Cybersecurity requirements for Grid Operators

D4.4

Authors:

Magda Zafeiropoulou (UBE)

Anastasis Tzoumpas (UBE)

Ivelina Stoyanova (RWTH)

Apostolos Kapetanios (ED)

Ferdinando Bosco (ENG)

Madalena Lacerda (E-REDES)

Responsible Partner	UBITECH ENERGY
Checked by WP leader	Ivelina Stoyanova (RWTH) - Date: 26/05/2023
Verified by the appointed Reviewers	Bartosz Kalinowski (TTST) - Date 29/05/2023
Approved by Project Coordinator	Padraic McKeever (Fraunhofer) – Date: 23/06/2023

Dissemination Level	Public	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	31/3/2023
Actual date of delivery	23/6/2023
Status and version	V1.0 – Final Version

Version	Date	Author(s)	Notes
0.1	13.02.2023	Anastasis Tzoumpas (UBE) Magda Zafeiropoulou (UBE) Apostolos Kapetanios (ED)	First version with ToC and first input.
0.2	17.02.2023	Magda Zafeiropoulou (UBE)	Elaboration on section 5.
0.3	27.02.2023	Madalena Lacerda (E-REDES)	Elaboration on section 4.
0.4	16.03.2023	Ivelina Stoyanova (RWTH) Ferdinando Bosco (ENG) Apostolos Kapetanios (ED) Magda Zafeiropoulou (UBE)	Elaboration in all sections.
0.5	31.03.2023	Apostolos Kapetanios (ED) Anastasis Tzoumpas (UBE)	Elaboration in all sections.
0.6	07.04.2023	Apostolos Kapetanios (ED) Magda Zafeiropoulou (UBE)	Elaboration in all sections.
0.7	21.04.2023	Apostolos Kapetanios (ED) Magda Zafeiropoulou (UBE)	Elaboration in all sections.
0.8	10.05.2023	Magda Zafeiropoulou (UBE) Anastasis Tzoumpas (UBE)	Elaboration in all sections.
0.9	15.05.2023	Anastasis Tzoumpas (UBE)	Final draft version ready for review.
1.0	22.06.2023	Madalena Lacerda (E-REDES) Anastasis Tzoumpas (UBE) Ivelina Stoyanova (RWTH) Apostolos Kapetanios (ED) Magda Zafeiropoulou (UBE) Ferdinando Bosco (ENG) Ivelina Stoyanova (RWTH)	Final version ready for submission.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

About OneNet

The project OneNet (One Network for Europe) will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

OneNet is funded through the EU's eighth Framework Programme Horizon 2020, "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

As the electrical grid moves from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. The project brings together a consortium of over seventy partners, including key IT players, leading research institutions and the two most relevant associations for grid operators.

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
ACER	Agency for the Cooperation of Energy Regulators
AMI	Advanced Metering Infrastructure
Art.	Article
CEP	Clean Energy Package
CII	Critical Information Infrastructure
CIS	Centre for Internet Security
CSIRTs	Computer Security Incident Response Teams
DER	Distributed Energy Resources
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
ENISA	European Union Agency for Cybersecurity
ENTSO-E	European Association for the cooperation of Transmission System Operators for Electricity
EPES	Electrical Power and Energy System
EU	European Union
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
FSP	Flexibility Service Provider
GDPR	General Data Protection Regulation
GRC	Governance, risk and compliance
ICT	Information and Communications Technology
IDS RAM	IDS Reference Architecture Model
IDSA	International Data Spaces Association
ISAC	Information sharing and analysis centres
ISMS	Information security management system
NCCS	Network Code on Cybersecurity
NIS	Network and Information Security
NISD	NIS Directive
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NRA	National Regulation Authority
NSM	Network and System Management
PLCs	Programmable Logic Controllers
RBAC	Role-based access control
RES	Renewable Energy Sources
SCA	Security Configuration Assessment
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

SGIS	Smart Grid Information Security
TRL	Technology Readiness Level
TSO	Transmission System Operator
UCS	Use Case Subject
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Executive Summary

The OneNet Reference Platform (as per OneNet Deliverable D6.5 and upcoming D6.8) aims to showcase that the concepts developed and evolved through the various work packages of the OneNet project can result to an architecture and a feasible system that can easily connect any flexibility platform and will enable the various stakeholders to exchange data focusing on reliability and trust.

The present Document (D4.4 "*Cybersecurity requirements for Grid Operators*") summarises the findings of Task 4.4 "Requirement analysis of cyber security measures for grid operators and customer integration" which investigates cybersecurity and confidentiality measures moving vertically from business through information and communication layer up to the component layer. As a result, the present document attempts to set cybersecurity and confidentiality requirements from the operator perspective focusing on the operational aspects of grid operators. The whole deliverable tightly correlates with the deliverable D5.8 in which the general requirements of cybersecurity are defined from a data management perspective.

The reader is provided in the present document with a detailed analysis of the legal and security framework to be applied in the context OneNet, based on relevant references, i.e. NISD, GDPR, NISTIR, ENISA, and the Electricity Network Codes and Guidelines. This conceptual framework lays the foundation for the identification and presentation of fundamental recommendations/measures for privacy, data protection and security. The document also provides a methodology for the identification of potential concerns within operators and their use case scenarios, as well as for their assessment in terms of likelihood and impact. A Use Case Subject (UCS) template for gathering data and performing self-assessment has also been defined. The analysis performed in this task visualizes a high level of cybersecurity awareness of the consortium and how security concerns can be solved by understanding principles and guidelines, and by clarifying key concepts coming from the legal framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

1 Introduction

1.1 Scope of the Document

OneNet will develop an open and flexible architecture to transform the actual European electricity system, which is often managed in a fragmented country- or area-level way, into a pan-European smarter and more efficient one, while maximizing the consumer capabilities to participate in an open market structure. According to OneNet Description of Action (DoA), WP4 contributes to the direction of fulfilling the OneNet vision by attaining two objectives:

- Create the necessary interfaces in terms of information models, timing requirements and interaction sequences in the context of e.g., pre-qualification, schedules, maintenance etc. whilst covering mainly the operational challenges that arise with the introduction of new products and markets as analysed in WP2 and WP3.
- Propose specific cybersecurity measures focused on the device level, as part of the OneNet integration plan, which will safeguard the whole system in relation with proposed guidelines of T5.8 and deliverable D5.8 “Report on Cybersecurity, privacy and other business regulatory requirements”.

