk-impact matrix - Target security level (ZCR-5-6, IEC 62443-3-2) EU reference architecture should consider architectures available in international standards. ENTSO-E and EU-DSO should align on respective architecture.	ENTSO-E and EU-DSO	7.2.4
	Methodology - Risk Assessment	Known basic risks for cyber incidents and attacks should be record	ENTSO-E and EU-DSO	7.2.4
	Methodology - Risk Assessment	Regular update on major risks and threats relevant for transmission and distribution operator	ENISA	7.2.4
	Methodology - Risk Treatment	Set-up of expert group with relevant stakeholders and final review with respective associations.	ENTSO-E and EU-DSO	7.2.4
	Methodology - Risk Treatment	Use of international standards: OT products: IEC 62443-4-1/-4-2 OT systems: IEC 62443-2-4/-3-3 IT Services: Domain specific; an advice by ENISA should be considered	ENTSO-E and EU-DSO	7.2.4
	Methodology - Risk Treatment	Residual risks are to be documented	ENTSO-E and EU-DSO	7.2.4
	Methodology - Risk Acceptance	An alignment on classification, minimum security requirements and residual risks	ENTSO-E and EU-DSO	7.2.4
	Methodology - Regular Review	A regular review (at least every 3 years) to consider changes in technology, threat and risks.	ENTSO-E and EU-DSO	7.2.4
	Certification Scheme	Use of profile (mapping of objectives to requirements from standard) as provided by SGTF EG2. ENISA to initiate update of profiles in case of new standard releases or updates in regulation.	ENISA	7.2.5
	Methodology - Risk Assessment	Consider objective (h) of ITRE committee amendments (if applicable after trilogue) within the risk-impact matrix	ENTSO-E and EU-DSO	7.2.5

Minimum Security Requirements	Security Requirements	Use of the profile for security requirements defined independent from the EU Cybersecurity Act approach to meet the same objectives as defined in the EU Cybersecurity Act.	ENTSO-E and EU-DSO	7.2.5
	Certification Scheme	Use of IECEE for respective profile for OT products and OT systems incl. OT services	ENISA	7.2.5
	Certification Scheme	Assessment criteria to be provided by standardisation groups	European Commission	7.2.5
	Certification Scheme	Analysis of the need for additional sector-specific assessment criteria. In such case, ENTSO-E and EU-DSO should develop such criteria in alignment with industry stakeholders, ENISA and the standardization bodies.	ENTSO-E and EU-DSO	7.2.5
	Certification Scheme	Use of Annex II of 768/2008/EC for Conformity Assessment Procedures	ENISA	7.2.5

Table 10: Recommended Baseline Requirements for All Operators

Please refer to the detail description in the chapters in case something is not clear from the summary table.

8. Advanced Cybersecurity Requirements for Operators of Essential Services

Operators of essential services (OES) that fall within the scope of the NIS Directive[44] are operators who have been identified by their respective Member State based on the following criteria:

- The entity provides a service which is essential for the maintenance of critical societal/economic activities;
- The provision of that service depends on network and information systems; and
- A NIS incident could have significant disruptive effects on the provision of the essential service.

The SGTF EG2 has chosen to follow the same direction for its recommendation to apply higher security requirements for energy system operators that are or will be identified as operators of essential service. While the baseline protection as defined in chapter 7 is recommended to be applied to all operators, some variation will apply to the application of the baseline requirements for OES. Furthermore, additional cybersecurity requirements are recommended to OES.

Four building blocks, briefly described in chapter 6.2 (namely, Protection of Current Infrastructure, Supply Chain Cybersecurity Risk Management, Protection against Cross-Border and Cross-organizational Risks and Active Participation in an Early Warning System), are recommended by SGTF EG2 for transmission and distribution operators of essential services.

Chapter 8.1 will describe where the recommended application of the baseline protection will vary compared to operators that are not identified as operators of essential services.

Cybersecurity in the supply chain is becoming increasingly important. Specific focus on cybersecurity risk management will be recommended in chapter 8.2.

The electricity energy system is interconnected and interdependent. Chapter 8.3 is taking into account that not all cybersecurity risks can be addressed at the organizational level.

In current times, where cyber attacks can be automated and advanced threats arise, it is important to have an early warning system in place to help operators protect their infrastructure actively. The recommendation on an active participation in the early warning system for energy system operators will be described in detail in chapter 8.4.

8.1 Protection of Current Infrastructure

In chapter 7, a baseline protection for all operators is recommended that follows a compliance-based approach by application of well-defined controls. Besides conformity to ISO/IEC 27001:2013, operators are recommended to deploy products that meet minimum security requirements that are based on a European reference architecture (e.g. SGAM or IEC 62351-10). A reference architecture defines a role model for the infrastructure deployed, but it cannot reflect the current installed base. Furthermore, energy systems vary depending on the application and use case. Consequently, to protect the current infrastructure, operators of essential services are recommended to use a risk-based approach by performing cybersecurity risk assessments on their current infrastructure.

[44] Directive (EU) 2016/1148

Operators of essential services should have the choice to use products, systems and services that conform to available EU cybersecurity certification schemes, if they can provide evidence that the security level of their respective system is equal or higher than the target security level (ZCR-5-6, IEC 62443-3-2) defined for the minimum security requirements. Evidence must be provided by a documented risk assessment performed according to the methodology as outlined in chapter 7.2.4. The methodology is the same as for the definition of minimum security requirements with the only difference that the system outline (chapter 7.2.4, section 'Context Establishment') is not based on a European reference architecture, but the current architecture of the respective system. The risk-based approach is expected to provide an equivalent or higher protection level of security than the compliance-based approach which offers more flexibility for the operators of essential services to meet their protection targets.

Operators of essential services will therefore have the same obligation as defined in chapter 7 for all operators with the adjustment that the risk management is based on the current infrastructure and that operators of essential services have the choice to deviate from the usage of products, systems and services that conform to available EU cybersecurity certification schemes if they can provide evidence that the achieved target protection level for a system is equal or higher than the one defined with the compliance-based approach.

Furthermore, SGTF EG2 recommends that national competent authorities (NCA) might consider providing a choice for energy system operators, who are not identified as operator of essential services, to follow the risk-based approach.

8.2 Supply Chain Cybersecurity Risk Management

Supply chain cybersecurity risk management is a broad topic that goes beyond the scope of minimum security requirements as defined and described in chapter 7.2. To address the objective of the Network Code on cybersecurity for the supply chain security: "Create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector" (see chapter 5), requires additional measures to be appropriately addressed.

One basis for supplier relationship management is defined in ISO/IEC 27002 chapter 15 by addressing two main objectives:

- 15.1. Ensure protection of the organization's assets that is accessible by suppliers
- 15.2. Maintain an agreed level of information security and service delivery in line with supplier agreements

Other standards exist that address supply chain security in different ways. ISO 28000 defines a security management system for supply chain security that goes beyond information security as defined in ISO/IEC 27002. Nevertheless, various threats and risks such as physical failure, operational failures, stakeholder failures, design failures, business continuity and information security failures are pointed out to be addressed (see ISO 28000:2015, chapter 4.3.1). ISO/IEC 27036 structures the supply chain security along the processes with supplier relationship planning, supplier selection, supplier relationship agreement, supplier relationship management and supplier relationship termination. This standard addresses risks for acquiring products and services (ISO/IEC 27036-1:2014, chapter 5.3). Furthermore, ISO/IEC 27036-3:2014 (chapter 5.2) points out the risks along the supply chain. The standard ISO 20243:2018 describes security techniques and practices that could be used to mitigate risks on maliciously tainted and counterfeit products. A comprehensive standard that provides guidance to federal agencies of the United States of America on risk management is defined in NIST 800-161 which applies a multitier risk management approach building on requirements defined in NIST SP 800-53 Revision 4. Lately, the Federal Energy Regulatory Commission (FERC) approved mandatory reliability standards for U.S. bulk electric systems that are defined in NERC CIP-013-1 which addresses supply chain risk management with a set of requirements and controls to be implemented in a compliance-based approach that includes notification and disclosure of vulnerabilities and incident requirements for vendors and verification of software integrity and patches provided.

Besides standards, there are various guidance papers available. One of the most recognized guidance document is the OE-BDEW whitepaper[45] that defines security requirements for control and telecommunication systems for process control in power systems and provides instructions for their implementation. It defines requirements for individual components and for systems and applications composed of these components. In addition, security requirements for maintenance processes, project organization and development processes are covered. The white paper is a procurement guide that covers those requirements of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019, which are technically or organizationally reflected in procurement projects, but it does not fully cover all ISO/IEC 270xx requirements for an utility organization.

SGTF EG2 recommends to follow ISO/IEC 27001:2013 for the supply chain cybersecurity risk management by analysing general risks as described in the standard ISO/IEC 27036-1:2014 chapter 5.3 and by performing a regular review of controls and practices of ISO/IEC 27002:2018 and ISO/IEC 27019:2017. The review on controls and practices should be documented with gaps and risks identified and respective mitigation measures applied. Supporting materials for such a review could be audit results, incidents, known vulnerabilities, performance monitoring of agreed SLAs and quality and penetration tests. Figure 18 provides an overview on the recommended supply chain risk management.

[45] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

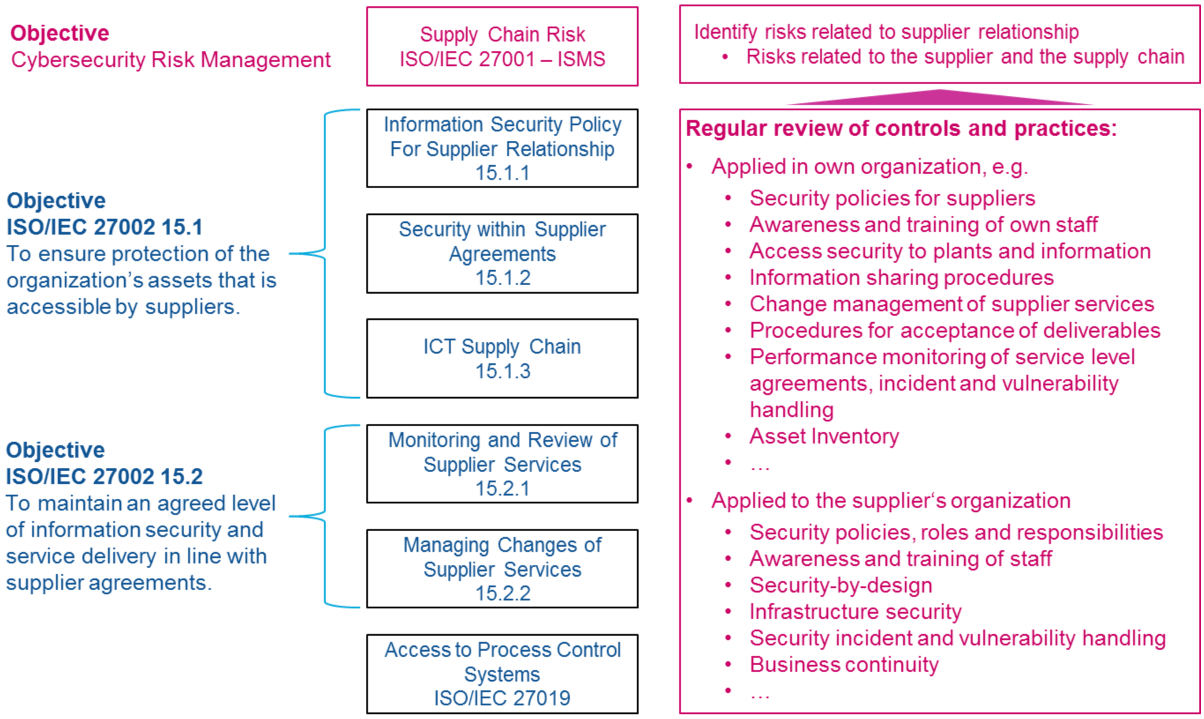


Figure 18: Supply Chain Cybersecurity Risk Management

As the recommended procedure is expected to be highly resource extensive, SGTF EG2 recommends the application to be limited to suppliers of products, systems and services that are highly critical for the security for the supply of energy.

8.3 Protection against Cross-Border and Cross-Organizational Risks

The transmission grid in Europe is interconnected to guarantee the security of supply of all the EU member states and to facilitate competition among different market players, thereby making the system highly meshed. Decentralized generation by renewables makes balancing the grid extremely challenging. Widespread real-time sensing and communications systems between all grid participants and consumers must be deployed to provide better situational awareness regarding the state of the grid and to add command and control capabilities. As more systems are added they will be exposed to a wide range of cyber risks and threats to system (service) availability, data integrity and data confidentiality. The complexity and interdependency of the grid, together with the convergence between operational and non-operational domains (OT/IT convergence) and a huge attack surface makes effective cyber defence a challenge. Increased market operations (cross-border trading) and decentralized (distant) balancing actions have resulted in the power system being operated closer to its operating limits, whilst under greater uncertainty. With more distributed production, by small-scale generation injected into the local distribution grid, all participants will need information about their own area of responsibility particularly for congestion management and security analysis in all relevant timeframes.

The current target for renewable[46] sources for Member States in the EU is 32% of the gross final consumption in 2030: "Member States shall collectively ensure the share of energy from renewable

[46] http://www.europarl.europa.eu/legislative-train/theme-resilient-energy-union-with-a-climate-change-policy/file-jd-renewable-energy-directive-for-2030-with-sustainable-biomass-and-biofuels

sources in the union's gross final consumption of energy in 2030 is at least 32%.", which shows the dimension of the challenge.

The management of cross-border and cross-organizational cyber-risks is a key objective for the European Commission that goes beyond any information security risk management, see chapter 7.1, within an organization. This chapter provides recommendation on the approach and methodology to address this objective.

Chapter 8.3.1 will describe an approach for the risk management methodology to assess cross-border and cross-organizational cyber risks. The risk management methodology has been applied to identify current extreme cyber risk scenarios, see chapter 8.3.2, in order to provide recommendations for a cyber risk management process of cross-border and cross-organizational risks for a potential Network Code on cybersecurity for the electricity subsector, see chapter 8.3.3.

8.3.1 Cyber Risk Methodology

A number of risk management and assessment standards and methodologies have been defined over many years. Taking the experience from the UK government into account, there appears to be no one-fits-all risk methodology[47]:

"There is no single method for doing risk management for cyber security which can be applied universally, to good effect."

A key activity of the SGTF EG2 has been to investigate the best methodology to be applied for the risk management of cross-border and cross-organizational cyber risks.

