IMPLEMENTING AN ISA/IEC-62443 AND ISO/IEC-27001 OT CYBER SECURITY MANAGEMENT SYSTEM AT DUTCH DSO ENEXIS

Carlos MONTES PORTELA
Enexis - NL
carlos.montes.portela@enexis.nl

Maarten HOEVE
ENCS - EU
maarten.hoeve@encs.eu

Fook Hwa TAN
Northwave - NL
fookhwa.tan@northwave.nl

Han SLOOTWEG
Enexis / Eindhoven University of Technology – NL
j.g.slootweg@tue.nl

ABSTRACT

This paper presents a real-life implementation of a Cyber Security Management System (CSMS) at Dutch DSO Enexis. The CSMS is based on the international standards ISA/IEC-62443 and ISO/IEC-27001. The combination of these international cyber security standards offers a structured approach for managing cyber security related risks in industrial environments of critical infrastructures like DSOs.

INTRODUCTION

Enexis is a leading DSO when it comes to applying ICS/Scada and station & distribution automation for its grid management related tasks. Enexis is using these technologies for monitoring and remote switching of HV/MV and strategic distribution stations Furthermore, monitoring of all other distribution stations (+/- 35.000 in total in the next years) and public light switching based on IP-networked devices at each and one of the distribution stations. The systems used for this purpose are commonly known as operational technology (OT). OT uses more and more technologies / concepts / protocols that are also used in IT environments for office automation. This has benefits as these technologies / concept / protocols are mature and have a large installed base. The latter can lead to cost reduction and better management tools in comparison to proprietary solutions of specific OT vendors. The problem is that with the technologies from IT, OT is also importing the cyber-security threats. Hackers can use tools and techniques developed for enterprise IT systems to penetrate deep into OT systems. This creates large risks as many of the legacy OT solutions were not designed with cyber security in mind. As a result, the cyber security related risks for DSOs grow when applying more and more new OT solutions and connecting existing ones with so called gateways. The existing risk management approaches at DSO Enexis did not cover risk management for cyber security related risks sufficiently. Therefore, an ISA/IEC-62443 and ISO/IEC-27001 based OT CSMS was implemented and integrated into the existing risk management framework of Dutch DSO Enexis. This activity started in 2016 and step by step the OT security maturity increased, resulting in a fully operational cyber security management system in 2018.

THE ROAD TO AN EFFECTIVE CYBER SECURITY MANAGEMENT SYSTEM

This section explains how the CSMS was implemented at DSO Enexis. Firstly, it shows why a CSMS based on an international standard is needed from a risk management point of view. Then an overview is given of the main activities that are needed to setup the CSMS and which actors were involved. Finally, it clarifies what approach was chosen in the implementation project at Enexis and what benefits were obtained by combining the standards ISA/IEC-62443 and ISO/IEC-27001.

Selecting an appropriate standard for the CSMS

In order to make future-proof decisions Enexis conducted a review of available standards in coordination with ENCS (European Network for Cyber Security). ENCS is a member-based association that focusses on OT security related research and consultancy for DSO's and TSO's. As a result, ISA/IEC-62443 was chosen as the main standard for cyber security in the OT domain of Enexis. It is a mature international standard, specifically targeted at the OT domain of industrial environments [1][2]. The standard is composed of several parts as shown in *figure 1*.

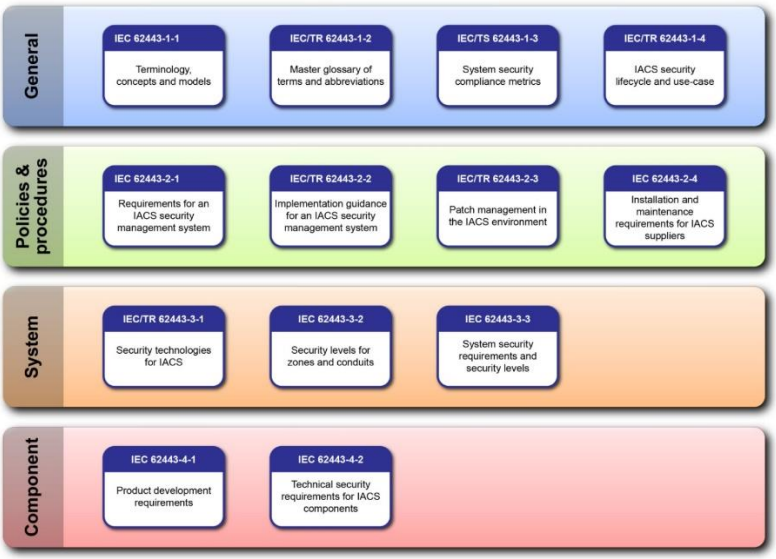

Figure 1 – ISA/IEC-62443 - High-level activities for setting up a cyber security program in an industrial environment