The OneNet Reference Architecture IT implementation (as per WP5 “Open IT Architecture for OneNet” and WP6 “Reference IT Implementation for OneNet”) has addressed cybersecurity aspects that refer to it as it is documented in D5.8 and D6.6. However, as the OneNet is an interoperable network of platforms, i.e. enables seamless and trusted data exchange among platforms that are operated by or serve other stakeholders -network operators being pivotal among them- there are cybersecurity considerations that need to be addressed from the side of such platforms, not as OneNet users but as counterparties of the OneNet system. Task 4.4 contributes to the overall WP4-level objectives by proposing cybersecurity, privacy, and other regulatory requirements and countermeasures. Specifically, this report focuses on eliciting societal, ethical, legal, data protection and security requirements, with a special attention to cybersecurity and privacy issues potentially arising along with the design and development of OneNet platform of platforms. As a result of the work of T4.4, the present document expresses recommendations on cybersecurity (drafting requirements and countermeasures) from the operator perspective.

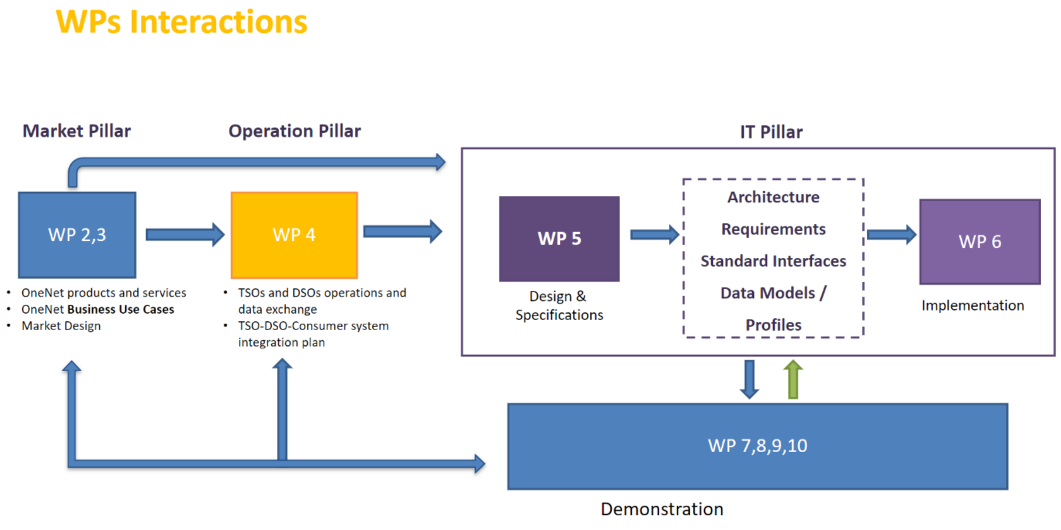


Figure 1: OneNet WPs interdependencies.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

As illustrated in Figure 1, there are a lot of interdependencies amongst tasks in different WPs, involving T4.4. Regarding the horizontal WPs, WP4 utilizes the data privacy requirements declared in this deliverable and in D5.8 to conduct a requirement analysis regarding cybersecurity measures for grid operators and customer integration. Moreover, other tasks of WP5 responsible for the development of the OneNet architecture, and the extended data and service interoperability in the OneNet platform of platforms, are considering input need from this deliverable, especially regarding standards for data security in the energy sector. The vertical WPs 7 to 10 shall leverage the information documented in this report, especially from the conducted survey and the extracted key messages, in order to enhance their perspective towards cybersecurity issues and data protection in the demonstration activities that will take place in the context of the OneNet project. So the outcome of this deliverable in conjunction with D5.8 constitutes the foundations from a security perspective based on which the OneNet concept is built upon.

1.2 Relation to other Deliverables

Current deliverable takes into consideration the BUCs presented in D2.3 (“Business Use Cases for the OneNet“) and is closely related to D5.8 “Report on Cybersecurity, privacy and other business regulatory requirements” and leverages input from D5.1 “OneNet Concept and Requirements” and D5.2 “OneNet Reference Architecture”, while it considers also the TSO perspectives (D4.1).

1.3 Document Structure

The structure of this deliverable is unfolded as follows:

Chapter 2 includes the methodology introduced for the creation of this deliverable.

Chapter 3 highlights key points of the legal regulatory framework in the energy sector along with the EU regulation regarding data protection that must be considered in the assessment of cybersecurity requirements for grid operators.

Chapter 4 highlights key points of the energy sector security framework along with details regarding the most important cybersecurity standards in the energy industry that are also important for the assessment of the cybersecurity requirements for grid operators.

Chapter 5 presents other H2020 projects that dealt with issues of cybersecurity in the energy sector.

Chapter 6 presents the results of a survey among the partners participating in the OneNet demonstrators, providing important information regarding their perspectives, knowledge, and expectations of cybersecurity in the context of OneNet.

Chapter 7 describes the requirements for Cross Stakeholder Data Governance in accordance with the principles and recommendations of the IDSA and the security constraints considered in the Reference Architecture of OneNet.

Chapter 8 presents the actual cybersecurity recommended measures and related processes.

Finally, **Chapter 9** concludes the work conducted in this deliverable and acts as a connection point delivering the key outcomes needed by other OneNet tasks.

2 Methodology

The methodology used in OneNet for the identification and definition of legal and security concerns is based on a three-step process workflow, where the conceptual framework constitutes the foundation (see Figure 2).

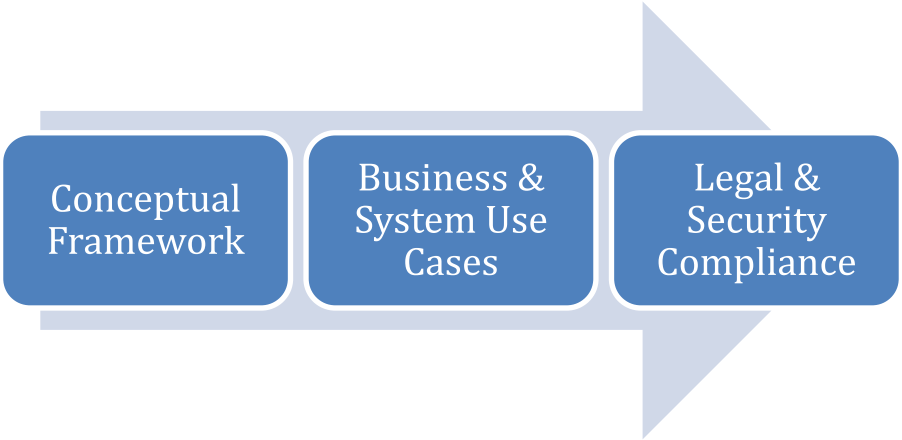


Figure 2: OneNet Legal & Security Methodology.

The conceptual framework forms the basis of the legal regulations and security standards to be applied for the defined OneNet objectives, use case scenarios and technology implementation. This conceptual framework provides the consortium with security rules and governance policies to be followed during the whole project lifecycle. For defining the conceptual framework, OneNet is using references such as GDPR, Electricity Network Codes and Guidelines, and NISD.