The horizontal standard ISO 31000:2009 outlines a generic, non-industry-specific guideline for risk management, while ISO/IEC 27005:2018 is a standard specific for information security risk management. In addition, there exist complimentary and industry sector specific standards, such as ISO/IEC 31010:2009 which is a supporting standard for ISO 31000:2009 that is providing guidance on the selection and application of systematic techniques for risk assessment. ISO 55001:2014 provides a universal framework for managing physical assets, which promotes and imbeds the key principle of Enterprise Asset Management (EAM) making risk elimination a primary focus to minimise business and operating risk. Accompanying ISO 55001 are two other standards, ISO 55000 Asset management – Overview, principles and terminology, and ISO 55002 Asset management – Management systems – Guidelines for the application of ISO 55001. ISO 55002 states that the overall purpose is to understand the cause, effect and likelihood of adverse events occurring, to manage such risks to an acceptable level, and to provide an audit trail for the management of risks. The intent is for the organization to ensure that the asset management system achieves its objectives, prevents or reduces undesired effects, identifies opportunities, and achieves continual improvement. The ISO 55002 guidebook provides a structured approach to follow for risk review and the identification, analysis, classification and elimination of risk of an organization's assets.

Alternative risk methodologies are for example described in ISO/IEC 62443 (formally ANSI/ISA-99), which compromises a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

[47] https://www.ncsc.gov.uk/blog-post/coming-soon-new-guidance-risk-management-cyber-security

ISO/IEC 62443-3-2 establishes requirements for a security risk assessment and system design; or the Information Security Forum – Information Risk Assessment Methodology (ISF-IRAM2)[48], which provides risk practitioners with a complete end-to-end approach to perform business-focused information risk assessments. These standards have many similarities with equivalent and equally respected US NIST cyber risk standards and frameworks, for example: NIST SP 800-30[49] and NIST SP 800-39[50] (Managing Information Security Risk – Organization, Mission and Information System View).

SGTF EG2 recommends to base the cross-border and cross-organizational cybersecurity risk management methodology on the international standards: ISO/IEC 27005:2018 and ISO 55001:2014.

The approach recommended by SGTF EG2 is to identify current plausible extreme cyber risk scenarios and to analyse what could possibly cause such extreme events in order to derive recommendations on mitigation of such cyber risks. It is suggested that extreme cyber risk scenarios could be caused by a single cyber-attack, or multiple and coordinated near simultaneous cyber-attacks on critical IT/OT systems, network, telecoms, conventional and smart grid/IoT devices, infrastructure or third-party services. The consequences of which are the causation of one or more of the emergency situations listed in the ENTSO-E "Incident Classification Scale" (March 2018)[51], see Figure 19.

Scale 0 Anomaly		**Scale 1 Noteworthy incident**		**Scale 2 Extensive incidents**		**Scale 3 Wide area incident or major incident / 1 TSO**	
Priority - Short definition (Criterion short code)		**Priority - Short definition (Criterion short code)**		**Priority - Short definition (Criterion short code)**		**Priority - Short definition (Criterion short code)**	
#20	Incidents leading to frequency degradation (F0)	**#11**	Incidents on load (L1)	**#2**	Incidents on load (L2)	**#1**	Blackout (OB3)
#21	Incidents on transmission network elements (T0)	**#12**	Incidents leading to frequency degradation (F1)	**#3**	Incidents leading to frequency degradation (F2)		
#22	Incidents on power generating facilities (G0)	**#13**	Incidents on transmission network elements (T1)	**#4**	Incidents on transmission network elements (T2)		
#23	Violation of standards on voltage (OV0)	**#14**	Incidents on power generating facilities (G1)	**#5**	Incidents on power generating facilities (G2)		
#24	Reduction of reserve capacity (RRC0)	**#15**	N-1 violation (ON1)	**#6**	N violation (ON2)		
#25	Loss of tools and facilities (LT0)	**#16**	Separation from the grid (RS1)	**#7**	Separation from the grid (RS2)		
		#17	Violation of standards on voltage (OV1)	**#8**	Violation of standards on voltage (OV2)		
		#18	Reduction of reserve capacity (RRC1)	**#9**	Reduction of reserve capacity (RRC2)		
		#19	Loss of tools and facilities (LT1)	**#10**	Loss of tools and facilities (LT2)		

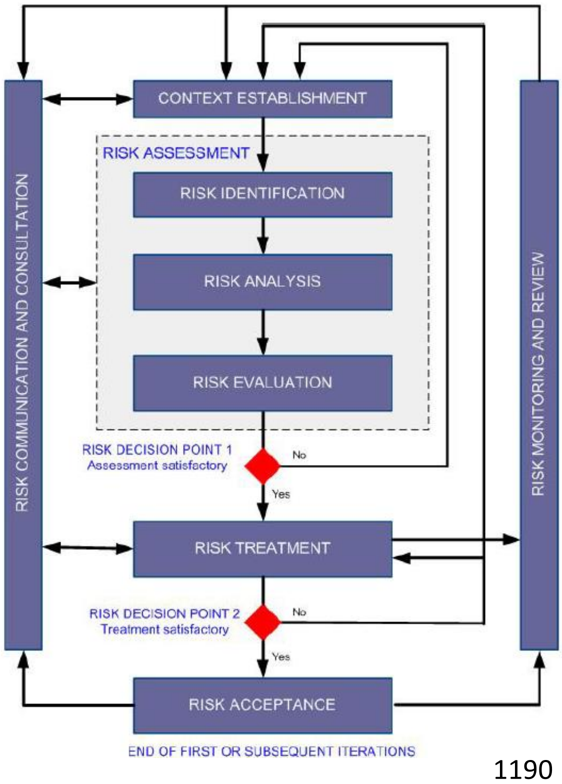
Figure 19: Incident Classification (Source: ENTSO-E)

Considered are only incidents with scale 2 or scale 3 for the analysis of extreme cyber risk scenarios.

[48] https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/
[49] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[50] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
[51] https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf

8.3.2 Extreme Cyber Risk Scenarios

Applying the ISO/IEC 27005:2018 methodology to identify and evaluate extreme cyber risk scenarios for cross-border and cross-organizational electricity grid processes, the workflow consists of the steps as shown in Figure 20.



B1. Context Establishment

B2. Risk Identification

B3. Risk Analysis

B4. Risk Evaluation

B5. Risk Treatment

B6. Risk Communication and Consultation

B7. Risk Monitoring and Review

B8. Risk Acceptance

Figure 20: ISO/IEC 27005 Risk Assessment

B1. Context Establishment

The interconnected power system of Continental Europe extends from Portugal to Poland and from Denmark to Turkey and feeds a load between 220 and 440 GW (mean demand 360 GW). This large system is operated in a synchronous way, meaning that, when we neglect phenomena with time constant smaller than a few seconds, the frequency is identical everywhere.

"The Continental European power system has been designed (in terms of control reserve and control response) to withstand a power imbalance of 300 MW in all operational situations …. However, without adequate countermeasures the consequences of a 3000 MW power imbalance would be immense. Loss of frequency stability resulting in a total system blackout is a probable scenario".[52]

For some ENTSO-E synchronized areas and islands this risk threshold is significantly lower than 3 GW. The ENTSO-E Continental Europe Operation Handbook (Appendix 3: Operational Security[53]) states that in order to ensure the safety of the system, protection must be provided against four main phenomena that may deeply disturb the system or initiate a large-scale incident, namely: (1) cascade tripping, (2) voltage collapse, (3) frequency collapse, and (4) loss of synchronism. There is no direct relationship between voltage and frequency, both can be independently controlled. However, both need to be kept near constant for the entire power system to be healthy. Voltage must be

[52] https://docstore.entsoe.eu/Documents/Publications/SOC/Continental_Europe/141113_Dispersed_Generation_Impact_on_Continental_Europe_Region_Security.pdf

[53] https://docstore.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy_3_Appendix_final.pdf

maintained throughout the network within a strict range of values to be compatible with the sizing of the equipment, to maintain the supply voltage to customers within contractual ranges, to guarantee system reliability and to avoid the occurrence of voltage collapse. Voltage too high can lead to accelerated ageing and the destruction of the equipment. Exceeding the range of values is acceptable but only for limited time duration. Congestion occurs when load flows reach physical and security limits.

In the event of a large power imbalance such as a power plant failure, the ENTSO-E region activates a primary control called Frequency Containment Reserve (FCR) within 30 seconds to 15 minutes to immediately stabilize the system, additional countermeasures may also be applied depending upon the specific circumstances of individual TSO members. The absolute frequency deviation allowed under this primary control must not exceed 200 mHz. Between 5 minutes and one-hour, a secondary control called Frequency Restoration Reserve (FRR) is activated to restore the balance. Primary control limits and stops frequency variations, secondary control brings frequency back to its target value. Between 15 minutes and one-hour, tertiary controls take over in the form of either manual changes to the dispatching of generating units or the decrease of consumption by very large consumers (under bilateral contracts). The IT/OT systems which manage these emergency situations are highly critical.

B2. Risk Identification

Key components for the risk identification are information assets, threats, existing and planned security measures and vulnerabilities.

Information Assets

It is first necessary to identify and value critical generic grid related assets such as IT/OT systems, telecom networks, conventional and smart grid/IoT devices, infrastructure and third-party services. The working group used a NIST 7628 Logical Reference Model[54] mapped into the Smart Grid Architecture Model (SGAM)[55] for this purpose in order to identify critical generic functional areas, see Figure 21.

[54] https://www.offis.de/fileadmin/content/files/download_tools/roadmaps_und_studien/BMWi_Verteilernetzstudie.pdf

[55] https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

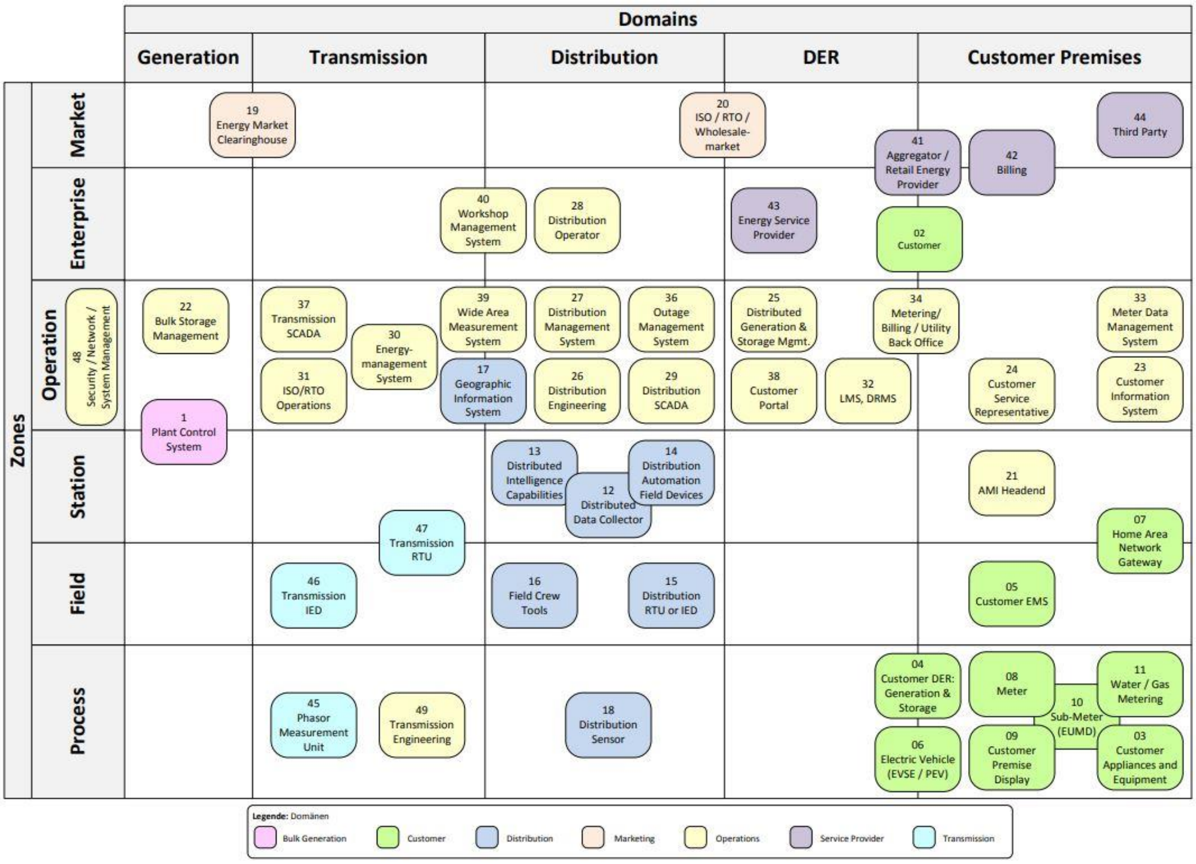


Figure 21: Mapping NISTIR 7628 Logical Reference Model into SGAM on the Function Layer
(Source: Forschungsprojekt Nr. 44/12, „Moderne Verteilernetze für Deutschland“ (Verteilernetzstudie))

For example, functional areas (30) TSO and (27) DSO are considered some of the most critical grid assets (the crown jewels). A successful cyber-attack against functional area (30) TSO Energy Management System, could cause all emergency situations to materialize, since it includes systems such as Load Frequency Control (LFC) and Automatic Generation Control (AGC) which maintains a close balance between total load and total generation in a control area by tracking system frequency as a measure of load-generation imbalance and by sending control signals to power generators to raise or lower their output accordingly. SGTF EG2 recognizes that the functional reference model used is incomplete and other functional areas must also be considered to obtain the complete picture of a rapidly evolving electricity grid.

Threats

The motivation for launching a cyber-attack against the power systems of Europe ranges from pranks and local consumer fraud, all the way to organized crime and state sponsored terrorism. We should assume that the power systems of Europe are an attractive target and are at constant risk of cyber-attack by adversaries with extended skills, resources and motivation. This assumption is supported by evidence provided by National security services[56], CERT organizations[57] and

[56] https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

[57] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

information security companies[58] about recent activities of organized actors. The evidence currently suggests that the threat to the European electricity grid is real, high and increasing.

Existing and Planned Security Measures

A range of relevant international standards that directly or indirectly cover or address IT/OT security controls have been defined such as ISO 27002, ISO 27019, ISO/IEC 62443, IEC 62351, IEC 61850. The Smart Grid Architecture Model[59] (SGAM) is also a useful three-dimensional reference model used to analyse and visualize smart grid use cases. SGAM offers a methodology to map security standards showing their applicability in the different smart grid zones and domains on different layers to support system designers and integrators in selecting appropriate security standards to protect their smart grid systems accordingly.

Vulnerabilities

The CVE[60] and NVD[61] databases currently both contain the details of over 106,000 vulnerabilities. In 2017, the total number of vulnerabilities identified in different ICS components and published on the ICS-CERT website[62] as 322. This includes vulnerabilities identified in general-purpose software and in network protocols that are also relevant to industrial software and equipment.

B3. Risk Analysis

The risk analysis needs to consider impact and likelihood.

Impact

Various risk impact or severity scales have been developed to measure the consequence or impact of a cyber-attack. IEC 62443-3-2 provides good examples of a risk impact scale, and the CEN-CENELEC-ETSI Smart Grid Information Security (November 2012)[63] report also provides risk impact levels based upon six categories: operational, legal, human, reputation, environmental and financial. Some grid participants already have their own risk impact processes and templates, for example: DSOs in the Netherlands are using the NTA8120:2014 Dutch standard based upon ISO/IEC 55001.