The first group – General - contains standards and technical reports (TR62443) that are general in nature and must be understood by the entire stakeholder community in order to successfully apply the standards. The second group – Policies & Procedures - addresses the people and process aspects of an effective cyber security program. The audience for these documents includes people who develop and operate these programs across the entire lifecycle of solutions. In the third group – System - the focus is on the technology related aspects of security. This includes both an assessment of available technologies and their suitability for use in this context, as well as the specific requirements related to the technical aspects of a security program. Finally, the fourth group - Components - focuses on the specific security related technical requirements of the products and components that are used to assemble industrial control systems.

Part ISA/IEC-62443-2-1 describes the process and content of an implementation of a CSMS: "Requirements for an IACS security management system". IACS stands for Industrial Automation Control Systems and is the ISA/IEC-62443 term for OT. At DSO Enexis this part of the standard was chosen to implement the CSMS.

The ISA99 committee is responsible for the development of the working products that lead to the standard. These working products are submitted to the IEC for consideration as standards and specifications in the IEC 62443 series of international standards following the IEC standards development process.

Main activities of implementing the CSMS

Implementing a CSMS is a continuous process that consists of 6 high-level activities [2]: Initiate CSMS program, High-level risk assessment, Detailed risk assessment, Establishing policy, organization and awareness, Select and implement countermeasures and Maintain the CSMS. These activities and their relationships are depicted in *figure 2*.

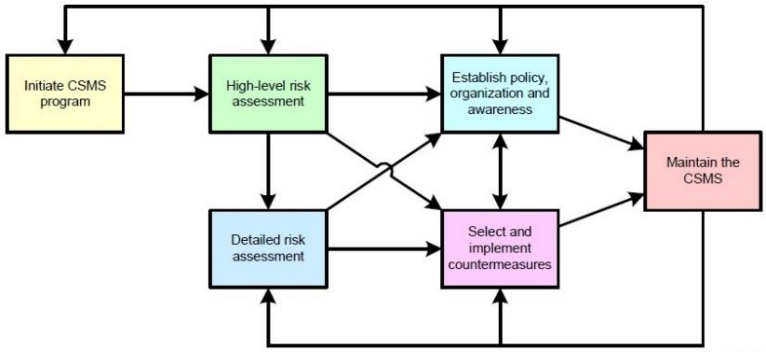

Figure 2 – ISA/IEC-62443 - High-level activities for setting up a cyber security program in an industrial environment

As these activities consist of many tasks requiring specific and new skills, Enexis invested in training internal staff on ISA/IEC-62443 knowledge and contracting external staff where necessary.

ENCS has been involved in setting up the CSMS related risk management policies and integrating cyber security risk assessment methodologies into the broader risk management process of the Asset Management department of Enexis. The Dutch information security consultancy company Northwave, has been involved in developing required policies, procedures and bridging the standard to fit Enexis specific needs and requirements.

Approach of implementing the CSMS at Enexis

Below each of the 6 main activities is described for the implementation of the CSMS at Dutch DSO Enexis:

Initiate CSMS program

Implementing a CSMS is a complex and time-consuming process. Depending on the size of the organization and the number of assets involved it can take either months or several years. Therefore, it is very important to invest effort and time in the initiation phase. Commitment of important stakeholders (e.g. formal and informal leaders) is important. Cyber security has proven to be a topic that is not tangible and well understood. Therefore, an interactive artist impression of the process of setting up the CSMS was developed. Via this tool the OT Security Officers of Enexis were able to communicate with internal and external stakeholders in a more natural and effective way [3].