This conceptual framework is instantiated by analysing OneNet use case scenarios and data exchange processes. This process doesn't aim to replicate the technical details of the use case scenarios. The end goal is to use these use cases and their respective functional specifications as inputs for the assessment of potential concerns (i.e., privacy, security) and suggest specific countermeasures. For the actual analysis of the use cases a use case security template can be defined and used as shown below in Table 1. This template is a simple and effective tool for monitoring and assessing potential concerns, and if necessary, partners can update during the project lifecycle with further details.

Table 1: Use Case Subject (UCS) Template

UC ID	**[Use Case Number and Subject]**
Description	[Use Case Description]
Owner	[Use Case Owner]
Service	[Selected Cross-Platform service]
Data Description	[Data Identification & Description]
Data Source	[List of Data Sources]
Data Producer	[List the Data Producer]
Personal Data	Yes / No / NA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Data Protection Mechanisms	If data contain personal data, specifies the purpose and the designed mechanisms to be applied Options: {Anonymisation, Pseudonymisation, Aggregation, Minimisation}
Potential Concerns	Based on analysis of the above information, identified potential concerns in terms of likelihood and impact.
Best Practices	Best Practices in relation to the above concerns

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 Legal Framework – Data Protection

The implementation of the OneNet Reference Architecture (see D6.5) is an open system that gives its users/platforms the flexibility to define and describe their own Cross-Platform-Services and related Business Objects (see D5.3 and D5.6). In this regard, although the OneNet system (i.e. the implementation of the Reference Architecture) does not handle personal data and is data agnostic in terms of the data exchange, the exchanged data might include personal information. In this context a specific data protection legal framework is depicted according to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as: GDPR [1]). The following subsections provides the reader with energy-domain specific details regarding this regulation, relevant to the project activities, its use case scenarios and expected outcomes.

3.1 OneNet Data Protection Legal Framework

As mentioned also in deliverable D5.8 “Report on Cybersecurity, privacy and other business regulatory requirements”, GDPR is one of the most important general legislations governing the privacy and protection of personal data of persons whose data is processed using automated or manual means. It focuses on enforcing individual rights, assuring tighter rule enforcement, boosting the EU internal market, facilitating international personal data transfers, and establishing global data protection standards. GDPR applies once personal data is processed; these are defined by the GDPR as:

“Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4 (1)).”

Examples of personal data could be the name and surname of a person directly engaged in the OneNet project, the home address of that person and the corporate e-mail address. It is of high importance to highlight at this point that account should be taken of all the means reasonably likely to be used to identify a person. In this respect:

“Personal data that has been de-identified, encrypted or pseudonymized, but can be used to re-identify a person remains personal data and falls within the scope of the law".

Personal data, on the other hand, that has been made anonymous to the point where the individual can no longer be identified is no longer considered personal data. Anonymization must be permanent in this scenario. Therefore, GDPR privacy protection must be explicitly considered during the entire project. In addition to the definition of the personal data, sensitive data is also defined in the context of the GDPR. Sensitive data is personal data revealing information about racial or ethnic origin, political opinions, religious or philosophical beliefs. Moreover, as sensitive data can be considered trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data and data concerning a person’s sex life or sexual orientation. In the context of OneNet, it is necessary to address the issue of personal and sensitive data protection in advance. For example, those data could be sensitive information of the market participants (wholesale and local flexibility markets), end-customers’ personal information etc. The following subchapter presents the requirements that have to be applied in order the OneNet to be in compliance with the GDPR.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

3.2 Personal Data Definition

Specific definitions regarding personal data are part of article 4 of the GDPR. They are mostly related to sensitive and specific aspects of the personality of physical subjects, and can be categorized as follows:

- **genetic data:** they are "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*" [article 4, n. (13)];
- **biometric data:** they are "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*" [article 4, n. (14)];
- **data concerning health:** they are "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*" [article 4, n. (15)].

The above categories of personal data are subject to additional protections and they are considered the core citizen data which require protection as stated by privacy regulations.

3.3 Smart Grids and Personal Data

In 2009 the European Commission set up the Smart Grid Task Force with the responsibility to advise on issues related to smart grid deployment and development and help shape EU smart grid policies. **Smart Grid Task Force** consists of five Expert Groups, including Expert Group 2 – *Regulatory recommendations for privacy, data protection and cyber-security in the smart grid environment.* This group provided a non-exhaustive example of personal data as follows:

- Household and organizations energy consumption,
- Consumer registration data: names and addresses of data subjects, etc.,
- Usage data (such as energy consumption), as these provide insight in the daily life of citizens,
- Amount of energy and power (e.g., kW) provided to the grid (energy production),
- Locally produced weather forecast – consumption prediction / forecasts,
- Demand forecast of building, campus and organization,
- Technical data (tamper alerts), as these might change how the data subject is approached,
- Profile of types of consumers, as they might influence how the consumer is approached,
- Data and function of individual consumers / loads,
- Facility operations profile data (e.g., hours of use),
- Frequency of transmission of data, as these might provide insight in the daily life of citizens,
- Billing data and consumer's payment method.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.4 Data Governance Roles

The processing of personal data in the smart grid context, requires a clear definition of GDPR Data Governance Roles such as data subject, data controller, data processor, third party and recipient. As per data protection regulation:

- **data subject** is the individual and natural person to whom personal data are referred.
- **data controller** (or simply the "controller") is the natural person or legal entity, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. In other words, the data controller is the one who is directly responsible for the processing, for its purposes, for the security measures, and so on.
- **data processor** (or simply the "processor") is the one who processes personal data on behalf of the controller. The processor may be an internal subject belonging to the entity which acts as controller or an external subject.
- **data recipient** is a "*natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing*".
- **third party** is a *"natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data".*

3.5 Smart Grids and Data Governance Roles

The Expert Group 1 – *Standards and Interoperability for Smart Grids Deployment*, in the context of the Smart Grid Task Force set up by the European Commission in 2009, issued a report [2] in November 2016 where it attempts to define the main data governance roles in Smart Grids (see previous chapter definitions).

All these roles are mapped into the GDPR:

- The data subject could be considered as the customer or the party connected to the grid.
- The controller could be considered as the party responsible for data management (partly) or the metered data responsible.

  The processor could be considered as the party responsible for data management (partly), metered data collector or metered data aggregator.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.6 Consent

A general rule of GDPR states that consent is absolutely required in order to process personal data. Consent is not necessarily in written format but must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous willing. In some specific cases – e.g., where personal data are required for the execution of a contract agreed with the data subject – consent is not required.

3.7 EU Legal Framework in the Energy Sector

The European Union's legal framework for electricity originated in the Third Energy Package legislation of 2009. This framework has recently been adjusted by the legislation forming the Clean Energy Package (CEP), and such amendments came into force in January 2020. Like every EU Regulation, the Package Regulations are legally binding, directly applicable, and enforceable by Member States. Since the aim of the mentioned Packages is to harmonize rules and principles on the subject for all EU Member States, most of the provisions laid down in the legislation are addressed to the legislative bodies of the Member States, which may specify the contents by internal provisions.