A template based on NTA8120:2014 is provided as example in Annex A-4 (chapter 11.4) that meets the requirements as defined in chapter 7.2.4.

Likelihood

A risk matrix is a tool used in risk management to qualitatively determine the level of risk by assessing the likelihood of an incident occurring and the severity of the consequence should the incident occur. Various risk matrices are available to calculate or measure impact x likelihood. IEC 62443-3-2 provides some risk matrix examples. The UK Charities Commission[64] provides a different way of assessing risk by giving extra emphasis or weighting to impact. The Common Vulnerability Scoring System (CVSS)[65] also provides a way to capture the principal characteristics of a vulnerability

---

[58] http://www.trapx.com/wp-content/uploads/2017/08/TrapX-Original-Research-Industrial-Control-Systems-Under-Siege.pdf

[59] https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

[60] https://www.cvedetails.com/

[61] https://nvd.nist.gov/

[62] https://ics-cert.us-cert.gov/

[63] ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf

[64] https://www.gov.uk/government/publications/charities-and-risk-management-cc26/charities-and-risk-management-cc26

[65] https://www.first.org/cvss/

and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Likelihood is reduced by the deployment of effective security controls, and risk calculations often involve a degree of judgement or subjectivity. Where data or information on past events or patterns is available, this is helpful in enabling more evidence-based (quantitative) judgements.

B4. Risk Evaluation

The SGTF EG2 performed structured What-If and Business Impact Analysis qualitative techniques to determine the unmitigated (without consideration for any existing countermeasures) cyber-attack risk to critical generic functional areas identified under B2. Both techniques are approved by ISO 31010:2009 for risk identification, assessment and evaluation purposes. The following five cyber-attack vectors (not ranked in any order) were identified as the most likely and plausible scenarios which could be the cause of cross-border and cross-organizational type emergency situations identified in B1:

1. Conventional cyber-attacks against corporate IT and operational OT systems and networks.
2. Manipulation of critical system data (unauthorized data modification).
3. Cyber-attacks against providers of critical third-party services.
4. Infiltration of the supply chain.
5. Coordinated and simultaneous cyber-attacks against power demand or supply.

1. Conventional Cyber-Attacks Against Corporate IT and Operational OT Systems and Networks

Advanced Persistent Threats (APTs) are long-term, coordinated and sophisticated multi-level attacks by hacktivists, organized crime and state sponsored actors, which often go undetected for weeks or even months. Common entry points are Internet connections, email phishing and social engineering, web site vulnerabilities, interaction with spoofed or infected web sites (waterholes), VPN connections for remote support and maintenance purposes, unauthorized access to remote facilities via insecure WIFI and other network connections and man-in-the-middle attacks. The first objective of the attacker is to steal legitimate user credentials (usernames and passwords) to gain entry and then traverse deeper into other corporate IT and operational OT systems usually to deploy malware. Such unauthorized access to control room systems could cause all emergency situations to arise. There is recent evidence of this risk materialization: APT targeting Energy Sector[66], APT Israel Electric Company[67], Irish Energy Networks[68], Water treatment plant control room[69], CrashOverride[70], Shamoon[71].

2. Manipulation of Critical System Data (Unauthorized Data Modification)

The integrity of key information such as scheduling data, balancing data and consumer (tariff) information is critical. Attacks against the integrity of data content could cause serious operational

[66] https://www.us-cert.gov/ncas/alerts/TA17-293A
[67] https://www.clearskysec.com/iec/
[68] https://www.independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html
[69] https://www.theregister.co.uk/2016/03/24/water_utility_hacked/
[70] https://www.us-cert.gov/ncas/alerts/TA17-163A
[71] https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

problems, for example, to cross-border intra-day capacity allocation trading, to the capacity calculation process and to consumer demand response. The integrity of daily scheduling information is critical for TSO planning and the market. There is currently no public evidence of successful data manipulation causing electricity grid problems; however companies with direct access to critical grid systems and data have been the subject of successful phishing attacks, often the first stage of a longer-term attack strategy. Consumers are becoming very energy price sensitive and the injection of false pricing information into smart device applications, email or SMS messaging could easily cause a large number of consumers to simultaneously act in a detrimental way.

3. Cyber-Attacks against Providers of Critical Third-Party Services

There is a reliance upon providers of third-party services such as public networks, GPS, Time synchronization, Wireless, Cellular, 3G, 4G, Radio time sequence, DNS services etc. which cannot be overlooked. Widespread adoption of Cloud applications (software-as-a-service) also makes companies susceptible to Cloud based weaknesses outside their organization. The electricity grid in some cases requires global clock synchronization to millisecond precision, providing accurate timestamps which allows us to make sense of data relative to events. There is evidence of recent risk materialization and academic research which highlights some problem areas: Accurate and secure clock synchronization[72], Undetectable attacks on PMU time synchronization[73], Netcom BW attack[74], DYN DDOS attack[75], APT against Global Managed Service Providers[76].

4. Infiltration of the Supply Chain

This threat can be described by a rogue actor infiltration of trusted software distribution channels targeting manufacturers of key grid equipment and software, taking advantage of the inherent trust between clients and vendors. By targeting the software and hardware development process (build, update and distribution) the attacker can covertly introduce malware into software and firmware updates and releases or deploy malicious hardware components. This results in the distribution of hardware with undesirable features or software code containing malware with a legitimate and trusted digital signature that cannot be distinguished by the end user. Via this attack vector, attackers can infiltrate well protected organizations or specific sectors by leveraging a trusted channel, even penetrating air gapped networks. Once infected, these systems and devices are open to different cyber-attacks which are difficult to clean post discovery, with equipment disposal usually the only option. There is recent evidence of this risk materialization: CCleaner[77], MeDoc[78], ShadowPad[79], Kingslayer[80].

---

[72] http://www.ntu.edu.sg/home/tanrui/pub/sync-tosn.pdf

[73] http://smartgrid-cybersecurity.events/wp-content/uploads/2017/04/PMU-StateEst-attack-timing-20170314b.pdf

[74] https://www.theatlantic.com/international/archive/2018/06/germany-cyberattacks/561914/

[75] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

[76] https://www.us-cert.gov/ncas/alerts/TA18-276B

[77] https://www.cert.be/docs/ccleaner-v533-ccleaner-cloud-v107-malware-infection.html

[78] https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

[79] https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

[80] https://www.rsa.com/en-us/blog/2017-02/kingslayer-a-supply-chain-attack

5. Coordinated and Simultaneous Cyber-Attacks against Power Demand or Supply

A cyber-attack against thousands of the same device at the same time is a plausible scenario. The infamous Mirai botnet infected 260,000 routers, IP security cameras and other insecure IoT devices. A variant of Mirai crippled Internet access to one million users in Germany, attacking routers with a remotely accessible TCP port. These incidents show that even relatively benign IoT devices can be attacked to devastating effect, including ancillary systems such as fire detection and intruder alarms. IoT devices such as Breakers provide the ability to remotely disconnect and reconnect consumers from the grid, Home Energy Management Systems (HEMS) are powerful tools for managing and improving heating, ventilation, lighting and air conditioning for optimizing energy costs. Search engines that index everything on the internet exist (such as Shodan[81] and Censys[82]) can be used to find IoT devices, sometimes with known open vulnerabilities. The numbers provided in Table 11 below calculate how many devices (in theory) would need to be simultaneously attacked to cause a 3 GW imbalance.

Device Power Production or Consumption	Number of Same Devices Causing 3 GW Load
1 kW	3.000.000
10 kW	300.000
20 kW	150.000

Table 11: Number of Devices that can cause an 3 GW Load

Examples for Typical device power consumption:

- Home Fridge/Freezer: 0.2 kW
- Hot Water Immersion Heater: 4 kW
- Electric Vehicle Charging (Public – Mode 3): 22 kW

Purely for the purposes of concept illustration, a 3 GW power imbalance could be caused by a coordinated and near simultaneous cyber-attack against 137,000 Mode 3 Electric Vehicle charging points. The 2018 ENTSO-E TYNDP scenarios report[83] highlights that the growth of electric vehicles will be exponential over the next ten years. IEC 61851 for EV conductive charging, states that Mode 3 is the safer and more reliable option to charge an EV in all available locations and should be the preferred long-term infrastructure solution.

"Connecting a mass market share of Electric Vehicles to the electricity grid can expose the grid to a dramatic increase in maximum power demand." [84]

Aggregators (also known as Demand Response Providers) provide balancing services by adjusting power demand and/or shifting loads at short notice. The pool of aggregated load (typically MW in size) is managed as a single flexible consumption unit and sold to the markets. Coordinated cyber-attacks against Aggregators could cause the same effect and in principle the same type of simultaneous attack could apply to smart meters, however one difference is that smart meters mostly use wired and wireless technologies not the internet, using Power Line Carrier (PLC) communications[85] so the risk of a botnet type attack against smart meters is much reduced. The EU

[81] https://www.shodan.io/
[82] https://censys.io/
[83] https://tyndp.entsoe.eu/tyndp2018/scenario-report/
[84] https://www3.eurelectric.org/media/26100/2011-04-18_final_charging_statement-2011-030-0288-01-e.pdf
[85] https://www.mdpi.com/2076-3417/6/3/68/htm

Third Energy Package (Directive 2009/72/EC) target for smart meters is at least 80% market penetration for electricity by 2020 (or 240 million smart meters deployed).

Attacks against demand or supply are a black-box attack vector. The adversary does not need to know the underlying topology or operational properties of the grid to be successful. Since transmitted power follows Kirchoff's Law[86] the grid operator often has little control over the power flows and any unexpected and abrupt change in demand could cause line overloads resulting in cascading failure. There is evidence of recent risk materialization and academic research which highlights problem areas: Mirai botnet[87], solar power inverters[88], VPN filter malware[89].

B5. Risk Treatment

To reduce risk, you either need to eliminate the vulnerability, reduce the probability that a threat actor can exploit vulnerability and/or reduce the consequences that would follow if this did occur. The response to identified risk can be one of four options: (1) Accept (tolerate), (2) Mitigate (treat), (3) Transfer, (4) Avoid (terminate). For some electricity sector participants, risk acceptance (tolerate) is not an acceptable option under National laws.

Risk Treatment Plan

For the five extreme cyber-attack scenarios identified under B4 the following actions are provided as examples of how to reduce the cyber risk profile of the European grid:

Conventional Cyber-Attacks Against Corporate IT and Operational OT Systems and Networks

These Cyber risks can be mitigated to some extent by deploying effective ISO/IEC 27002:2013 and ISO/IEC 27019:2017 type security controls, the key controls being:

- (i) Network separation and segregation between corporate IT and operational OT systems and the configuration of restrictive network access control lists and firewall rules
- (ii) System hardening; the removal of all unnecessary and unused functionality
- (iii) Identity and access management, end-user management, multi-factor authentication, segregation of duties
- (iv) network monitoring, particularly packet inspection and anomaly detection
- (v) Malware detection and prevention
- (vi) Vulnerability identification via scanning, patch management
- (vii) Asset management
- (viii) Well-rehearsed system recovery procedures from clean backups to clean devices

Manipulation of Critical System Data (Unauthorized Data Modification)

NIST-7628 guidelines for smart grid security[90] recommend that integrity for power system operations includes assurance that:

- (i) Data has not been modified without authorization
- (ii) Source of data is authenticated
- (iii) Time stamp associated with the data is known and authenticated

[86] https://en.wikipedia.org/wiki/Kirchhoff%27s_circuit_laws
[87] https://en.wikipedia.org/wiki/Mirai_(malware)
[88] https://www.theregister.co.uk/2017/08/07/solar_power_flaw/
[89] https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware
[90] https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

(iv) Quality of data is known and authenticated

New technologies such as the latest Blockchain[91] type technologies may offer some long-term solutions.

Cyber-Attacks against Providers of Critical Third-Party Services

There is an undoubted critical reliance upon providers of third-party services. These providers must ensure the security, reliability and availability of key services, otherwise there could be a real risk to grid operations. The availability of telecoms is becoming more and more critical with the development of renewables connected to DSOs assets in rural areas. Accurate and secure clock synchronization is also critical. System redundancy to eliminate reliance on just one technology or on one service provider is a good defensive control.

Infiltration of the Supply Chain

Trusted computing[92] and code attestation techniques may well be the only answer to this difficult problem. Third-party code attestation is a process in which a vendor's code is tested for resilience against one or more security standards. Such tests are performed by an independent third party through a documented and standard certification process. However, the identification of malicious software and hardware is challenging.

Coordinated and Simultaneous Cyber-Attacks against Power Demand or Supply

Large unexpected and abrupt changes in demand or supply are difficult for TSOs and DSOs to prepare for. *"Grid operators typically assume that consumers collectively behave similarly to how they did in the past under similar conditions (time of day, season and weather)"[93].* New innovative Grid Edge type technologies, solutions and businesses can have the same impact on the grid affecting demand and supply, but currently have less regulatory burden which represents a hidden transfer of risk from market actors to DSOs/TSOs. Another important factor for attack success is environmental conditions. A well-organized cyber-attack launched against the electricity grid in the evening (peak load) during a very cold winter month or very hot summer month with little solar and wind generation could easily test the absolute operating limits of the grid. Increasing the operational risk threshold through greater control reserve and control response to address a large unexpected power imbalance may be required in the future. Grid operators should have an accurate estimate of the total number of high wattage IoT devices in their operational area.

B6. Risk Communication and Consultation

Computing devices are automatic machines which can be wrongly instructed, as highlighted by the recent disclosure of common CPU/chip security design problems: Spectre/Meltdown[94], x86 backdoor[95]. Digitalization will make energy systems more vulnerable to digital risks. Full prevention of cyber-attacks is impossible, but the impact can be limited if grid participants are well prepared. *"While digitalization can bring many positive benefits, it can also make energy systems more vulnerable to cyber-attacks. To date, the disruptions caused to energy systems by reported cyber-attacks have been relatively small. However, cyber-attacks are becoming easier and cheaper to*

[91] https://en.wikipedia.org/wiki/Blockchain
[92] https://en.wikipedia.org/wiki/Trusted_Computing
[93] https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf
[94] https://www.kb.cert.org/vuls/id/584653
[95] https://latesthackingnews.com/2018/08/12/a-hacker-found-god-mode-in-some-old-x86-cpus/

organize. Moreover, the growth of the Internet of Things (IoT) is increasing the potential "cyber-attack surface" in energy systems".[96]

Instantaneous generation and consumption need to be in balance at all times. Intermittent decentralized generation (very often renewable) results in increased deviations from the production forecast and therefore makes balancing the grid more challenging for the Distribution sector, which has effects on the balancing at transmission level. Distribution System Operators will have to take on more responsibility for balancing supply and demand response locally, as well as providing security and reliability to overall system operations. A consequence is that Transmission and Distribution System Operators will have to strengthen co-operation particularly with respect to information exchange on operational aspects of the grid, in order to establish production plans with adequate granularity suitable for grid balance control.