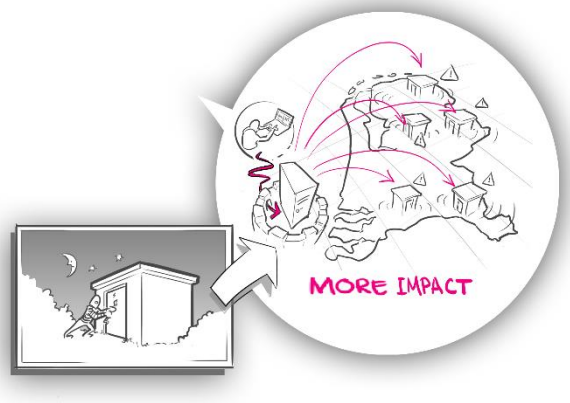

Figure 3 – Artist impression showing increased impact of a cyber security attack in comparison with a physical attack

Part ISA/IEC-62443-2-2 offers implementation guidance for setting up a cyber security management system. Unfortunately, this part of the standard has not been published yet. As a result Enexis, ENCS and Northwave carefully defined a strategy taking into account different aspects:

- Timely delivery of tangible results
- Cost effective implementation & operation of the CSMS
- Compliance with current and foreseen future cyber security requirements of the regulator
- Availability of internal and external resources

A detailed planning was drafted and during weekly

meetings the expected and actual progress was discussed. Involvement of strategic, tactical and operational security personnel has proven to be an important success factor of the CSMS implementation at Enexis. By having them involved from the start, defined work packages necessary to get the CSMS implemented were accepted. Besides defining the planning and involving the relevant internal and external stakeholders, the Initiate CSMS program consists of defining the scope of the CSMS: what is and what is not governed by the CSMS?

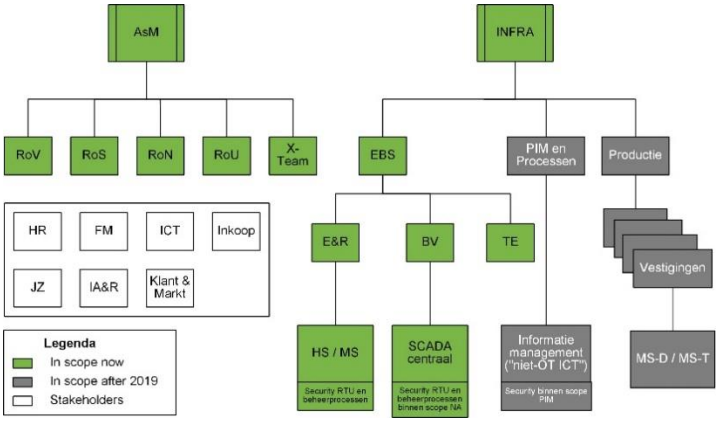

Figure 4 – Scope of CSMS

As shown in figure 4 Enexis chose to have an initial scope where the highest OT security risks were included. Therefore, the entire Asset Management business unit and the central Scada / Control Centre, the central OT data centre, all HV/MV stations and all related processes within the internal Service Provider INFRA were included in the initial scope. In 2020 the rest of Service Provider INFRA will be in scope to finally have all substations (HV/MV and MV/LV) in scope.

High-level risk assessment

During the high-level risk assessment, a methodology for identifying and assessing the priority of cyber security related risks needed to be defined. At DSO Enexis the choice was made to use the bowtie method [4]. A bowtie diagram visualizes the cyber security risk you are dealing with in one understandable picture. The diagram is shaped like a bowtie, creating a clear differentiation between the proactive and reactive side of risk management. The bowtie method is a qualitative risk analysis method that is used at Enexis for all kinds of risks related to electricity and gas grid management. It has proven to serve very well for analysing OT cyber security related risks. And as a bonus, the OT cyber security approach was fully accepted by the Risk Officer responsible for the broader asset risk management framework as the methodology and tools used are identical.

Policy and procedures were developed defining why and how Enexis is using the bowtie method for OT cyber security related risks. An important step in prioritizing the risks, is assessing them via the risk matrix that defines the risk tolerance of the Asset Owner. At Enexis the Asset Owner consists of the board that acts on behalf of the shareholders being municipalities and provinces in the service area of Enexis. By using the risk matrix OT cyber security risks can be compared with other asset related risks and prioritized accordingly. It makes the whole process of assessing and treating them more objective and transparent. After assessing and prioritizing the OT cyber security risks, a more detailed understanding of the risks can be obtained executing the detailed risk assessment. The outcome of the high-level risk assessment has served Enexis in choosing which risks to analyse in more detail first as it is a resource intense task. So, the execution of the risk analysis has also had a risk based approach. The highest risks have been analysed in detail and treated with a higher priority. Figure 5 shows the workflow defined by parts ISA/IEC-62443-3-2 and 3-3 of the standard. It offers a practical step-by-step approach and has given Enexis a formalized approach for assessing and treating OT cyber security related risks.