4 Energy Sector Security Framework

This section will describe the security framework applicable to the European energy sector, more specifically, by providing an overview of the proposal under discussion for the cybersecurity network codes, the NIS 2 Directive, the main cybersecurity standards and the main recommendations, guidelines and frameworks established both within the Smart Grid Information Security (SGIS) working group, NISTIR and ENISA.

4.1 Cybersecurity Network Codes

4.1.1 Supporting regulatory framework and process

The Internal Market Regulation (Regulation (EU) 2019/943) [3] that was published under the Clean Energy Package foresees, in Article 59(2), the establishment of new network codes and the revision of existing ones to make sure that the technical rules and guidelines that support its implementation exist and are harmonized until certain extent at an EU level.

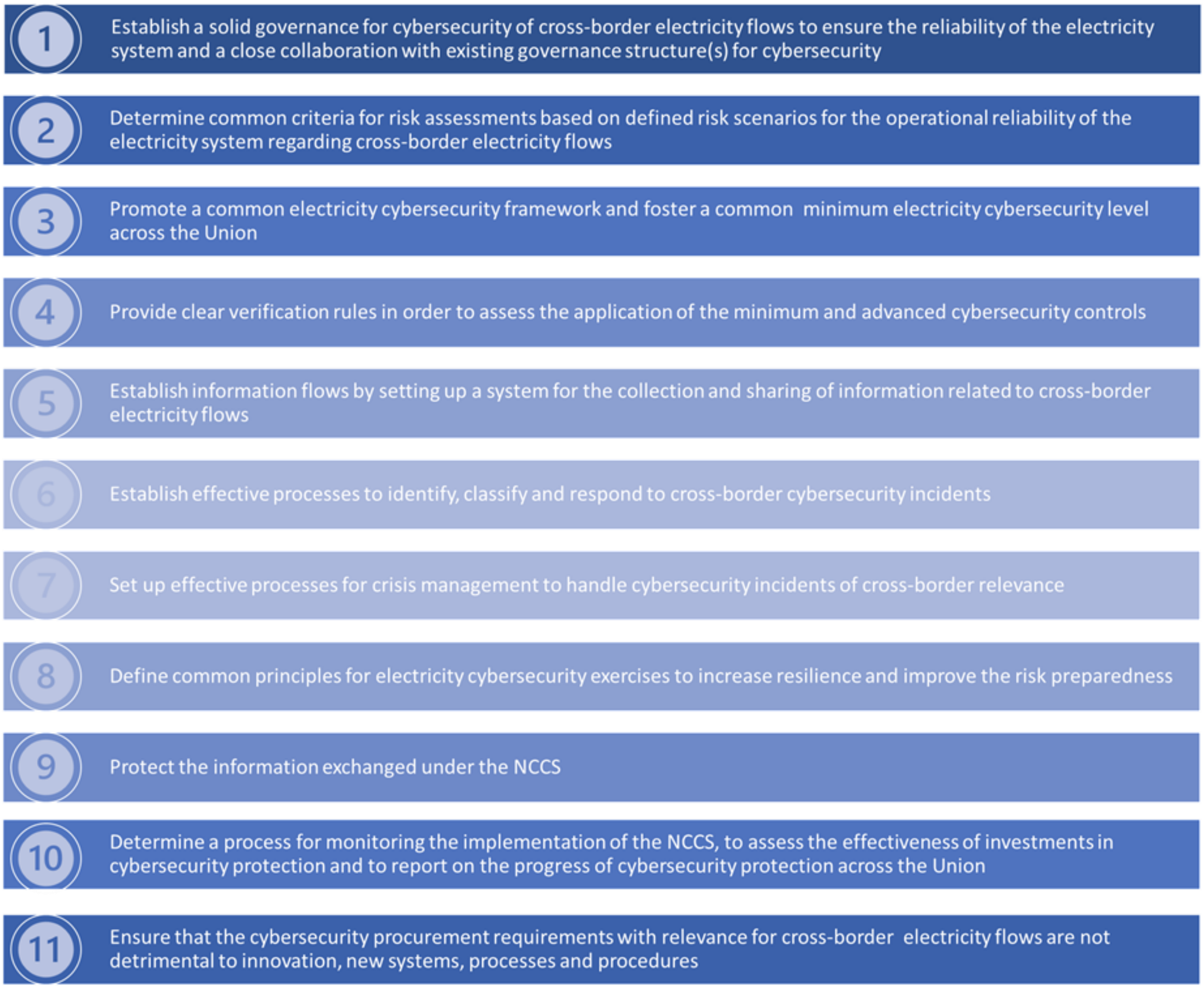
Within the new network codes, the Regulation foresees the development of “sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management”. The Network Code on Cybersecurity (NCCS) comes in response to this provision and is the first one being developed according to the (co)drafting process defined in the Regulation, meaning, it is a result of joint work between ACER, ENTSO-E and the EU DSO Entity. At the time of writing this deliverable, ACER has already submitted the NCCS to the EC in July 2022 for revision [4], now awaiting adoption of delegated acts.

4.1.2 Guiding principles and objectives

The NCCS focuses on the definition of common minimum requirements, an integrated approach for risk assessments, a common cybersecurity framework, and clear responsibilities on protection and exchange of information. It must also respond to the provisions under Article 58(2) of the Regulation, by ensuring a minimum degree of harmonization and by taking into account regional specificities, thus leaving some room for more concrete rules to be defined at the regional/national level. The NCCS is binding in nature, meaning that once it is adopted by the EC through a delegated act, its requirements will be immediately reflected in the stakeholders’ businesses, which can have a fundamental bearing on them.

The NCCS main aim is to define common cybersecurity requirements to guarantee security of supply and ensure the highest degree of cybersecurity protection in the EU electricity sector. It assigns responsibilities to diverse bodies, ranging from EU level bodies, regional bodies and national level bodies, and defines shared responsibilities between the different institutions regarding risk assessments, information flows in case of a cybersecurity incident and monitoring of the operational reliability of the NCCS. The main objectives of the NCCS are mapped in Figure 3.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739



1. Establish a solid governance for cybersecurity of cross-border electricity flows to ensure the reliability of the electricity system and a close collaboration with existing governance structure(s) for cybersecurity
2. Determine common criteria for risk assessments based on defined risk scenarios for the operational reliability of the electricity system regarding cross-border electricity flows
3. Promote a common electricity cybersecurity framework and foster a common minimum electricity cybersecurity level across the Union
4. Provide clear verification rules in order to assess the application of the minimum and advanced cybersecurity controls
5. Establish information flows by setting up a system for the collection and sharing of information related to cross-border electricity flows
6. Establish effective processes to identify, classify and respond to cross-border cybersecurity incidents
7. Set up effective processes for crisis management to handle cybersecurity incidents of cross-border relevance
8. Define common principles for electricity cybersecurity exercises to increase resilience and improve the risk preparedness
9. Protect the information exchanged under the NCCS
10. Determine a process for monitoring the implementation of the NCCS, to assess the effectiveness of investments in cybersecurity protection and to report on the progress of cybersecurity protection across the Union
11. Ensure that the cybersecurity procurement requirements with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures

Figure 3: NCCS objectives.