B7. Risk Monitoring and Review

Risk management is not a one-off event and should be viewed as an ongoing routine process ensuring that newly identified risks are addressed as they arise and the re-assessment of previously identified risks that may have changed. An organization identifies and classifies risk to develop appropriate security measures. Risk identification and classification involves security assessments of grid information systems and interconnections to identify critical components and any weak security areas. Understanding cross-border and cross-organizational cyber risk is essential for proper investment in appropriate and effective security controls. The example of coordinated and simultaneous cyber-attacks against power demand or supply is a good example of why our cyber risk assumptions need to be constantly reviewed and updated.

B8. Risk Acceptance

The methodology as described in this section will result in risk mitigation measures as a recommended output for operators. The reflection and possible implementation of such measures will of course remain the responsibility of respective energy system operators of essential services.

SGTF EG2 recommends following the ISO/IEC 27001:2013 principle that each organization has to decide on the decision making process for the acceptance of residual risks. Consequently, SGTF EG2 recommends that operator of essential services documents all risk acceptance with appropriate reasoning.

8.3.3 Recommendation for a Cyber Risk Management of Cross-Border and Cross-Organizational Risks

NIST SP 800-39 states that "Governance" is a set of responsibilities and practices exercised by those responsible for an organization (e.g. board of directors) with the express goal of:

(i) Providing strategic direction
(ii) Ensuring that organizational mission and business objectives are achieved
(iii) Ascertaining that risks are managed appropriately
(iv) Verifying that the organization's resources are used responsibly

[96] https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf

It also identifies risk management activities at three levels: Tier 1 – Organizational level, Tier 2 – Mission/business process level, and Tier 3 – Information system level. To improve the overall cyber resilience of the European electricity grid the following recommendations are suggested:

1. SGTF EG2 recommends that a cyber security risk management advisory group for the electricity subsector is created with the express purpose of identifying and managing common cross-border and cross-organizational Tier 2 and Tier 3 cybersecurity risks appropriately. SGTF EG2 recommends that ENTSO-E together in equal partnership with the new EU-DSO organization are formally tasked and sufficiently resourced to perform this work on behalf of and for the benefit of all European electricity sector participants.

2. SGTF EG2 recommends that ISO/IEC 27005:2018 together with ISO 55001:2014 are the most appropriate standards for an electricity subsector cross-border and cross-organizational cyber security risk management methodology, because they are internationally recognized standards already in use and accepted by many European electricity subsector participants. Together they provide a powerful and flexible framework methodology and tool box for performing cyber risk assessments in an adequate, structured and repeatable way. ISO 55001 asset management helps by managing and reducing the risks that can be linked to specific assets.

3. To perform cross-border and cross-organizational cyber risk assessments, operators will need to agree upon and use the same risk identification and risk evaluation models. SGTF EG2 recommends that a similar functional reference model to the NIST 7628 Logical Reference Model mapped into the Smart Grid Architecture Model (SGAM), see Figure 21, is specifically defined, harmonized, validated and maintained by all operators, in order to assist in the identification of critical generic grid related assets such as IT/OT systems, telecom networks, conventional and smart grid/IoT devices, infrastructure and third-party services. SGTF EG2 also recommends that a risk impact matrix similar to the template based on NTA8120 (see chapter 11.4, Annex A-4) and the CENELEC/SGAM example[97] is specifically defined, harmonized, validated and maintained by all operators, maybe containing additional categories or subcategories (such as impact of power quality). This will provide a common risk impact analysis model for cross-border and cross-organizational electricity subsector cyber risk, reflecting the fact that some synchronized areas, TSOs and DSOs are larger than others so their individual risk tolerance thresholds can be different.

4. The electricity grid is only as secure as its weakest link. Compliance to International standards does not necessarily make you secure, particularly against new risks. ISO/IEC 27002:2013 and ISO/IEC 27019:2017 tells you what you should do in terms of security controls, but not how to do it. Design principles and guidelines on how to implement effective security controls are in high demand from electricity grid participants. SGTF EG2 recommends that the cyber security risk management advisory group should be used to identify and recommend appropriate cyber security standards and frameworks and to identify requirements for common key security controls and recommended best-practice solutions for the benefit of all operators, for example, a black-start recovery process and guidelines describing how to rebuild critical IT/OT systems and infrastructure from a clean baseline.

[97] ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf - Page 29

5. As a general recommendation, SGTF EG2 is in favour of a technology neutral Network Code on cybersecurity, that allows for the incorporation of new technologies and use cases. Any technical examples or use cases outlined should be deemed as non-exhaustive and non-restrictive.

8.4 Active Participation in the Early Warning System

The NIS Directive[98] has set-up the base of an early warning system by obligating Member States to designate national competent authorities (NCA), single points of contact and CSIRTs (Computer Security Incident Response Teams) with tasks related to the security of networks and information systems. The NIS Directive promotes effective operational cooperation between Member States and has established security and notification requirements for operators of essential services.

In the NIS Directive, the reporting of incidents mainly supports the post analysis of incidents while an early warning system aims to actively support the protection of critical energy infrastructure. The set-up of the NIS Directive provides some well defined instruments such as communication channels to operators of essential services in each Member State with a dedicated person of contact and a European CSIRT network that supports cross-border information sharing. Nevertheless, the main difference is that in an early warning system, the central point of contact, e.g. CSIRT of a Member State, provides appropriate capabilities and capacities on information sharing (multiplier to connected stakeholder) and analysis of threats and incidents reported. By playing this role, a CSIRT will take an operational responsibility to support active protection of the energy systems operated by operators of essential services (OES).

An overview on existing information sharing requirements in the EU is provided in chapter 8.4.1.

The value of information can be linked to threat intelligent layers in order to explain at which information level an information sharing platform can provide standardised automated information and where individual forensic and analysis competences possibly combined with intelligent services are needed. This is explained in more detail in chapter 8.4.2.

How the implementation of the NIS Directive could be extended to address an early warning system is discussed in chapter 8.4.3.

An early warning system would require a code of conduct for participants. The content of a code of conduct is briefly listed in chapter 8.4.4.

Chapter 8.4.5 discusses the possibility to connect operators to the early warning system that are not identified as operators of essential services.

Recommendation on a technical realization is provided in chapter 8.4.6.

Open points that need to be addressed for the set-up of an early warning system are listed in chapter 8.4.7.

8.4.1 Existing Information Sharing Requirements in the EU

According to the NIS Directive on European level, the CSIRT network was set-up as a cooperation network between Member State CSIRTs, EU-Institution's CERT (CERT-EU) and ENISA (as secretariat). Member states participate with one or more National Competent Cybersecurity authority (NCA), e.g.

[98] Directive (EU) 2016/1148

the respective CSIRT, responsible among others for incident handing at Member State level especially for the operator of essential services (a definition of OES is provided in the beginning of chapter 8).

In order to effectively handle current cybersecurity threats affecting EU Member States, the European Commission provided the recommendation (EU) 2017/1584 on ‘Coordinated Response to Large-scale Cybersecurity Incidents and Crises’, also called the “Blueprint”. The core objective of this blueprint is to offer shared situational awareness and effective response. It covers cooperation at all levels. On the technical level, it supports incident handling as well as monitoring and surveillance of incidents including continuous analysis of threats and risks. At the operational level, it supports the preparation of decision-making for political level, coordination of the management of cybersecurity crisis, assessment of the consequences and impact at EU level and proposal of possible mitigating actions. It also supports input on EU level crisis response mechanisms like the Integrated Political Crisis Response (IPCR). Finally on political and strategic level, it supports management of both, cyber and non-cyber aspects of a crisis including measures under the framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

The network of CSIRTs has its own Standard Operating Procedures (SOPs) following the blueprint for a coordinated response to large-scale cybersecurity incidents and crises at EU-level. Early warning is encouraged on a voluntary basis for incidents that may have a cross-border impact. The network utilizes means of autonomous information sharing between participating members. The primary function of the network is to prepare relevant reports informing the political hierarchy with the purpose of supporting coordination at EU political level.

Figure 22 provides an overview on the incident reporting structure under the NIS Directive. Operators of essential services (OES) inform their national SPoC (Single Point of Contact), e.g. their respective competent cybersecurity authority (NCA) or CSIRT, in case of a major cybersecurity related incident occurred. Cross-border reporting is handled between the Member States by the CSIRT network.

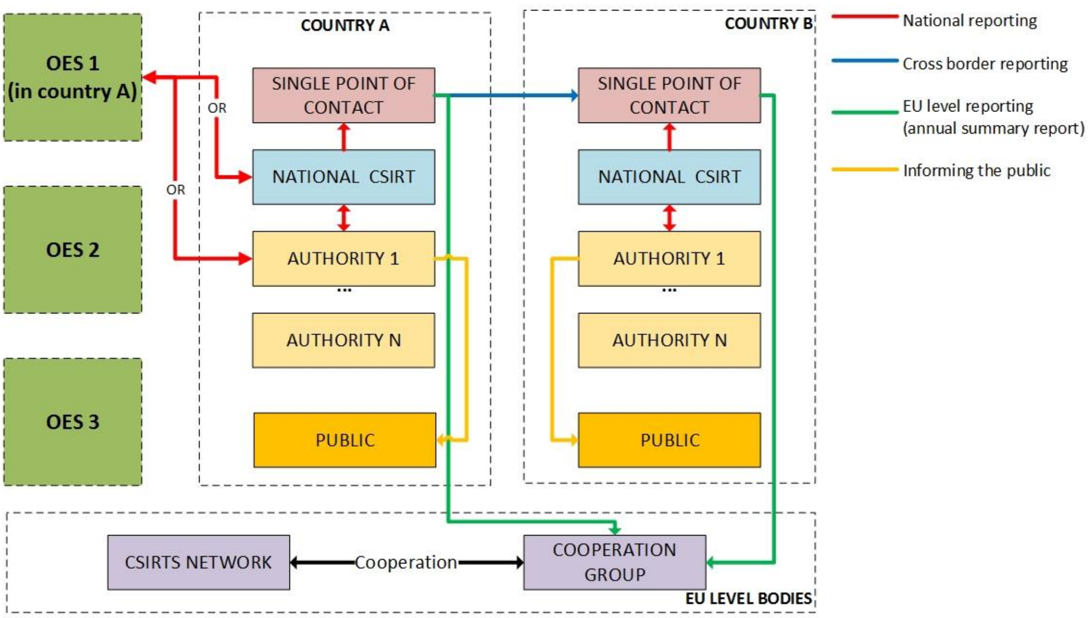


Figure 22: Incident reporting under the NIS Directive (Source: ENISA)

Mandatory ex-post reporting of significant incidents mainly fulfils a statistical purpose for a situation report of what actually happened and gives an overview of the current incidents of OES (NIS Directive, Art. 14, clause 3). For non-OES participants the directive allows notifications of significant incidents on a voluntary basis (NIS Directive, Art. 20).

The disadvantage of post reporting of major issues is that it does not support proactive preparation or even preventive actions to be taken by operators not yet hit by the respective cyber incident. Furthermore, the mandatory reporting of the NIS Directive applies only to the OES that are identified by Member States; typically by applying thresholds for criticality of respective services.

8.4.2 Threat Intelligence Layers and the Value of Information

Security in general follows a staged principle usually beginning with an outer perimeter in a defence-in-depth approach. The resources required to overcome the defensive measures increases at each stage the closer one gets to the centre. This same principle is applied in todays' digital environments, especially in relevant ICT-networks. The perimeter defence, usually consisting of firewalls operating on various OSI layers, ensures a general level of security whereas highly specialized and sophisticated systems isolate and protect the vital components at the core of the network. As actual attacks have shown, the protection of the perimeter is not sufficient to protect critical systems. Due to the complex nature of cybersecurity threats, it is important that anomalies at each protection stage are detected and dealt with as early as possible.

Detecting cybersecurity attacks requires both the sensors and the knowledge about what to look for. The knowledge is commonly referred to as Threat Intelligence (TI) and it can be layered as presented in Figure 23.

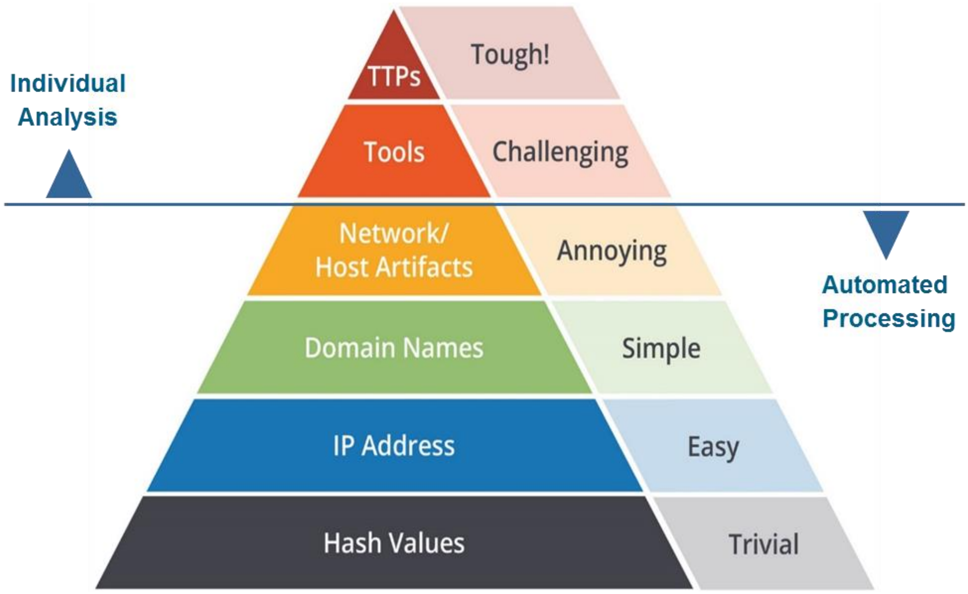


Figure 23: Threat Intelligence Layers (Source: David J. Bianco, personal blog)

Whereas at the bottom, hash values are relatively easy to exchange between partners and are uniquely connected to a piece of a malware, this uniqueness fades the higher up it goes in the pyramid. IP-addresses are not as tightly coupled to an item as hash values, because IP addresses can be dynamically assigned and can change over time, including changing the entity who owns them.

However, having a base of knowledge of malicious IPs is the key to prevention of attacks. Because this is also known by malware developers, domain names and as a consequence domain generation algorithms are widely used to overcome the limited flexibility of IP addresses as well as the restrictions that are put in place once an attack is being prevented. Last, but not least, the network and host artefacts are traces that could lead to more information about a threat in action, such as information in intercepted protocol messages. The volatility of this information is rather high, which requires frequent corrections that make this type of information cumbersome to handle.

The information above the threshold, see Figure 23, is clearly processed intelligence. The automatic processing of information in an autonomous manner is only advisable up to the threshold. Above that level individual analysis, situational interpretation, and proper judgement requires separate treatment. Also the exchange of such specific intelligence does not take place in an automated manner, but typically in personal meetings and direct conversations. The lower parts of the pyramid are usually either classified as white, green or amber level in a Traffic Light Protocol (TLP)[99] and thus exchangeable either freely or freely within the affected organizations. Information about tools and tactics, techniques and procedures (TTP) are often confidential and therefore on the red level which is not allowed to be disseminated or even persistently saved.