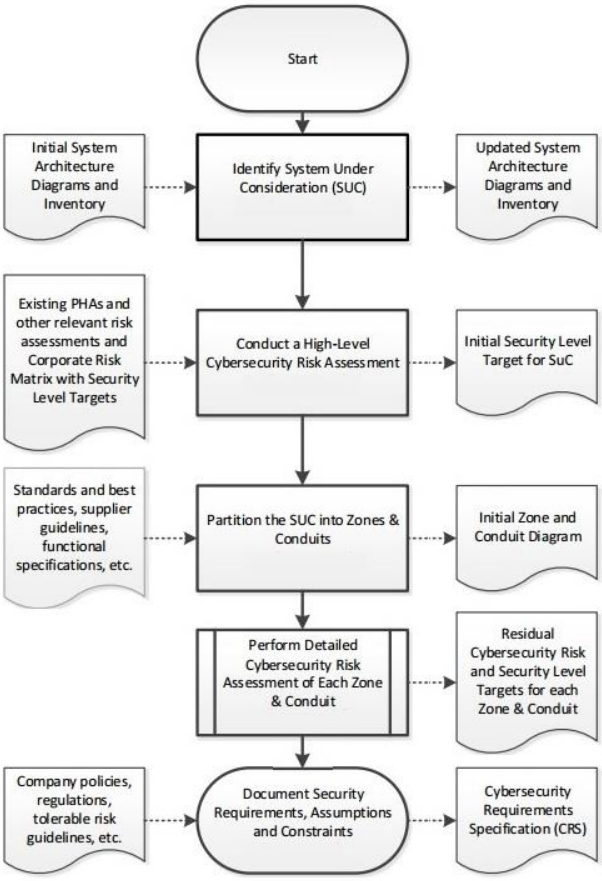

Figure 5 – High-level risk assessment of ISA/IEC-62443-3-2

The standard allows the end user to select an appropriate risk assessment and prioritization methodology. It only states that the organization shall have one, but does not specify which one. That leaves enough flexibility to choose a methodology that best suits the company culture and the context it operates in. To actually obtain valuable results the high-level risk assessments at Enexis were performed via workshops with approximately 6 to 10

participants. Each participant representing a relevant aspect of the system or domain under evaluation. This increased quality and acceptance of the risk assessment outcome and acceptance of the CSMS as a whole.

Detailed risk assessment

The detailed risk assessments were conducted for all relevant OT systems and components within the scope of the CSMS. As it concerns a more detailed and therefore more technical activity, different and more specialized participants executed this task. Furthermore, experts from ENCS and commercial cyber security organizations were hired to assist in obtaining a realistic view of the current situation at Enexis. As Enexis is an organization with more than 100 years of history, formed after several mergers, many generations of different OT systems exist. Therefore, an extensive cyber security assessment lasting over 9 months was performed on multiple HV/MV substations. Contracted ethical hackers, cyber security specialists from ENCS and OT (cyber security) experts from Enexis jointly analysed the OT cyber security risks in detail to be able to perform an accurate detailed risk assessment and formulate adequate measures. Besides technical findings, also personnel and policy / procedural findings were found. Traditionally the digital assets of HV/MV stations are left untouched as much as possible once fully tested and successfully operating. Changing software or configurations of station automation equipment, leads to costly and time-consuming testing that needs to be done in order to guarantee a safe and reliable operation of the electricity grid. Therefore, one of the defined countermeasures has been to develop policies and procedures that allow for controlled patching of OT assets as a result of a cyber security incident. An example of such an incident is the publication of a vulnerability in one of the components used by Enexis in an international source for vulnerabilities like ICS CERT [5]. Besides the policies and procedures personnel have been and will be trained to be able to accurately estimate the magnitude of an incident and make an informed decision on if and when to apply a patch. This example shows why the 6 main activities of setting up the CSMS are interconnected in figure 2. The results of a high-level risk assessment may lead to the need of setting up new policies, that may lead to extra necessary countermeasures, that may lead to updating the outcome of detailed risk assessments, etc.