Apart from that, and given the constant development of the electricity sector, that comes with a frequent introduction of new systems, processes and procedures, these shall also respect cybersecurity requirements. Hence, these new trends and related future cybersecurity risks will be regularly reported, within the framework of the NCCS.

It is important to highlight that the NCCS is not defining requirements from the ground up, it actually builds on top of existing legal requirements and complements them to maximize cybersecurity in the EU electricity system. Namely, the general rules on security and information systems established in the NIS Directive are complemented by the NCCS, to ensure that cybersecurity incidents are properly identified as a risk and that necessary measures are included in the risk-preparedness plans. Also, by being quite generic in scope, the NCCS doesn't provide all necessary rules for ensuring cybersecurity of cross-border flows but provides a clear timeline and the main principles to be followed in the development of necessary requirements, criteria, methodologies and performance indicators that complement the network code itself.

4.2 NIS 2 Directive

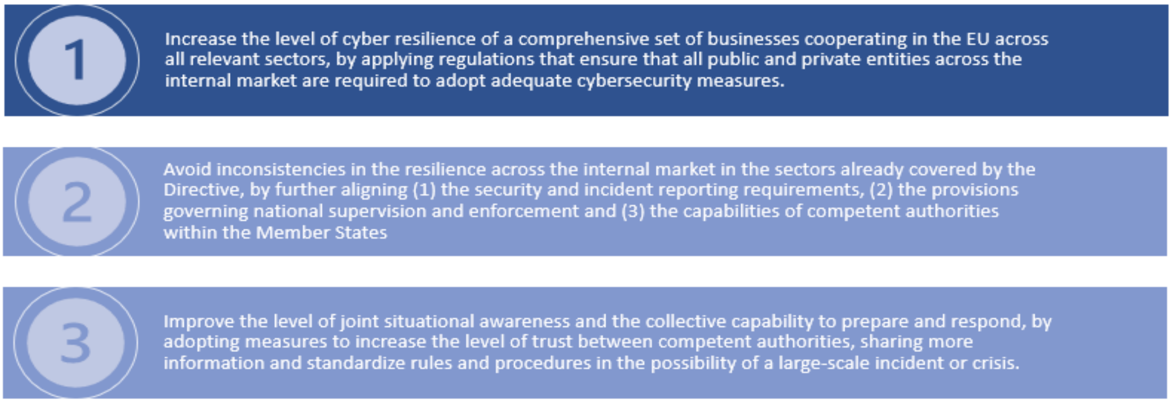
4.2.1 Supporting regulatory framework and process

The NIS (Network and Information Security) 2 Directive [5] is aligned with the actions foreseen in the EU's Cybersecurity Strategy for the digital decade and was created to suppress the limitations of NIS 1, as a consequence of the rapid pace of digitalization, the increased interconnectivity of sectors and the heightened cyber security risks resultant from increased risk exposure of the energy sector. Growing interdependencies result from the increasingly cross-border and interdependent network of service provision using key infrastructures across EU, such as energy, transport, digital infrastructure, drinking water and health. Thanks to those interdependencies, any disruption may have cascading effects more broadly, potentially resulting in far-reaching and long-standing negative impacts.

The NIS 2 Directive applies to all entities which provide their services or carry out their activities in the EU and considered as an "essential" or an "important" entity in a defined list of sectors, within which the energy sector is considered as essential. The required measures foreseen in the directive include risk analysis and incident response; encryption and cryptography; vulnerability disclosure; cybersecurity training and ICT (Information and Communications Technology) supply chain security. The NIS 2 Directive is intended to be a baseline for minimum hazard on cybersecurity and establishes interlinkages between the cyber and physical security of entities.

4.2.2 Guiding principles and objectives

With the NIS review, three broad objectives are described in Figure 4 [6].



1 Increase the level of cyber resilience of a comprehensive set of businesses cooperating in the EU across all relevant sectors, by applying regulations that ensure that all public and private entities across the internal market are required to adopt adequate cybersecurity measures.

2 Avoid inconsistencies in the resilience across the internal market in the sectors already covered by the Directive, by further aligning (1) the security and incident reporting requirements, (2) the provisions governing national supervision and enforcement and (3) the capabilities of competent authorities within the Member States

3 Improve the level of joint situational awareness and the collective capability to prepare and respond, by adopting measures to increase the level of trust between competent authorities, sharing more information and standardize rules and procedures in the possibility of a large-scale incident or crisis.

Figure 4: NIS 2 Directive objectives.

To achieve such goals, the NIS 2 Directive imposes the obligation to notify competent authorities of significant incidents and cyber threats, with the usage of an automatic and direct forwarding of incidents notifications.

ENTSO-E, in cooperation with the EU DSO entity, shall select the types of ICT products, services and processes for which sets of cybersecurity procurement recommendations are developed based on the priorities of high-impact and critical-impact entities.

It is of responsibility of Member States to address cybersecurity in the supply chain for ICT products and services used by entities for the provision of their services. It is advised to encourage the promotion and facilitation of voluntary coordinated vulnerability disclosure. For that, it is a best practice to make use of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

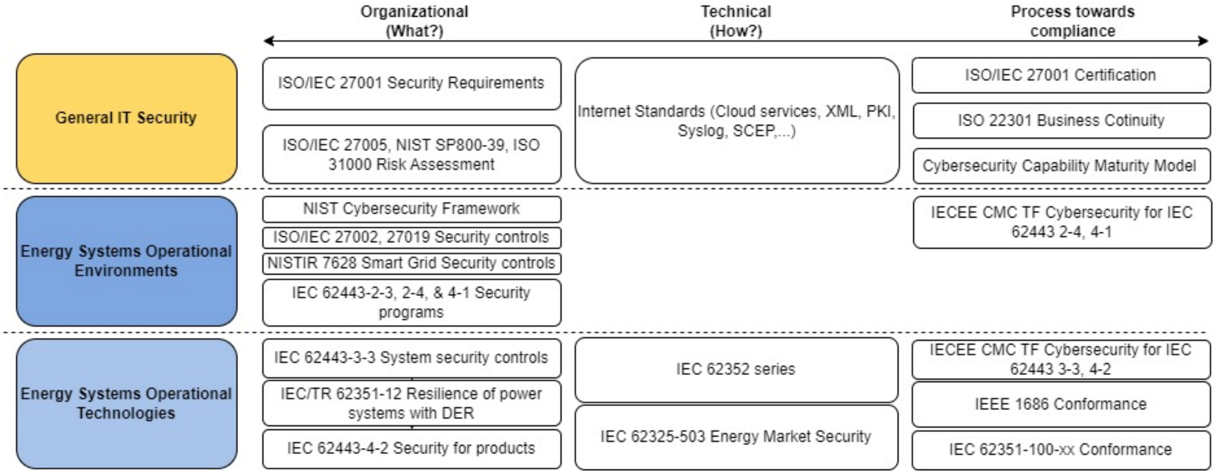
information-sharing tools to support and encourage voluntary cybersecurity information sharing between companies.