For any information exchange, it has to be defined in an early warning system which information according the pyramid presented above can be automatically processed and exchanged and which information should be processed more strictly.

An efficient exchange of information could include different approaches for sharing threat information. One possible approach is to include multiple exchange circles, where technical information known to be belonging to adversaries ("vetted" information) is automatically shared. This circle based approach already exists and is incorporated into sharing platforms such as MISP[100] (Malware Information Sharing Platform); MISP will be described in more detail in chapter 8.4.6. In addition to that, more confidential and/or vague information can be exchanged in communities with mutual trust, e.g. information sharing and analysis centres (ISACs) and sometimes with a need for an even closer relationship which includes exchange and discussion of crucial information on individual basis or even face-to-face.

In general, it should be defined on a technical level what can and could be shared in an early warning system without restriction, e.g. basic technical information about known malware (hash values, network artefacts, etc.) and indicators of compromise (IoC), and what needs additional procedures or controls in order to be shared, e.g. processed information about tools and procedures of adversaries.

SGTF EG2 recommends to agree on information sharing principles within the NIS Cooperation Group.

8.4.3 Extension of the NIS Directive with the Concept of Voluntary Information Sharing

Information exchange can enable all the participating stakeholders to derive a detailed view on the current cyber threat situation, to identify possible trends, and allow them to react and take preventive counter measures early as protective measures. These protective measures such as applying additional internal security measures (e.g. with firewall-rules or access control rights) will

[99] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol
[100] https://www.misp-project.org/

not only improve resilience of dedicated organisations, but also strengthen the cyber resilience of the highly interconnected energy sector. Furthermore, early warnings can help to detect an already active incident and may assist in the containment of this incident.

As stated at the beginning of chapter 8.4, an early warning system requires an operational entity to manage and process the information received and to provide recommendations on mitigation and protective measures to the community. One successful implementation example can be found in the United States with the E-ISAC[101] set-up as public-private partnership generously supported by the government. There also exist successful examples in Member States that are worthwhile to be mentioned:

- Austria: The associations of the electricity and gas companies initiated the first sectoral energy CERT in Europe - Austrian Energy CERT[102] – in constant contact with the authorities and the national CERT.at. It has been accredited[103] by Trusted Introducer and is a full member[104] of FIRST.
- Norway: KraftCERT[105] was established by a power company (Stattkraft) and grid company (Stattnet), both state owned, together with a distribution service operator (Fortum) after an initiative from NorCERT. It is also a member[106] of FIRST and a candidate for accreditation[107] by Trusted Introducer.

Two example models can be considered for a set-up in the EU and Member States. One is the utilization and extension of existing national CSIRTs or national competent cybersecurity authorities (NCA) or alternatively to follow the US approach with a public-private partnership such as an ISAC, e.g. E-ISAC[108] or EE-ISAC[109]. Information Sharing and Analysis Centres (ISACs) are entities within the constituency typically established by infrastructure owners and operators, in some cases facilitated and supported by governments, to foster information sharing on good practice regarding physical and cyber threats, including the mitigation of these threats.

A challenge of sharing detailed voluntary information with governmental institutions could be that according to a strict interpretation of the national criminal law, every government employee must intervene ex officio even on a basis of vague evidence, that national law was broken. As the law stands, the Office of the Public Prosecutor has on evidence to undertake an examination of its own motion and bring an action regardless of the interests of the private sector[110]. It is not important which organization is affected by a cyber-incident, but it is much more significant to get details about a threat vector itself. An intermediary organization, e.g. a CERT or an ISAC, that is highly trusted and able to anonymise voluntarily shared information while supporting the incident reporter

[101] https://www.eisac.com/
[102] For further information see https://www.aec.arge.or.at/ and https://www.energy-cert.at/en/
[103] https://www.trusted-introducer.org/directory/teams/aec.html
[104] https://first.org/members/teams/aec
[105] https://www.kraftcert.no/
[106] https://first.org/members/teams/kraftcert
[107] https://www.trusted-introducer.org/directory/teams/kraftcert.html
[108] https://www.eisac.com/
[109] http://www.ee-isac.eu/
[110] Ex-officion according Criminal Procedure Code of Austria: §2 or Germany: §152

on reporting relevant information might be considered in the approach to set-up an early warning system in the EU and in the Member States.

Furthermore, existing set-ups in Member States on information sharing at on operational level by CSIRTs or NCAs including established communication infrastructure to operators of essential services and between CSIRTS should be considered in a potential set-up of an early warning system.

SGTF EG2 recommends ENISA to facilitate a discussion with the Member States in the NIS Cooperation Group on how to best set-up an early warning system and information sharing in the EU and Member States.

8.4.4 Code of Conduct for an Early Warning System

Sharing information requires rules for sharing. These rules are typically put into a so-called 'Code of Conduct' that gives affected organizations and involved employees a framework on sharing cybersecurity related information with the constituency by providing:

- An information classification scheme, e.g. Traffic Light Protocol (TLP)[111].
- A Single Point of Contact (SPoC) based on the requirements of the NIS Directive.
- A role definition and respective requirements for the roles.
- Rules for sharing information.

Furthermore, interface partners should be authenticated as one measure to protect against misuse of an early warning system by a malicious actor.

SGTF EG2 recommends Member States to agree on a Code of Conduct for an early warning system.

8.4.5 Possible Participation of Operators that are not Operators of Essential Services

For operators of essential services (OES) it is recommended that they actively participate in an early warning system as already stated in chapter 6.2. This might lead to a situation where numerous operators that are not identified as OES are not uninformed about current risks and threats.

SGTF EG2 recommends to offer operators that are not identified as OES the possibility to voluntary participate in the early warning system. They might not be able to contribute with relevant information due to missing CSIRT capabilities, but could utilize shared information to protect their own infrastructure for the benefit of all electricity system operators.

8.4.6 Information Sharing Platform

An early warning system is a solution for threat information gathering, processing and notification. Various tools and platforms exist that support this purpose. However, the Malware Information Sharing Platform (MISP)[112] can be regarded as the de-facto standard for threat information sharing, although a variety of other platforms such as CRITs[113] exist. Crucial for any information sharing platform is the ability to administer the information sharing process and interfaces to different groups, exchange modes and solid authentication mechanism to prevent unwanted access to potentially sensitive information as well as secure database systems that also ensures data integrity.

---

[111] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol
[112] https://www.misp-project.org/
[113] https://github.com/crits/crits

SGTF EG2 recommends to use MISP as a platform for the early warning system. MISP is funded under the Connecting Europe Facility[114], an open source community project that aims to facilitate the exchange and sharing of threat information amongst the participants. The most prominent facilitator of the MISP infrastructure is the Computer Incident Response Centre Luxembourg (CIRCL)[115]; other major contributors include the NATO NCIRC, CERT-EU and the CERT of the Belgian Ministry of Defence.

Threat information sharing platforms have to fulfil individual sets of security requirements specific to each user group. Examples of these user groups are:

- Malware reversers
- Security analysts
- Intelligence analysts
- Law enforcement personnel

It is recommend to apply to each user group the necessary access rights and fulfil their security requirements. Many different precautions are possible and they should be taken into account, of which the most common is to maintain separate instances of the sharing platform to be able to assign different security measures to each instance in order to reflect the importance of the data stored within them. The information exchange between the various instances is then just another case of the otherwise regular information exchange.

Although, and as mentioned above, a variety of tools exist to address the threat intelligence exchange and more could be developed, the standards used to facilitate the exchange are of greater importance, because they ensure the interoperability between the platforms. The two widely used protocol standards are the Trusted Automated exchange of Intelligence Information (TAXII)[116] and the Structured Threat Information Expression (STIX)[117]. TAXII is an application protocol that uses HTTPS to exchange information. It greatly simplifies the independent development of server and client applications. STIX on the other hand is a language and serialization format that is used in the exchange of threat information.

A deployment of any platform would be possible in three principal scenarios:

- Deployment as a stand-alone installation
- Deployment as a virtual machine
- Deployment as a docker container

The best choice for a MISP set-up should be agreed as part of the set-up discussion recommended in chapter 8.4.3.

8.4.7 Open Items for Setting-Up of an Early Warning System

In previous chapters, the options for the set-up of an early warning system while considering existing CSIRT, NCA or ISAC set-up and communication infrastructure (chapter 8.4.3), the definition of a code

[114] https://ec.europa.eu/digital-single-market/en/news/misp-open-source-platform-threat-intelligence
[115] https://www.circl.lu/
[116] https://oasis-open.github.io/cti-documentation/taxii/intro
[117] https://oasis-open.github.io/cti-documentation/stix/intro

of conduct (chapter 8.4.4), the possible participation of operators that are not identified as operators of essential services (chapter 8.4.5) and technology options for the platform (chapter 8.4.6) has been discussed.

Further topics that are still to be discussed, agreed or to be clarified that are necessary for setting-up an energy related early warning system are:

Classified information by Member States

Some cybersecurity related information might be classified (e.g. by a Member State) and this information cannot be shared. There should be a procedure discussed and agreed, on how to share only the cybersecurity relevant part of classified information, which may help other Member States and Operators to avoid a possible cybersecurity incident. Possible approaches could be to sanitize or anonymize information or use a trusted public-private partnership type organization that would simplify confidentiality handling.

Building-up trust between all involved actors

Information sharing is highly depending on trust. It is important to build-up trust between all the involved actors, i.e. between Member States and within the Member States. Typically, this requires regular gatherings and personal contacts. Clearance rules for participating experts must be considered.

National trust anchor through CSIRT or NCA

The national CSIRT or NCA should act as a trust anchor for all connected organizations of a Member State. It is the daily routine of CSIRTs and NCAs to exchange sensitive information and it is therefore recommended to use these existing structures as a trust base. Alternatively, similar structures might be implemented in a public-private partnership model.

National information sharing platform

Every nation state should set-up and host his respective information sharing platform that is interconnected to the platforms of other Member States. International connections to allies such as the United States E-ISAC need to be discussed and agreed by all Member States.

Legal Requirements

Active participants of the early warning system should be allowed to directly report incidents/hash values/TTPs to the local information sharing platform. This might require a legal framework that promotes sharing.

Security of communication

In an early warning system, sensitive information will be shared. Adequate technical measures need to be implemented to secure the communication and guarantee the integrity and confidentiality of the shared information.

Vendor Involvement

System vendors can provide fast response support due to their system knowledge and experience. The possible participation of vendors needs further consideration concerning trust (European based organization vs. non-European based organization) and rules of participation in an early warning system. Possible rules could include vendors to provide a person of contact to respective Member States and to support mitigation on Member States request.

8.5 Summary of Recommendations

For the building blocks of advanced cybersecurity for operators of essential services as defined in chapter 6.2 and described in detail in chapter 8.1, chapter 8.2, chapter 8.3 and chapter 7.2, following requirements are recommended by SGTF EG2.

Building Block	Area	Requirements	Owner	Chapter
Protection of Current Infrastructure	Risk Assessment	Operator of essential services are recommended to use a risk-based approach by performing cybersecurity risk assessments on their current infrastructure	Operator	8.1
	Baseline Security for OES	Operator of essential services follow the obligation as defined in chapter 7 for all operators with the adjustment that the risk management is based on the current infrastructure and that operator of essential services have the choice to deviate from the usage of products, systems and services that are conform to EU cybersecurity certification schemes that are available in case they can provide evidence that the achieved target protection level is equal or higher than the one defined with the compliance-based approach	Operator	8.1
	Baseline Security for non-OES	National regulatory authorities (NRA) might consider providing a choice for energy system operators, who are not identified as operator of essential services, to follow the risk-based approach.	NCA	8.1
Supply Chain Cybersecurity Risk Management	Risk Management	SGTF EG2 recommends to follow ISO/IEC 27001:2013 for the supply chain cybersecurity risk management by analysing general risks as described in the standard ISO/IEC 27036-1:2014 chapter 5.3 and by performing a regular review of controls and practices of ISO/IEC 27005:2018 and ISO/IEC 27019:2017. The review on controls and practices should be documented with lists gaps and risks identified and respective mitigation measures.	Operator	8.2
	Risk Management	SGTF EG2 recommends to limit the risk management to suppliers of products, systems and services that are highly critical for the security of the supply of energy.	Operator	8.2
Protection against Cross-Border and Cross-Organizational Risks	Methodology	Cross-border and cross-organizational cybersecurity risk management to be based on the methodology on the international standards: ISO/IEC 27005:2018 and ISO 55001:2014.	ENTSO-E and EU-DSO	8.3.1
	Methodology	Address cyber scenarios that could cause scale 2 or scale 3 emergency situations listed in the ENTSO-E “Incident Classification Scale”	ENTSO-E and EU-DSO	8.3.1

Protection against Cross-Border and Cross-Organizational Risks	Risk Treatment	Follow the ISO/IEC 27001:2013 principle that each organization (OES) has to decide on implementation and risk acceptance of residual risks. Consequently, SGTF EG2 recommends that operator of essential services documents all risk acceptance with appropriate reasoning	Operator	8.3.2
	Set-Up	Establish a cyber security risk management advisory group for the electricity subsector with the express purpose of identifying and managing common cross-border and cross-organizational Tier 2 and Tier 3 cybersecurity risks.	ENTSO-E and EU-DSO	8.3.3
	Methodology	A risk identification and risk evaluation model similar to the functional reference model of the NIST 7628 Logical Reference Model mapped into the Smart Grid Architecture Model (SGAM) should be specifically defined, harmonized, validated and maintained by all electricity sector participants.	ENTSO-E and EU-DSO	8.3.3
	Methodology	A risk impact matrix should be defined, harmonized, validated and maintained by all electricity sector participants.	ENTSO-E and EU-DSO	8.3.3
	Methodology	The established cyber security risk management advisory group should identify requirements for key security controls and recommended best-practice solutions	ENTSO-E and EU-DSO	8.3.3
	General	Technology neutrality to be considered as a priority for the Network Code on cybersecurity	European Commission	8.3.3
Active Participation in the Early Warning System	Set-Up	Facilitate a discussion with the Member States in the Cooperation Group how to best set-up of an early warning system and information sharing in the EU.	ENISA	8.4.3
	Code of Conduct	Member States to agree on a Code of Conduct for an early warning system.	ENISA	8.4.4
	Participation of non-OES	Offer operators that are not identified as OES the possibility to voluntary participate in the early warning system.	European Commission	8.4.5
	Platform	Use MISP as a platform for the early warning system.	European Commission	8.4.6

Please refer to the detail description in the chapters in case something is not clear from the summary table.

9. Supportive Elements for All Operators

The objectives of the Network Code on cybersecurity outlined in chapter 5 are addressed by the recommendations on security practices and measures that transmission and distribution operators should follow as an operator (see chapter 7) or as an operator of essential services (see chapter 8).