Establishing policy, organization and awareness

When Enexis started implementing ISA/IEC-62443-2-1 no mature OT security practice existed. As a result, most of the policies demanded by the standard for a professional treatment of OT cyber security risks needed to be implemented. Figure 6 shows all the elements of the CSMS and for all elements policies were written. For example for “Personnel security” a policy was written related to screening of internal and contracted personnel and for “Incident planning and response” on how to deal with OT security incidents.

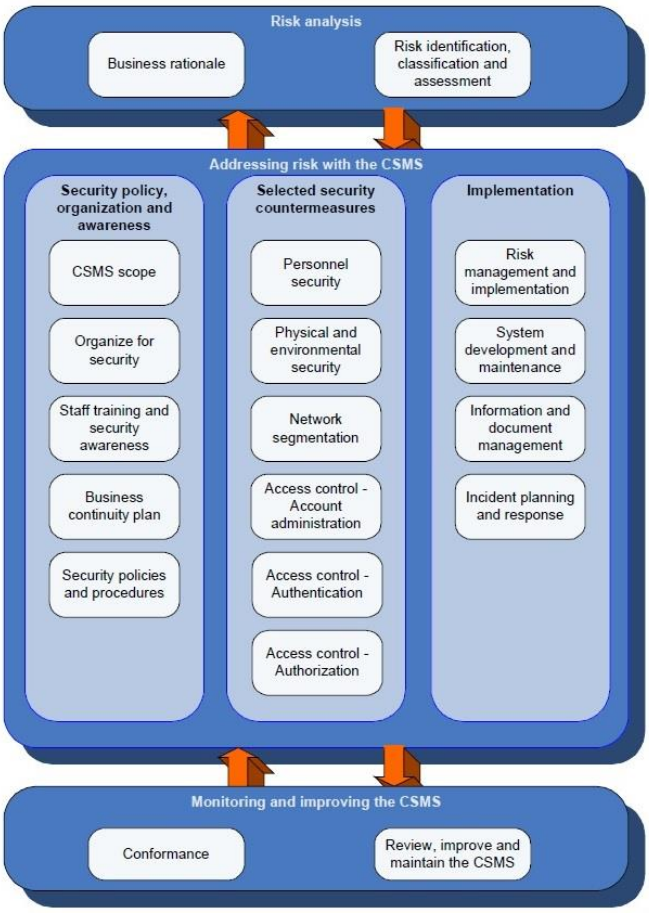

Figure 6 – Elements of an ISA/IEC-62443 CSMS

Besides policies, effort was put into creating appropriate awareness. This was done through formal training at ISA, internal awareness campaigns using artist impressions, informal meetings, more formal presentations at management team meetings, Red Team / Blue Team trainings, etc. Formal OT security roles were defined and assigned to internal and external FTE’s. This has been a step-by-step approach starting with Asset Management having dedicated OT Security Officers to cover risk management and policy development. The next step was having dedicated security roles in the central environment (Scada and Distribution Automation) and finally for the decentralised environments (HV/MV stations).

Select and implement countermeasures

By following the process described in the ISA/IEC-62443 standards and tailoring it for Enexis, a large number of countermeasures were implemented effectively. Some of these measures are:

- Defining & implementing policies for firmware patching and OT security incident planning and response
- Implementation of an advanced Intrusion Detection System to detect anomalies in the OT network traffic
- Training and awareness for all relevant stakeholders
- Advanced firewalls between the OT and IT environment
- Advanced IEC-60870-5 protocol proxies for enforced one-way 104 traffic in critical points of the architecture

Maintain the CSMS

Every month a meeting takes place to evaluate the progress and the performance of the CSMS. The OT Security Officers from Asset Management will define actions if necessary, based on the evaluation in collaboration with the OT Security Manager and Operational OT Security Officer from the internal service provider INFRA. Furthermore, formal internal audits are executed to verify if OT security adheres to established policies and procedures. Via ENCS and OT and IT Security Officers of Enexis that participate in meetings organized by the National Cyber Security Center of The Netherlands, new OT security trends are monitored as well as changes in the legal or regulatory framework. This enables Enexis to react on relevant developments and adapt the CSMS accordingly.