A type of entity that is described in the NIS 2 Directive - CSIRTs (Computer Security Incident Response Teams) – shall be responsible for analysing cyber threats, vulnerabilities and incidents at national level. For this, it might be helpful to facilitate a proactive scanning of the network and information systems to detect vulnerabilities with potential significant impact, considering that the network and information systems are not intruded, or their functioning negatively impacted.

In addition, with the aim to ensure that NIS 2 Directive is followed properly, a cooperation group formed by representatives of Member States, the European Commission and ENISA will work for the exchange of best practices and of information concerning cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, as well as standards and technical specifications.

4.3 Cybersecurity Standards in the Energy Sector

Both the complexity of business processes and the variety of assets used within the smart grids' environment requires more than one cybersecurity standard to be used to address the different security requirements, controls, strategies, and technologies. Hence, the different standards and guidelines have different purposes, with some being more focused on the high-level organizational security requirements (what?) and others on the technical implementation of these cybersecurity controls (how?) [7]. The categorization and classification of the different standards and guidelines can be found in Figure 5 and the main standards and guidelines are described in the sub-sections below.



	Organizational (What?)	Technical (How?)	Process towards compliance
General IT Security	ISO/IEC 27001 Security Requirements ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment	Internet Standards (Cloud services, XML, PKI, Syslog, SCEP,...)	ISO/IEC 27001 Certification ISO 22301 Business Cotinuity Cybersecurity Capability Maturity Model
Energy Systems Operational Environments	NIST Cybersecurity Framework ISO/IEC 27002, 27019 Security controls NISTIR 7628 Smart Grid Security controls IEC 62443-2-3, 2-4, & 4-1 Security programs		IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1
Energy Systems Operational Technologies	IEC 62443-3-3 System security controls IEC/TR 62351-12 Resilience of power systems with DER IEC 62443-4-2 Security for products	IEC 62352 series IEC 62325-503 Energy Market Security	IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 IEEE 1686 Conformance IEC 62351-100-xx Conformance

Figure 5: Cybersecurity standards and Guidelines that apply to smart energy operational environments.

4.3.1 ISO/IEC 27001

The ISO/IEC 27001 [8] international standard on "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" provides requirements for the setup of an information security management system (ISMS). Namely, it identifies information assets and associated information security requirements, while also considering legal, regulatory, and contractual requirements. It also allows to evaluate the information security risks and treat these risks either through a risk analysis and evaluation, or through the application of appropriate controls. It also allows to select and implement relevant controls to manage unacceptable risks.

4.3.2 ISO/IEC 27002

The ISO/IEC 27002 [9] international standard on "Information security, cybersecurity and privacy protection – Information security controls" provides a set of generic information security controls, and includes guidelines for implementation by organizations. It addresses the following areas: organization of information security; asset management; access control; cryptography; physical and environmental security; system acquisition, development, and maintenance; supplier relationship; Information security incident management; and compliance.

4.3.3 ISO/IEC 27019

The ISO/IEC 27019 [10] international standard on "Information technology — Security techniques — Information security controls for the energy utility industry" provides guidance for information security management based on ISO/IEC 27002 requirements. It covers process control systems used in energy utilities, for the monitoring and control of generation, storage, distribution and transmission of electricity, gas and heat, and for the control of associated supporting processes.

Thus, it covers systems, applications and components such as the overall IT-supported central and distributed process control, monitoring and automation technology as well as information systems used for their operation; digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs); supporting information systems used for process control; communication technology used in process control; Advanced Metering Infrastructure (AMI) components; measurement devices; digital protection and safety systems; energy management systems; distributed components of smart grid environments; all software, firmware and applications installed on above-mentioned systems; any premises housing the above-mentioned equipment and systems; remote maintenance systems for above-mentioned systems.

4.3.4 IEC 62351 series

The IEC 62351 series [11] defines the cybersecurity requirements to allow the implementation of security technologies in the operational environment and is composed of objects for network and system management, role-based access control (RBAC), cryptographic key management, and security event logging. Table 2 presents the list of standards and guidelines included within the series.

Table 2: List of standards included in the IEC 62351 series.

Standard	Denomination
IEC/TS 62351-1	Introduction
IEC/TS 62351-2	Glossary of Terms
IEC 62351-3 to 6	Data and Communication Security
IEC 62351-7	Network and System Management (NSM) of the information infrastructure
IEC 62351-8	Role-Based Access Control for Power System Management
IEC 62351-9	Key Management

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

IEC/TR 62351-10	Security Architecture
IEC 62351-11	Security for XML Files
IEC/TR 62351-12	Resilience for Power Systems with DER Systems
IEC/TR 62351-13	What Security Topics Should Be Covered in Standards and Specifications
IEC 62351-14	Cyber Security Event Logging

4.4 SGIS Report

The Smart Grid Information Security (SGIS) is a working group that was mandated by the European Commission to support the deployment of smart grids in Europe, by promoting an information and communication system that is secure by design. The group has published a report [12] providing guidance for smart grid deployment and identifying main standards to be adopted by stakeholders.

From a guidance perspective, the report defines a set of recommendations, including the establishment of a SGIS Framework as a methodology for risk assessment, allowing measures to be identified to tackle existing security threats.

The group also highlights the importance of selecting the right security standards to reinforce security and reliability of smart grids from a technical, an organizational or procedural point of view, therefore, not only a standardization landscape is described but also an analysis is carried out to identify, not only the applicability of the existing standards on the different SGAM domains and layers, but also the main gaps from these same standards.

4.4.1 Analysis to existing standards

The report identifies the main gaps from existing standards, which are related to shortcoming or even missing coverage of dedicated requirements. In general terms, the standards analysed are enough to guarantee information security, however, gaps and improvement measures have been identified for several standards.

For instance, and as a first outcome from this analysis, there are several standards that do not cover privacy by design, which is the case for IEC 62443-2-1, IEC 62443-3-3, ISO /IEC 15118-2 (Road Vehicles – Vehicle-to-Grid Communication Interface). On another note, ISO/IEC 19790 by itself is not enough to provide sufficient security conditions to a cryptographic module, thus, a common set of security requirements for modules to be used in the future will be needed.