Further guidance is recommended by SGTF EG2 for a consistent implementation within Europe as pointed out in chapter 6.3 that provides implementation guidance for energy system operators on the objectives of the Network Code on cybersecurity, see Figure 5.

Two areas has been identified where guidance is recommended by providing sector-specific best-practice sharing in the area of crisis management, chapter 9.1, and in the area of supply chain security, chapter 9.2.

Chapter 9.3 will provide recommendation on usage of a maturity framework in order to measure and steer cybersecurity implementation. Particular in mature organizations the application of maturity frameworks can support the identification of gaps and prioritization of implementation in order to continuously improve the security posture of respective organization.

9.1 Guidance on Crisis Management

The handling of emergency situations is a well-known area for energy system operators who have to manage distributed energy systems. However, the experience and practice is mainly built on handling emergencies caused by operational disruption due to accidents or by natural disaster. A Network Code on Emergency and Restoration[118] exist for transmission system operators that define the processes that energy transmission system operators must follow when an incident on their area of responsibility occurs. A Network Code on emergency and restoration has been put in place in November 2017 by a Commission Regulation[119].

Looking into crisis management of an emergency situation caused by cybersecurity incidents such as cyber-attacks, the organizational preparedness of an energy system operator requires additional controls and security measures in place. For IT system operators, a guideline on organizational set-up of a Cyber Security Incident Response Team (CSIRT) and incident handling can be found for example from NIST SP 800-61 Rev.2[120] or in the 'Handbook for CSIRTs'[121] from Carnegie Mellon Software Engineering Institute. For OT system operators, limited information is available. With the digitalization of the operational infrastructure (OT), the need and understanding of organizational preparedness for cybersecurity incidents covering the operational technology has been on the agenda for energy system operators. This has resulted in cyber defence experts responsible for OT-systems being employed by energy system operators. A few operators have started to join Information and Analysis Centre (ISAC) organizations such as the EE-ISAC[122] in order to share information on best practice and incidents; the active participation in an early warning system for operator of essential services is a recommendation discussed in chapter 8.4. Another visible

[118] https://electricity.network-codes.eu/network_codes/er/
[119] COMMISSION REGULATION (EU) 2017/2196 of 24 November 2017: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.312.01.0054.01.ENG
[120] https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf
[121] https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
[122] www.ee-isac.eu

outcome is the need of training of CSIRT experts for cyber defence of energy systems. One example of such training is the cyber defence exercises of NATO CCDCOE Locked Shields 2018, where energy systems have been included in a digital grid emulation of 22 city district energy supply systems including control centres, substations and field devices. The Locked Shields Exercise is the world's largest and most complex international live-fire cyber defence exercise, see Figure 24.

Figure 24: Energy Grid Scenario explained to the President of Estonia (Source: NATO CCDCOE Locked Shields Exercise 2018)

The building-up of cyber defence capabilities, participation in ISACs and a recommendation towards an early warning system as well as Cyber defence exercises is supported by the Commission's 'Clean Energy for All Europeans' proposals adapted on 30th November 2016 with the acknowledgement of the importance of cyber security for the energy sector and the need to secure risk preparedness and crisis management. It proposes an obligation to assess rare and extreme risks via appropriate measures (via the risk preparedness proposal[123]). Something that has already been considered in the Cyber Europe[124] 2014 ENISA exercise with a scenario that revolved around a proposal for an EU regulation related to Member States' importing of energy resources. Cyber Europe had three phases that collectively involved over 800 cybersecurity professionals from 29 EU and EFTA countries and 300 organisations.

Crisis handling of cyber incidents in energy systems can include a broad range of capabilities:

- Procedures outlined in the Network Code on emergency and restoration[125]
- Execution on business continuity plans
- Incident handling and vulnerability handling procedures
- Communication technology that is not affected by a black-out
- CSIRT experts that have detailed expert knowledge of the systems and infrastructure
- Capabilities of keeping compromised systems up and running in an ongoing cyber-attack

[123] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0410

[124] This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States.

[125] https://electricity.network-codes.eu/network_codes/er/

- Capabilities for internal and external communication, e.g. national CSIRTS
- Capabilities to analyse attack vectors and protect systems under attack
- Capabilities on back-up and restore

Crisis management is a topic of organizational preparedness that needs capabilities to be build-up and exercised as well as a network such as an ISAC as pointed out before.

SGTF EG2 recommends having energy domain-specific guidance for implementation available without being restrictive for the implementation in order to reflect individual operational needs. Figure 25 provides an overview on typical crisis management steps: Organizational preparedness, respond and recover.

Figure 25: Steps of a Cybersecurity Incident Handling

Organizational preparedness includes awareness & training, an asset management inventory and clear rules on the use of assets as well as protection and recovery mechanism such as malware handling and back-up restore. It is about being prepared for the cyber-incident where experts needs to know which systems to protect first, which procedures to follow, how to communicate and how to keep systems up and running. The above mentioned NATO Locked Shields cyber defence exercise is doing exactly this. Train CSIRT experts to keep energy systems that are compromised and under attack running at any cost.

Respond handles the execution during a cyber incident. As such, it is the doing of the organizational preparedness with the usage of information such as asset information in order to keep crisis situation under control. An early warning system as recommended in chapter 8.4 can support this activity by sharing indicators of compromise (IoC) and indicators of attack (IoA) and by getting support on possible mitigation measures by an Information Sharing and Analysis Centre (ISAC).

Recovery defines the steps where the normal operational state is re-established and forensic and analysis activities are started to improve the organizational capabilities and infrastructure learned from the experience during the crisis situation.

Respective selected controls of the ISO/IEC 27002 and ISO/IEC 27019 that should be covered by an energy domain-specific guidance are listed in Table 12.

Selected ISO/IEC 27002 and ISO/IEC 27019 Controls for Crisis Management	
A.5.1.1	Policies for information security
A.5.1.2	Review of the policies for information security
A.6.1.1	Information security roles and responsibilities
A.6.1.5	Information security in project management
A.7.2.2	Information security awareness, education and training
A.8.1.1	Inventory of assets
A.8.1.2	Ownership of assets
A.8.1.3	Acceptable use of assets
A.12.1.1	Documented operating procedures
A.12.2.1	Controls against malware
A.12.3.1	Information backup
A.12.4.1	Event logging
A.12.5.1	Installation of software on operational systems
A.12.6.1	Management of technical vulnerabilities
A.16.1.1	Responsibilities and procedures
A.16.1.2	Reporting information security events
A.16.1.3	Reporting information security weaknesses
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to information security incidents
A.16.1.6	Learning from information security incidents
A.16.1.7	Collection of evidence
A.17.1.1	Planning information security continuity
A.17.1.2	Implementing information security continuity
A.17.1.3	Verify, review and evaluate information security continuity
A.17.2.1	Availability of information processing facilities
17.2.2 ENR	Emergency communication

Table 12: Selected ISO/IEC 27002 and ISO/IEC 27019 Controls for Crisis Management

As pointed out before, it is important to have domain-specific guidance for energy system operators available. SGTF EG2 recommends that ENISA together with ENTSO-E and EU-DSO should provide respective guidance on implementation.

9.2 Guidance on Supply Chain Security

The handling of supply chain security has been addressed in chapter 7.2 with an approach of defining minimum security requirements for products, services and processes as one potential measure to support the baseline protection. It has also been addressed in chapter 8.2 with a recommendation on a methodology for a supply chain cybersecurity risk management for operators of essential services. This chapter will describe where guidance on supply chain security is recommended as a supportive element for the Network Code on cybersecurity.

Supply chain security aim to address cybersecurity throughout the supply chain. The principle of supply chain security is shown in Figure 26. An operator operates and maintains his system operational critical assets (see chapter 7.1.1). These assets are typically provided by an integrator who has built and commissioned a system and provides maintenance services. The system is built using products provided by suppliers who again have sub-suppliers included in his delivery. This is a cascading chain where an operator addresses cybersecurity in his supplier relationship according to ISO/IEC 27002 and ISO/IEC 27019. The controls address policies, requirements, risk management, vulnerability and incident handling, monitoring and procedures for quality assurance. Refer to chapter 8.2 for an overview on existing standards and guidance documentations available for this area.

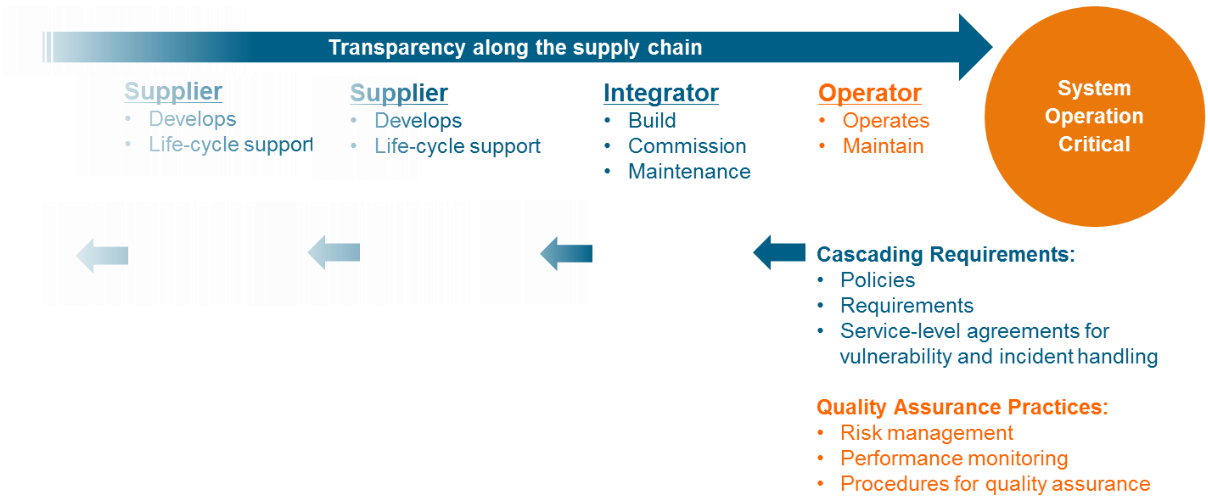


Figure 26: Principle of Supply Chain Security

Transparency in the end deliverable is decreasing along the supply chain due to missing supplier relation and contractual agreements. Consequently, supply chain security is built on trust to the respective direct supplier along the supply chain, i.e. an operator defines cybersecurity policies, requirements, service-level agreements on vulnerability and incident handling for his integrator and supplier and has procedures in place for risk management, verification of quality delivered and monitoring of performance of his suppliers. In this chain, the respective integrator or supplier will define a similar set on cascading requirements to his supplier and will implement respective quality assurance practices in his organization and so on.

Respective ISO/IEC 27002 controls that need to be addressed for the supply chain security either in cascading requirements or in quality assurance practices are listed in Table 13.

Area	ISO/IEC 27002 Requirements	
Cybersecurity policy for supply chain security	A.5.1.1	Policies for information security
	A.7.2.2	Information security awareness, education and training
	A.9.1.1	Access control policy
	A.9.1.2	Access to networks and network services
	A.9.4.1	Information access restriction
	A.12.2.1	Controls against malware
	A.12.5.1	Installation of software on operational systems
	A.13.2.1	Information transfer policies and procedures
	A.13.2.4	Confidentiality or nondisclosure agreements
	A.15.1.1	Information security policy for supplier relationships
Cybersecurity in supplier agreements	A.13.1.2	Security of network services
	A.13.2.2	Agreements on information transfer
	A.15.1.2	Addressing security within supplier agreements
Asset management for supply chain security	A.8.1.1	Inventory of assets
	A.11.2.4	Equipment maintenance
	A.12.5.1	Installation of software on operational systems
Information and communication technology in the supply chain	A.12.6.1	Management of technical vulnerabilities
	A.16.1.3	Reporting information security weaknesses
	A.15.1.3	Information and communication technology supply chain
Change management and monitoring of the supply chain	A.15.2.1	Monitoring and review of supplier services
	A.15.2.2	Managing changes to supplier services

Table 13: ISO/IEC 27002 controls for supply chain security

For supply chain security, SGTF EG2 recommends:

- ENTSO-E and EU-DSO should provide guidance on security policies and agreements for suppliers on common security practices. SGTF EG2 recommends to align the guidance with relevant stakeholders.
- ENTSO-E and EU-DSO should provide guidance on procurement requirements. SGTF EG2 recommends to align the guidance with relevant stakeholders. Furthermore, SGTF EG2 recommends to base this effort on the widely recognized OE-BDEW whitepaper[126] (see chapter 8.2 for details on the whitepaper) and to improve the structure by adding a clear separation of roles such as operator, service provider, integrator and manufacturer. Furthermore, minimum security requirements as recommended in 7.2 should be considered in such guidance as an option where it might simplify procurement requirements if available.

It should be noted that there are supply chain risks such as hidden functions in hardware components or software, e.g. by infiltration of the supply chain by a threat actor (as already mentioned as one specific risk in chapter 8.3.2) or as a legislation act by a nation, that cannot be addressed by standard supply chain approaches and where a risk treatment might be considered for rare, very critical components.

[126] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

9.3 Energy Cybersecurity Maturity Framework

Organizations with widely implemented cybersecurity practices and controls and a high-level of awareness are often confronted with senior management questions concerning the level of implementation. The level of implementation of cybersecurity in organizations can be measured by so-called cybersecurity maturity frameworks.

SGTF EG2 has already pointed out the possible use of a cybersecurity maturity framework in the 1st interim report[127] of the Network Code on cybersecurity:

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

Chapter 9.3.1 will provide an introduction to the typical concepts of maturity frameworks while chapter 9.3.2 explains why a maturity framework needs to cover controls and practices that are defined in the ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 standard.

An overview on existing capability models in relevant standards is provided in chapter 9.3.3 and an introduction on national and international approaches on maturity frameworks are described in chapter 9.3.4.

Chapter 9.3.5 will provide an analysis and recommendation concerning a European Cybersecurity Maturity Framework.

9.3.1 Introduction of the Concept of Maturity Frameworks

A maturity framework typically is a tool, e.g. an excel spreadsheet, that supports assessors to check the level of implementation for specific security domains that is typically based on a progression model of capabilities. A progression model follows a continuous improvement philosophy by defining level of maturity, e.g. practices are performed ad hoc, practices are defined, practices are implemented, and practices are continuously improved. The progression model is applied to security domains such as risk management handling, asset management handling, vulnerability and incident handling, access control, supply chain management, business continuity or people management with awareness and training, etc. For each of these domains, practices and controls appropriate to the level of maturity are defined, see Figure 27.