Combining ISA/IEC-62443 with ISO/IEC-27001

In its attempt to professionalize its OT security practice further, Enexis has decided to go for a formal ISO/IEC-27001 certification. ISO/IEC-27001 is a more generic standard for managing information security risks. ISA/IEC-62443 is a specialization of ISO/IEC-27001. As of today formal certification of the CSMS is not possible for ISA/IEC-62443. An ISO/IEC-27001 certification, based on ISA/IEC-62443 content, offers Enexis extra means to show its commitment to managing OT cyber security risks in a professional manner. Furthermore, it will serve as a means to show compliance to the Dutch regulator for DSOs. At the moment of writing external audits for the ISO/IEC-27001 certification have started. Formal ISO/IEC-27001 certification is expected by the end of 2019. By having the OT domain certified via ISO/IEC-27001, integration with the broader security management initiatives at Enexis Group level can be achieved in an efficient way as the Enexis Group policy for cyber security is also based on ISO/IEC-27001.

RESULTS

In 2016 Enexis started with the initiation phase of the CSMS program. Step by step maturity increased: a cyber security risk analysis method has been chosen, all OT cyber security risks have been assessed and documented, countermeasures have been defined, formal OT security roles have been defined and assigned, external parties have been contracted for periodic penetration testing and forensic analysis during possible attacks, testing crisis scenarios caused by an OT cyber security incident, internal audits and follow up, etc. OT security has been integrated into the strategic, tactical and operational processes of Dutch DSO Enexis. OT security is currently part of the lines of business it affects.

DISCUSSION

Enexis has found that ISA/IEC-62443-2-1 combines well with ISO/IEC-27001: ISO/IEC-27001 provides guidelines for the general processes and certification and ISA/IEC-62443 for specific application to OT. Using both standards increases cost, as one has to keep track of compliance to both. Having a generally recognized, certifiable CSMS standard for OT would reduce such cost. Having further European harmonization on ISMS's (term used for CSMS in ISO/IEC-27001) for DSO's would be beneficial. It would reduce the total cost per DSO as more expertise would be available. Formal certification would then be more feasible as the number of organizations using it would grow. The European NIS directive requires that "operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations" [6]. Many EU member states interpret this requirement by asking DSOs to implement an ISMS. But many different ISMS standards are applied. Germany uses a specially developed scheme based on ISO/IEC-27019. France uses a nationally defined scheme. Smaller countries are mostly still looking for the right approach. The NIS cooperation group, headed by ENISA, has developed a reference document on security measures for Operators of Essential Services [7]. But this only contains general advice, and only has one paragraph on OT systems. This lack of harmonization increases the complexity of implementing an ISMS for grid operators.

By harmonizing further, the scope and level of detail of the risk assessments, the risks to the European grid as a whole can also be managed better. Cyber-attacks that impact a few hundred thousand households can cause a Europe-wide blackout. Attackers with such a goal would look for the weakest points to achieve it. So, it is vital that all DSOs in Europe mitigate their risks to acceptable levels. This is much easier to regulate if risk assessments are harmonized to become comparable. Steps towards such harmonization are planned as part of the upcoming network code on cyber-security [8].

REFERENCES

[1] Wikipedia, 2019, "Cyber security standards", *https://en.wikipedia.org/wiki/Cyber_security_standards*

[2] ISA/IEC, 2019, "ISA/IEC-62443 Standards", https://www.isa.org/standards-publications/ and https://webstore.iec.ch/searchform&q=IEC%2062443

[3] Jamdots, 2017, "An interactive artist impression of CSMS at Dutch DSO Enexis", https://jamdots.nl/view/285/Enexis-OT-security

[4] CGE Risk, 2019, "Explanation of bowtie method", https://www.cgerisk.com/knowledgebase/The_bowtie_method

[5] ICS Cert, 2019, "ICS Cert Advisories - Provide timely information about current security issues, vulnerabilities, and exploit", https://ics-cert.us-cert.gov/advisories

[6] European Commission, 2017, "NIS Directive", https://ec.europa.eu/digital-single-market/en/network-and-information-security-NIS-directive

[7] NIS Cooperation Group, 2018, "Reference document on security measures for Operators of Essential Services", https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[8] Smart Grid Task Force - Expert Group 2, 2019, "Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity", https://ec.europa.eu/energy/en/topics/market-and-consumers/smart-grids-and-meters/smart-grids-task-force