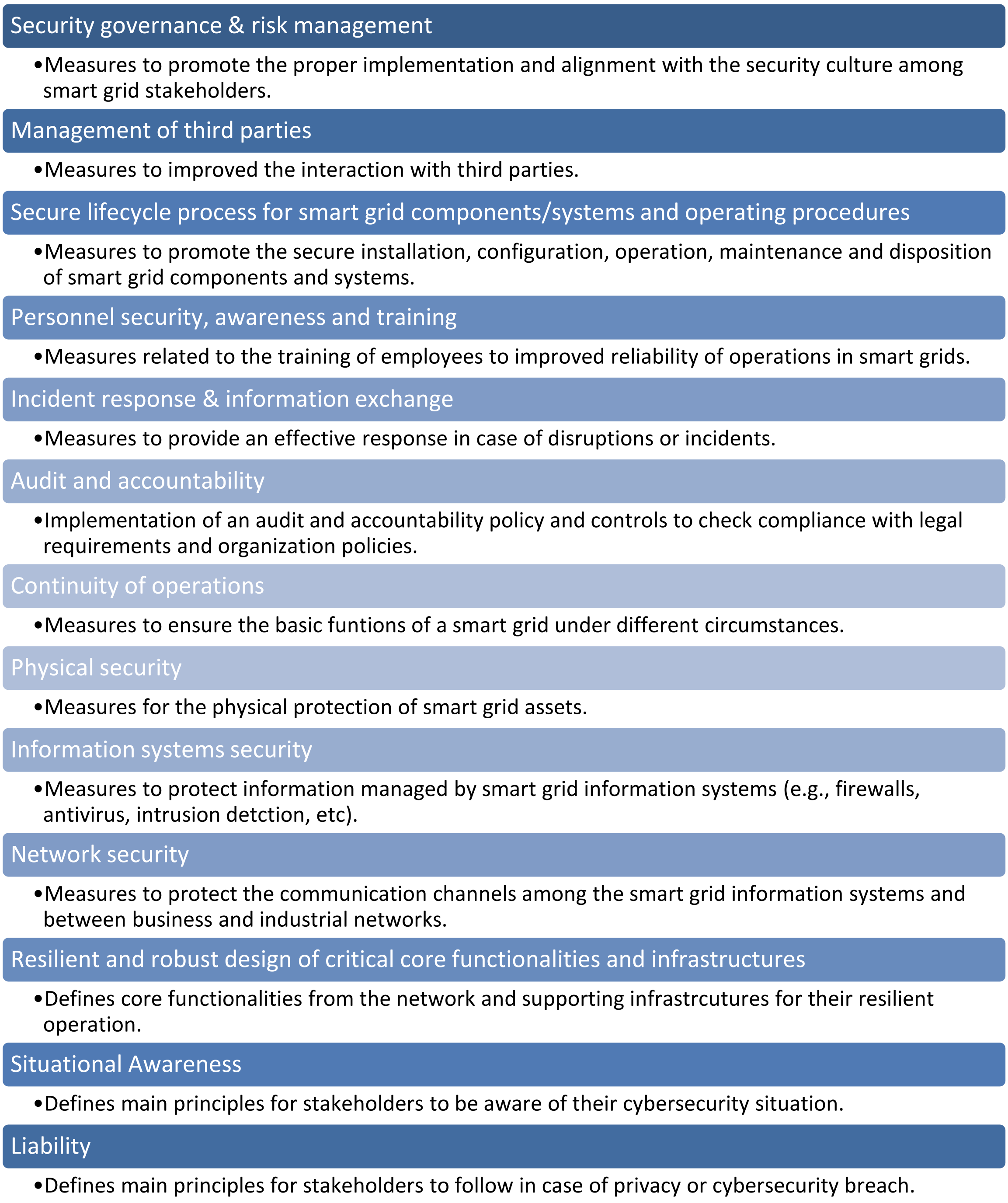
More specifically for ISO/IEC 15118-2 (Road Vehicles – Vehicle-to-Grid Communication Interface), besides not including recommendations for signature devices, it is missing references on metering standards, it doesn't consider an off-line case and lacks provisions for service, parameterization and installation. Regarding IEC 62056-5-3 (DLMS/COSEM Security), it lacks definitions for key management of application level symmetric keys, which can be addressed by defining certificate profiles and by interacting with a public key infrastructure. Also, the application layer security mechanisms described in the standard need to be embedded into an overall system security architecture, which is not being addressed.

Lastly, regarding IEC 62351-x (Power Systems Management and Associated Information Exchange – Data and Communication Security) there are also several shortcomings identified. For example, IEC 62351-8 is lacking a mandatory profile for RBAC support, some usage examples for the roles and rights for easier administration and it doesn't address device management and operation, which are required to guarantee a unified RBAC approach. IEC 62351-10 lacks the incorporation of the European view on DER needs, and regarding IEC 62351-11, some improvements are required from the security point of view, such as sensitivity labelling, cryptographic protection and enforcement of labelling.

Nonetheless, the report concludes that the standards that are needed to guarantee information security in smart grids are already available, but require continuous incorporation of existing and new technologies, architecture, use cases, policies and best practices.

4.4.2 European Set of Recommendations

A European set of recommendations has been defined to support stakeholders in building and designing a smart grid infrastructure that is secure by design. The recommendations are thoroughly described in the "Proposal for a list of security measures for Smart Grids" report [13] and can be divided into 13 domains, which are presented and described in Figure 6.



Security governance & risk management

- Measures to promote the proper implementation and alignment with the security culture among smart grid stakeholders.

Management of third parties

- Measures to improved the interaction with third parties.

Secure lifecycle process for smart grid components/systems and operating procedures

- Measures to promote the secure installation, configuration, operation, maintenance and disposition of smart grid components and systems.

Personnel security, awareness and training

- Measures related to the training of employees to improved reliability of operations in smart grids.

Incident response & information exchange

- Measures to provide an effective response in case of disruptions or incidents.

Audit and accountability

- Implementation of an audit and accountability policy and controls to check compliance with legal requirements and organization policies.

Continuity of operations

- Measures to ensure the basic funtions of a smart grid under different circumstances.

Physical security

- Measures for the physical protection of smart grid assets.

Information systems security

- Measures to protect information managed by smart grid information systems (e.g., firewalls, antivirus, intrusion detction, etc).

Network security

- Measures to protect the communication channels among the smart grid information systems and between business and industrial networks.

Resilient and robust design of critical core functionalities and infrastructures

- Defines core functionalities from the network and supporting infrastrcutures for their resilient operation.

Situational Awareness

- Defines main principles for stakeholders to be aware of their cybersecurity situation.

Liability

- Defines main principles for stakeholders to follow in case of privacy or cybersecurity breach.

Figure 6: European set of recommendations domains.

This set of recommendations is to be reviewed yearly, to make sure it is adapted to the upcoming developments in the sector, as both security measures and forms of attacks are constantly evolving over time.