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

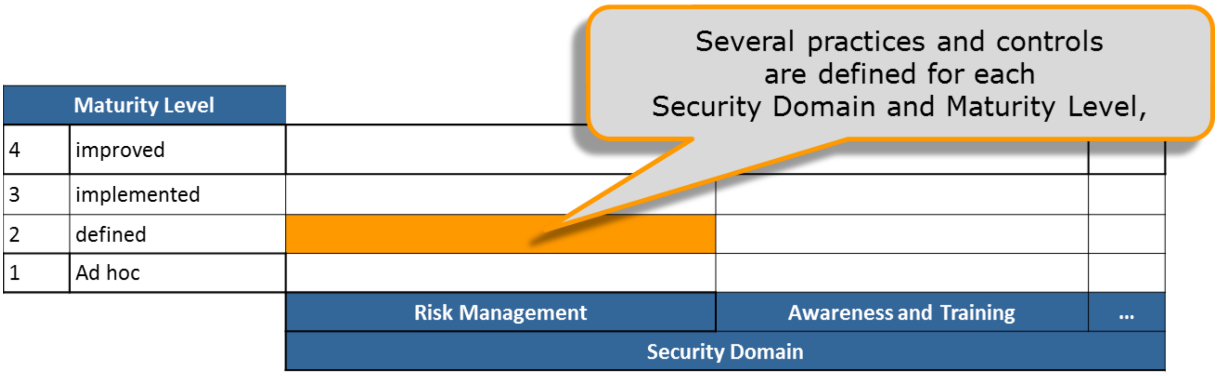


Figure 27: Example of a Maturity Framework model

In some maturity framework the numbers of practices and controls can range up to 750 (e.g. 15 domains x 4 levels x 10 practices or controls per level), but the numbers applied to an organization depends on the targeted maturity level; if for example only maturity level '1' is considered, only 150 practices and controls would be relevant.

Many existing maturity frameworks are based on the CMMI methodology. CMMI[128] was developed at Carnegie Mellon University (CMU) and is today administered by the CMMI Institute, a subsidiary of ISACA[129]. It provides a set of best practices organized by critical business capabilities to improve performance. It comprises a number of documents targeting specific industries, business models, or core competencies. As such CMMI is merely a bracket providing a common platform and needs further detailing by appropriately choosing a specific standard.

The complete picture of such an assessment provides and understanding of the capabilities of an infrastructure and organization to protect against cyber risks and threats.

A more detailed view and comparison on existing maturity frameworks are provided in the following chapters 9.3.3 and 9.3.4.

9.3.2 ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019 in regards to Maturity Frameworks

The ISO/IEC 270xx series is not a standard suggesting or following a maturity methodology. The philosophy of this standard is based on a risk-based approach with a continuous improvement implementation via a Plan-Do-Check-Act (PDCA)-cycle. However, a recommendation for a maturity framework needs to reflect practices and controls of ISO/IEC 27002 and ISO/IEC 27019. Consequently, it is briefly described.

The international standards ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 are used to install an ISMS in organizations of the energy sector. The standard ISO/IEC 27001 consist of two main parts, the management framework of an Information Security Management System (ISMS) and the controls. The management framework is described in chapter 4 – 10 of ISO/IEC 27001 while Annex A contains the controls listed in form of a table.

[128] https://cmmiinstitute.com/
[129] https://www.isaca.org/pages/default.aspx

The management framework of ISO/IEC 27001 addresses the set-up, operation and improvement of an Information Security Management System (ISMS) integrated into an organization, see Figure 28.

ISO/IEC 27001:2013 Annex A describes the reference control objectives and controls; 114 controls are listed. ISO/IEC 27019 provides 14 additional controls. The controls are structured into following security domains:

- Information security policies (A.5)
- Organization of information security (A.6)
- Human resource security (A.7)
- Asset management (A.8)
- Access control (A.9)
- Cryptography (A.10)

Figure 28: Integration of ISMS in an Organization

- Physical and environmental security (A.11)
- Operations security (A.12)
- Communications security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A.15)
- Information security incident management (A.16)
- Information security aspects of business continuity management (A.17)
- Compliance (A.18)

9.3.3 Capability Models in Standards Relevant for the Electricity Subsector

The SGTF EG2 has looked into two key standards and standard frameworks that are relevant for the electricity subsector and which are addressing capability models: IEC 62443 and NIST Framework v1.1.

IEC 62443 Maturity Capabilities

The series of IEC 62443 consist of several parts addressing cybersecurity for industrial automation and control system (IACS) in a holistic approach, i.e. considering the different life-cycles of systems and components as well as addressing functional and process related requirements. Further parts are defined that are addressing network security or risk management methodology, etc.

IEC 62443-2-4 and IEC 62443-4-1 are proposing a maturity model for processes following the Capability Maturity Model Integration (CMMI)[130] maturity methodology, i.e. the maturity methodology is based on:

- CMMI-SVC model for the service establishment and management process (IEC 62443-2-4)
- CMMI-DEV model for the product and service development process (IEC 62443-4-1)

[130] https://cmmiinstitute.com/

IEC 62443 combines the CMMI maturity level 4 and 5 and added an execution aspect in the maturity level 3, see Table 14.

Maturity Level	CMMI Level	IEC 62443 Level
1	Initial	Initial
2	Managed	Managed
3	Defined	Defined (Practiced)
4	Quantitatively Managed	Improving
5	Optimizing	

Table 14: Maturity Level in IEC 62443 compared to CMMI

Following security categories are considered in IEC 62443-2-4:

- Security Program 01 – Solution Staffing
- Security Program 02 – Assurance
- Security Program 03 – Architecture
- Security Program 04 – Wireless
- Security Program 05 – Safety Instrumented Systems
- Security Program 06 – Configuration Management
- Security Program 07 – Remote Access
- Security Program 08 – Event Management
- Security Program 09 – Account Management
- Security Program 10 – Malware Protection
- Security Program 11 – Patch Management
- Security Program 12 – Back-up and Restore

Following security categories are considered in IEC 62443-4-1:

- Security Management (SM)
- Specification of Security Requirements (SR)
- Security by Design (SD)
- Secure Implementation (SI)
- Secure Verification and Validation Testing (SVV)
- Management of Security-Related Issues (DM)
- Security Update Management (SUM)
- Security Guidelines (SG)

Currently, a new proposal for IEC 62443-2-2 is discussed at IEC TC 65 that combines security level with maturity level in order to derive protection level. A protection level will combine technical implementation (security level) with process implementation (maturity level) in order to have a comprehensive definition on the cybersecurity protection level.

NIST Framework v1.1

The American National Institute of Standard and Technology (NIST) published the first cybersecurity framework[131] in February 2014, under the title "Framework for Improving Critical Infrastructure

[131] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Cybersecurity, following up Obama Executive Order n. 13636[132] that assigned the task to develop a "*…set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. ….".* The Executive Order went on to stress the need for flexible, repeatable, performance-based and cost effective approach to help owners and operators of critical infrastructure to identify, assess and manage cyber risk.

One major achievement that NIST reached with its cybersecurity framework was an overall simplification of the cybersecurity frameworks operated by Federal Agencies that was based mainly on the NIST Special Publication 800-37 "Risk Management Framework for Information Systems and Organizations", as a tool for defining the approach to the lifecycle of Security and Privacy, and on the NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations", as checklist for compliance security controls. Both these documents, although presenting a holistic approach to cybersecurity, showed a fair degree of complexity and, while mandatory for U.S. Federal Agencies, resulted in a poor take-up with organizations and companies that had less financial and personnel resources.

On April 16, 2018, NIST released version 1.1 of the cybersecurity framework[133], that implements several enhancements as better coverage of issues of cyber Supply Chain risk management, clarification of technical concepts (compliance, account authentication, identity proofing) and introducing a new section to explain how the framework can be used by organizations to understand and assess their cybersecurity risk, including the use of measurements.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts:

- Implementation Tiers
- Framework Core
- Profiles

Figure 29: NIST Cybersecurity Framework v1.1 (Source: NIST)

Implementation Tiers provide context on how an organization views cybersecurity risks and the processes in place to manage that risks. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices from Partial (Tier 1), Informed (Tier 2), Repeatable (Tier 3) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed:

- **Partial** - The cyber security risk management of an organization is partial if it does not systematically take account of cyber risk and environmental threats.

[132] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf
[133] https://www.nist.gov/cyberframework

- **Informed** - The cyber risk management practices of an organization are informed if the organization has internal processes that take account of the cyber risk, but they do not cover the entire organization.
- **Repeatable** - The cyber risk management model of an organization is repeatable if the organization regularly updates its own cyber security practices based on the risk management process output.
- **Adaptive** - The cyber risk management model of an organization is adaptive if the organization frequently adjusts its cyber security practices by using its past experiences and risk indicators.

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices consist of five concurrent and continuous functions - Identify, Protect, Detect, Respond, Recover.

Figure 30: NIST Framework v1.1 Functions (Source: NIST)

NIST defines 23 security categories in his Core framework, see Figure 31.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 31: NIST Security Categories. (Source: NIST)

A Framework Profile (“Profile”) represents the outcomes based on business needs that an organization has selected from the framework categories and subcategories. The current profile can then be used to support prioritization and measurement of progress towards a target profile.

9.3.4 National and International Cybersecurity Maturity Frameworks

Various maturity frameworks and approaches exist today that are addressing capabilities in cybersecurity of organizations in different shades. This chapter briefly describes some of the capability models and frameworks in order to provide an understanding of the different objectives and approaches of a cybersecurity maturity framework. Please note that this chapter does not target to give a complete overview, but to underline the different objectives and approaches available.

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[134] is publicly available by the US Department of Energy[135]and can be used by any organization. The maturity model defines a set of Maturity Indicator Levels (MILs): Not Performed (MIL 0), Initiated (MIL 1), Performed (MIL 2), Managed (MIL 3) addressing 10 domains:

- Risk management (RM)
- Asset, change, and configuration management (ACM)
- Identity and access management (IAM)
- Threat and vulnerability management (TVM)
- Situational awareness (SA)
- Information sharing and communications (ISC)
- Event and incident response, continuity of operations (IR)
- Supply chain and external dependencies management (EDM)
- Workforce management (WM)
- Cybersecurity program management (CPM)

Practices are sorted into two objectives following a progression model: Approach objectives (several per domain) and management objective (one per domain). Approach objectives are defining specific practices relevant for a security domain while the management objective is defining how this security domain is managed.

ES-C2M2 is a well-recognized maturity framework in the electricity subsector.

CSET®

The Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) developed CSET[136] (Cybersecurity Evaluation Tool) for asset owners with the primary objective of reducing risks to the nation’s critical infrastructure. CSET is a public available tool that can be used flexible to the need by providing the option to select applicable industry recognised standards for US such as NIST 800-53, NIST 800-82, NERC CIP, NISTIR 7628 or uses frameworks such as ES-C2M2 or NIST framework. CSET guides the assessor though the questions

[134] https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1
[135] https://www.energy.gov/offices
[136] https://ics-cert.us-cert.gov/Assessments

with various options to configure it to the personal need. CSET does not provide options for ISO or IEC standards.

World Economic Forum – Partnering for Cyber Resilience

In 2012, the World Economic Forum published some principles and guidelines[137] addressing risks and responsibilities in a hyper connected world. The document includes a simple maturity questionnaire with 19 questions targeting the board level of an organization addressing the overall approach concerning cybersecurity within an organization ranging from unaware, fragmented , top-down, pervasive to networked. The approach has been extended[138] in 2017 with new principles and tools for board level. The approach is referring to standards, but does not link recommended principles and guidelines to respective standards.

The Norwegian National Security Authority (NSM) Approach

In August 2017, NSM published a document stating basic principles for ICT-security[139]. The document gives 23 basic principles to counter cyberattacks divided into 4 categories:

- Identify and Map
- Protect
- Maintain and Discover
- Handle and Restore

The maturity of an organization is measured on the implementation as shown in Table 15.

Implementation status	Maturity level
Organization successfully chose own principles	High
Organization aligned with 23 basic principles	Sufficient
Organization aligned with 10 important measures	Low
Organization not aligned with 10 important measures	Very low

Table 15: Maturity Categorization in the NSM approach

The approach from Norway does not specifically targets the energy sector and tries to address the complexity of a maturity in an approach that can be used by all organizations, i.e. from SME to a cooperate organization.

The Australian Cyber Security Centre (ACSC) Approach

ACSC is an Australian Government initiative that brings together existing cyber security capabilities across Defence, the Attorney-General's Department, Australian Security Intelligence Organisation, Australian Federal Police and Australian Criminal Intelligence Commission. In April 2018, ACSC published a cybersecurity maturity framework named the "Essential Eight maturity model"[140], to complement the advices in their document "strategies to mitigate cyber security incidents"[141].

ACSCs essential eight maturity model consist of five maturity levels from zero to four, whereof zero to three representing not, partly, mostly and fully aligned with the intent of the mitigation strategies

[137] http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf
[138] http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
[139] https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf
[140] https://www.asd.gov.au/publications/protect/Essential_Eight_Maturity_Model.pdf
[141] https://www.asd.gov.au/publications/Mitigation_Strategies_2017.pdf

for cybersecurity incidents. The fifth level (four) is reserved for higher risk environments. ACSC gives level three as a baseline for regular organizations to aim for (fully aligned with the mitigation strategy, see above), while organisations facing higher risk environments shall aim for level four regarding the threat vectors relevant for them.

The mitigation strategy of the essential eight maturity model is divided in three categories as following:

1. Mitigation strategies to prevent malware delivery and execution
    - Application whitelisting for servers and workstations
    - Patch applications for servers and workstations
    - Configure Microsoft Office macro settings for workstations
    - User application hardening for workstations
2. Mitigation strategies to limit the extent of cybersecurity incidents
    - Restrict administrative privileges for workstations and servers
    - Patch operating systems for servers and workstations
    - Multi-factor authentication for workstations and servers
3. Mitigation strategies to recover data and system availability
    - Daily backups for workstations and servers

The Italian National Cybersecurity Framework

Italian National Cybersecurity Framework[142] realized 2015 by CIS-Sapienza is based on the NIST framework while introducing an additional concept of priority levels in order to support organizations and companies in the identification of cybersecurity subcategories to be implemented while balancing the effort.

The Framework suggests the use of a priority scale of three levels:

- High Priority: Actions that enable the slight reduction of one of the three key factors of cyber risk. Such actions are prioritized and must be implemented irrespective of their implementation complexity.
- Medium Priority: Actions that enable the reduction of one of the three key factors of cyber risk, that are generally easily implementable.
- Low Priority: Actions that make possible to reduce one of the three key factors of the cyber risk and that are generally considered as hard to be implemented (e.g. significant organizational and/or infrastructural changes).

The UK Information Assurance Maturity Model (IAMM)

The National Cyber Security Centre (NCSC) of UK has decided[143,144] to withdraw support for their own Information Assurance Maturity Model (IAMM) due to following reasons:

- Using maturity models to compare organisation is like comparing "apples with oranges".
- The encouragement of organisations to focus on continual improvement failed because many organizations have been limited to use the tool as a compliance tool.

[142] http://www.cybersecurityframework.it/en
[143] https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm
[144] https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm

- National incentives based on maturity schemes failed as it does not reflect that each organization is unique.

The current approach of NCSC is on providing guidance[145] helping UK government departments, agencies, the critical national infrastructure and its supply chains to protect their informations and systems.

NIS Cooperation Group

In January 2018, the NIS Cooperation Group has published security measures[146] for all operators of essential services that aim to support Member States to establish cross-sectoral measures or sector specific measures. Security domains and measures defined are:

Part 1: Governance and Ecosystem

- Information System Security Governance
  - Information system security risk analysis
  - Information system security policy
  - Information system security accreditation
  - Information system security indicators
  - Information system security audit
  - Human resource security
  - Asset Management
- Ecosystem Management
  - Ecosystem mapping
  - Ecosystem relations

Part 2: Protection

- IT Security Architecture
  - System configuration
  - System segregation
  - Traffic filtering
  - Cryptography
- IT Security Administration
  - Administration accounts
  - Administration information systems
- Identity and Access Management
  - Authentication and identification
  - Access rights
- IT Security Maintenance
  - IT Security Maintenance procedure
  - Industrial control systems
- Physical and Environmental Security
- Physical and environmental security

Part 3: Defense

- Detection

145 https://www.ncsc.gov.uk/index/guidance
146 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

    - Detection
    - Logging
    - Logs correlation and analysis
- Computer Security Incident Management
    - Information system security incident response
    - Incident report
    - Communication with competent authorities

Part 4: Resilience

- Continuity of Operations
    - Business continuity management
    - Disaster recovery management
- Crisis Management
    - Crisis management organization
    - Crisis management process

No information is available on the methodology that has been used to derive these measures.

9.3.5 Recommendation on a Cybersecurity Maturity Framework and Approach

The previous chapter 9.3.3 and chapter 9.3.4 have provided an insight on the existing landscape on capability models, maturity frameworks and national and international approaches.

The analysis has shown that there is a comprehensive maturity capability model available from NIST (NIST cybersecurity framework v1.1, see above) and that for the electricity subsector ready-to-use frameworks are available such as ES-C2M2 or CSET. A usage of a maturity framework is of value if used to measure and steer implementation and this is only feasible with organizations that have the capabilities and capacity to use such an instrument. Nevertheless, national approaches like in Norway or Australia try to leverage the approach by drastic simplification in order to provide guidance to the majority of organizations and to address typical cyber threats and risks.

Taking this into context of the Network Code on cybersecurity in the electricity subsector, the SGTF EG2 has agreed the following statements concerning an Energy Cybersecurity Maturity Framework:

- The SGTF EG2 underlines the value of a cybersecurity maturity framework if used voluntary as an instrument particular for mature organizations to measure and steer cybersecurity implementation.
- A link to practices and controls to basic standards, see chapter 7.2.1, particular ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 is needed in order to reflect the direction and approach as defined in this recommendation for a Network Code on cybersecurity.
- Taking into consideration the experience from the National Cyber Security Centre (NCSC) of UK, a maturity framework is not a compliance tool, but a tool supporting organizations in steering cybersecurity. This must be the overall guidance on such tool.
- Simplified approaches might be useful from a National perspective, but organization with the capabilities and capacity to use a maturity framework to measure and steer cybersecurity implementation do need a comprehensive instrument that goes into depth.

Table 16 provides a high-level comparison of security domains linked to the ISO/IEC 27002:2017 and ISO/IEC 27001:2013 security controls:

ISO/IEC 27002:2017	ES-C2M2	NIST Framework v1.1	NIS Coop. Group Security Measures
Information security policies (5)	Information sharing and Communications	Governance (ID.GV)	Information System Security Governance (1.1)
Organization of information security (6)	Cybersecurity Program Management	Awareness and Training (PR.AT) Communications (RS.CO)	Information System Security Governance (1.1)
Human resource security (7)	Workforce Management		Information System Security Governance (1.1)
Asset management (8)	Asset, Change and Configuration Management	Asset Management (ID.AM) Maintenance (PR.MA) Protective Technology (PR.PT)	IT Security Architecture (2.1)
Access control (9)	Identity and Access Management	Identity Management, Authentication and Access Control (PR.AC)	IT Security Administration (2.2) Identity and access management (2.3) Physical and environmental security (2.5)
Cryptography (10)		Information Protection Processes and Procedures (PR.IP)	IT Security Architecture (2.1)
Physical and environmental security (11)		Information Protection Processes and Procedures (PR.IP)	Physical and environmental security (2.5)
Operations security (12)	Situational awareness Threat and Vulnerability Management	Information Protection Processes and Procedures (PR.IP) Protective Technology (PR.PT) Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	IT security maintenance (2.4) Detection (3.1)
Communications security (13)		Data Security (PR.DS)	IT Security Architecture (2.1)
System acquisition, development and maintenance (14)		Information Protection Processes and Procedures (PR.IP)	IT security maintenance (2.4)
Supplier relationships (15)	Supply Chain and External Dependencies Management	Business Environment (ID.BE) Supply Chain Risk Management (ID.SC) Security Continuous Monitoring (DE.CM)	Ecosystem Management (1.2)

Information security incident management (16)	Event and Incident Response, Continuity of Operations	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP) Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM) Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)	Computer security incident management (3.2)
Information security aspects of business continuity management (17)	Event and Incident Response, Continuity of Operations	Information Protection Processes and Procedures (PR.IP)	Continuity of Operations (4.1) Crisis Management (4.2)
Compliance (18)		Governance (ID.GV)	
ISO/IEC 27001:2013			
Risk Management (Information Security Management System (ISO/IEC 27001:2013))	Risk Management	Risk Assessment (ID.RA) Risk Management Strategy (ID.RM)	Information System Security Governance (1.1)

Table 16: High-Level Comparison of Security Domains

It should be noted that the mapping is not comprehensive in the way that it compares only security domains and categories, and does not go into single controls and practices of respective frameworks and standards. Taking this into consideration, the table provides a good indication on coverage, but cannot be taken as conclusive.

Maturity levels recommended by the different approaches are compared in Table 17. Maturity levels are varying slightly from approach to approach, but typically covering a similar granularity.

CMMI	IEC62443	NIST Framework v1.1	ES-C2M2
			Not Performed
Initial	Initial	Partial	Initiated
Managed	Managed	Informed	Performed
Defined	Defined Practiced	Repeatable	
Quantitatively Managed	Improving	Adaptive	Managed
Optimizing			

Table 17: High-Level Comparison of Security Level

While the NIST framework v1.1 is addressing the critical infrastructure in general, ES-C2M2 is covering specifically the electricity subsector. The discussion within SGTF EG2 has concluded that both frameworks are feasible to be used. Even though there are differences in the direction and how controls and practices are included, the application of any of these maturity frameworks is seen beneficial by the SGTF EG2.

Missing parts in all existing maturity framework considered in this report is the missing link to ISO and IEC standards. Nevertheless, the SGTF EG2 considers the effort to create a new framework based on ISO/IEC standards as not justified, while it would recommend to provide a comprehensive mapping of controls and practices to at least one of the frameworks. A preference has been given to ES-C2M2 due to his specific focus on the electricity subsector.

The recommendation of SGTF EG2 is ENISA to provide a mapping of ES-C2M2 to controls of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 and to provide a list of controls that are not covered. ENISA might discuss with ENTSO-E and EU-DSO on the value to provide an extended maturity that includes controls not already covered in the existing maturity framework.

Furthermore, SGTF EG2 recommends operators who intend to use a maturity framework to follow the Plan-Do-Check-Act (PDCA) methodology, i.e.:

- Plan Plan evaluation
- Do Perform evaluation
- Check Analyse identified gaps concerning criticality, e.g. by using a risk-impact matrix as recommended in chapter 7.2.4 (see chapter 11.4 Annex A-4)
- Act Plan, prioritize and implement improvements

9.4 Summary of Recommendation

For the supportive elements as defined in chapter 6.36.2 and described in detail in chapter 9.1, chapter 9.28.2 and chapter 7.2 , following requirements are recommended by SGTF EG2:

Building Block	Area	Requirements	Owner	Chapter
Crisis Management	Implementation Guidance	ENISA together with ENTSO-E and EU-DSO to providing guidance on implementation of respective ISO/IEC 27002 and ISO/IEC 27019 controls	ENISA	9.1
Supply Chain Security	Guidance on Policies and Agreements	ENTSO-E and EU-DSO to provide guidance on security policies and agreements for suppliers on common security practices. SGTF EG2 recommends to align the guidance with relevant stakeholders.	ENTSO-E and EU-DSO	9.2
	Guidance on Procurement Requirements	ENTSO-E and EU-DSO to provide guidance on procurement requirements. SGTF EG2 recommends to align the guidance with relevant stakeholders representing manufacturer. Furthermore, SGTF EG2 recommends to base this effort on the widely recognized OE-BDEW whitepaper[147] while to improve the structure by adding a clear separation of roles such as operator, service provider, integrator and manufacturer. Furthermore, minimum security requirements should be considered in such guidance as an option where it might simplify procurement	ENTSO-E and EU-DSO	9.2

[147] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

		requirements if available.		
Energy Cybersecurity Maturity Framework	Maturity Framework	ENISA to provide a mapping of ES-C2M2 to controls of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019 and to provide a list of controls that are not covered. ENISA might discuss with ENTSO-E and EU-DSO on the value to provide an extended maturity that includes controls not already covered in the existing maturity framework.	ENISA	9.3
	Maturity Framework	SGTF EG2 recommends operators who intend to use a maturity framework to follow the Plan-Do-Check-Act (PDCA) methodology, i.e.: • Plan - Plan evaluation • Do - Perform evaluation • Check - Analyse identified gaps concerning criticality using a risk-impact matrix • Act - Plan, prioritize and implement improvements	Operator	9.3

2363 Please refer to the detail description in the chapters in case something is not clear from the
2364 summary table.

10. Conclusion

The SGTF EG2 mission was to prepare the ground for a Network Code on cybersecurity for the electricity subsector. The recommendations provided for a potential Network Code on cybersecurity follow an holistic and risk-based approach that aims to protect energy systems used by transmission and distribution system operators.

A methodology has been defined that allows to specify a protection baseline for all energy system operators by utilizing the proposed EU Cybersecurity Act as an instrument of choice. Identified operators of essential services will have to assess their current infrastructure to achieve a similar or higher security level than the prescriptive approach chosen for operators that do not reach the criteria defined by the NIS Directive for operators of essential services.

These cybersecurity recommendations are to be supported by best practice sharing in supply chain security and crisis management. Supply chain security aims to increase trust and transparency in the supply chain while crisis management aims to support the resilience of energy system operators. Furthermore, a supportive tool, an energy cybersecurity maturity framework, has been recommended to support mature organizations to steer cybersecurity implementation.

Energy systems are interconnected and interdependent. To take cross-organizational and cross-border risk mitigation into consideration, SGTF EG2 has proposed a methodology to provide mitigation recommendations based on identified risks to energy system operators. An approach that could even lead to recommendations on measures to market participants that are not directly affected by a potential Network Code on cybersecurity, but which systems and services might have an impact on the stability of the European energy network.

With the set-up of an early warning system for the energy sector, an active protection on cybersecurity threats is recommended. An information sharing platform is a powerful instrument to support the resilience of the European energy infrastructures. A key success factor for an early warning system will be in the hands of the Member States by building-up trust and by collaboration and cooperation across public and private organisations, Member States and international allies and partners.

The recommendations provided in this report for a Network Code on cybersecurity addresses cybersecurity in a holistic approach that has the ability to adjust to a changing threat and risk landscape in the energy sector. It requires the cooperation of stakeholders in the energy value chain as well the support of the Member States.

11. Annex

11.1 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	-
APPLia **(Observer only)**	Lenka Jančová, Applia	Mustafa Uğuz, Arçelik
CENELEC **(Observer only)**	Didier Giarratano, Schneider Electric	John Cowburn, Smart Energy Networks

11.2 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
Christina Skouloudi	Agency for Network and Information Security ENISA

11.3 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 Europe
Eric Scheer, Siemens	T&D Europe	Willem Strabbing, ESMIG	ESMIG
Joy Ruymaekers, EANDIS	CEDEC	Prokopis Drograris, Enisa	ENISA
Konstantinos Moulinos, Enisa Christina Skouloudi, Enisa	ENISA		
David Willacy, National Grid	ENTSO-E		
Andrea Foschini, Terna	ENTSO-E		
Philip Strøm, 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 Europe	Fredrik Torp, Vattenfall	GEODE
Kyriakos Satlas, European Commission	CERT-EU	Roman Tobler, Wiener Netze	GEODE
Nuno Medeiros, EDP	Eurelectric	Christophe Poirier-Galmiche, Enedis	EDSO
Armin Selhofer, Österreich Energie	GEODE	Christiane Gabbe, Innogy	EDSO
		Joy Ruymaekers, Eandis	CEDEC
		Artur Świętanowski, PSE	ENTSO-E
		Maarten Hoeve, ENCS	ENCS
		Ioannis Retsoulis, Eurelectric	Eurelectric

11.4 Annex A4: Risk-Impact Matrix - Template

Example template for a risk-impact matrix based on NTA 8120[148]:

		Effect						
		Insignificant	**Very small**	**Small**	**Moderate**	**Substantial**	**Serious**	**Extreme**
Safety		Minor injury without first aid	Minor injury with first aid	Medical treatment by doctor	Injury with absence	Injury with absence > X wk	Permanent injury	Lethal end
Reputation	**Critical media attention**	Internal commotion without media attention	Local attention	Commotion in sector without media attention	Regional attention	National attention for some time	National attention for longer time	Intensive attention for longer time / international attention
	Political attention					Local	National	Public discussion national politics
Environment		Insignificant environmental damage / disturbance, easily recoverable	Very little environmental damage / disturbance, quickly recoverable	Little environmental damage / disturbance, recoverable	Medium environmental damage / disturbance, difficult to recover	Substantial environmental damage / disturbance, very difficult to recover	Serious environmental damage / disturbance, hardly recoverable	Serious environmental damage / disturbance, irrecevorable
Compliance	**Administrative law**	Inidividual complaint that operator violates a rule	Grouped complaint(s) that operator violates a rule	Arbitration procedure individual case / formal request for information	Formal warning / formal investigation	Arbitration procedure concerning fundamental execution of task / fine < X M€	Compulsory rule / conditional penalty / invastion regulator / fine > X M€	Loss designation / silent executor / (partly) loss power of decision
	Criminal law						Criminal law procedure	Criminal law sanction
Financial		Damage smaller than X €	Damage from X € to X €	Damage from X € to X €	Damage from X € to X €	Damage from X € to X €	Damage from X € to X €	Damage higher than X €
Operational		X hours outage in LV substation	X hours outage in LV substation	X hours outage in LV/MV substation	X hours outage in several LV/MV substation	X hours outage in several LV/MV substation	X hours outage in several LV,MV substation, X hours outage in HVsubstation, unavailability of control centre	Major blackout of larger district or area, X hours outage in HV substation, unavailability of control centre

148 https://www.nen.nl/News/News/Dutch-standard-on-asset-management-for-energy-network-operations-NTA-8120-also-available-in-English.htm

- Empty on purpose -