4.4.3 SGIS Framework

The SGIS report proposes an improvement to the former SGIS Toolbox, so it is more focused on the necessity to perform risk analysis. It evaluates this necessity by enable the answer to the following questions: "What is the goal of a risk analysis? Who will use the results? Security measures were chosen during the risk analysis?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

What was the motivation behind the choice of these security measures and why did the risk analyst choose these specific security measures?"

Based on these questions, the framework defines the following steps:

- Preliminary Assessment (Define scope; Data Protection Impact Assessment (DPIA) if personal data is used),
- SGAM Mapping (Use case mapping in SGAM),
- Threats Mapping (Identify and analyse threats, risks and vulnerabilities),
- Define a Risk Mitigation Plan (Identify mitigating measures and link these to the risks),
- Define Traceability (why a specific security measure is chosen to mitigate a defined risk),
- Define a Mitigation Plan (compare incident costs to budget and costs of mitigation measures),
- Define an Action Plan (Actions to be taken; Classify based on priority and budget).

4.5 NISTIR 7628 Guidelines for Smart Grid Cybersecurity

The cybersecurity requirements of each organization should evolve as technology advances and as threats to grid security inevitably multiply and diversify. NISTIR 7628 [14] provides an analytical framework that stakeholders can use to develop effective Smart Grid related characteristics, risks and vulnerabilities. NISTIR 7628 outlines the security standards and best practices for the electric power grid to ensure its safe and reliable operation. In that sense, it provides cybersecurity requirements and recommendations for the smart grid components, systems and communication network. Incident response and resilience, as well as threat analysis and cybersecurity testing and evaluation are also within the scope of NISTIR 7628.

4.5.1 Guiding principles and objectives

The main concerns of NISTIR 7628 are to provide a comprehensive framework for securing the electricity network from cyber threats, by addressing the points shown in Figure 7.

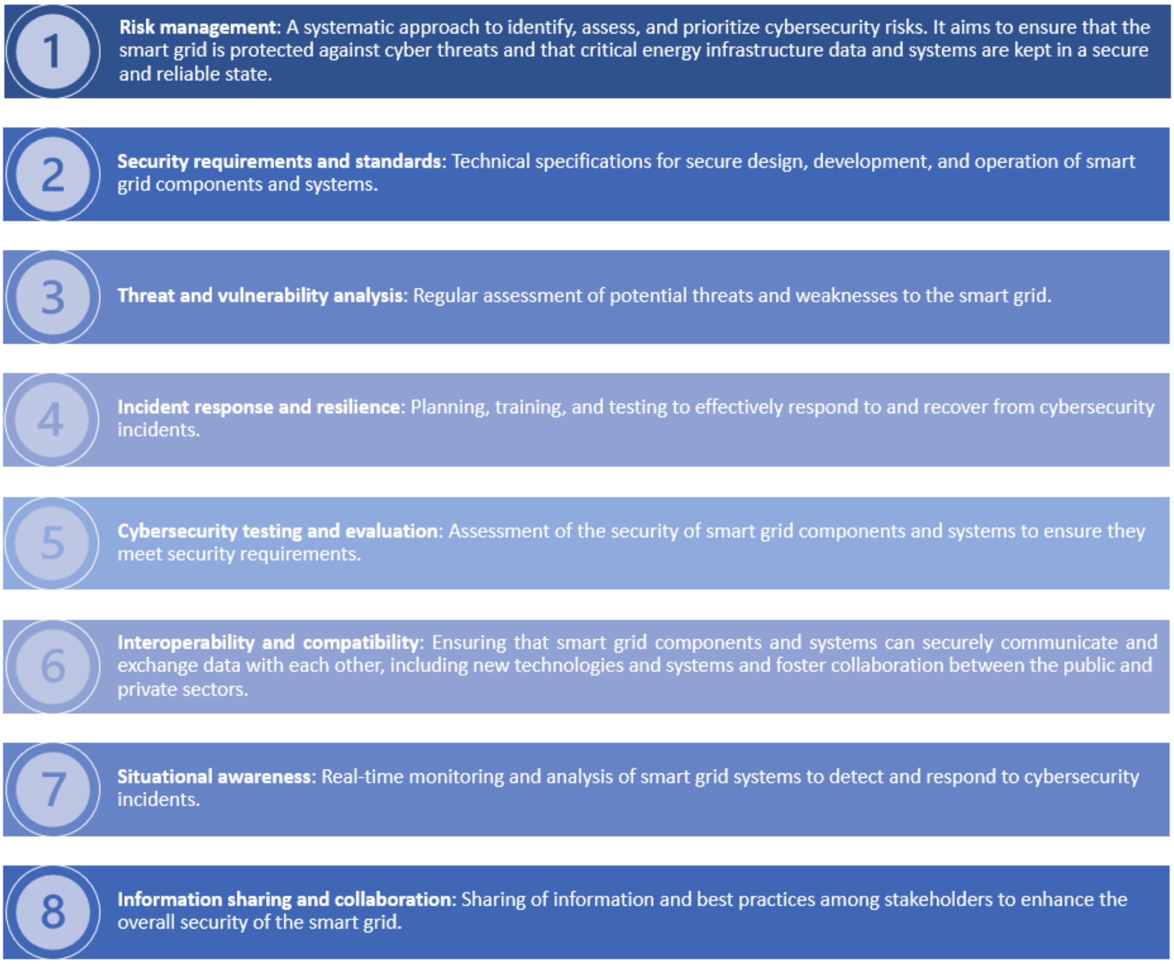
Upon the framework presented in Figure 7, the three main cybersecurity goals are to ensure **availability** for power system reliability, such as taking a few seconds for substation and feeder SCADA data; **integrity** for power system operations, by assuring that data is not modified without authorization and the source of data is authentical and **confidentialit**y, which is becoming more important with the increasing availability of customer's information online.

NISTIR 7628 divides the main stakeholders of the smart grid into seven domains: Generation, Transmission, Distribution, Markets, Operations, Service Providers and Costumers and analyses their respective interactions. The interactions between the different components of the different domains constitute logical interfaces with classifications about the priorities (High, Moderate or Low) regarding Confidentiality, and Availability, Integrity and Confidentiality.

These security requirements and standards are designed to protect the smart grid from cyber threats and to ensure its safe and reliable operation.

Some of the most important security requirements consist of operating the power system continuously 24/7 with high availability regardless of any compromise in security or the implementation of security measures that hinder normal or emergency power system operations. This must be kept during any security attack or compromise and must recover quickly after a security attack or the compromise of an information system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



1 **Risk management**: A systematic approach to identify, assess, and prioritize cybersecurity risks. It aims to ensure that the smart grid is protected against cyber threats and that critical energy infrastructure data and systems are kept in a secure and reliable state.

2 **Security requirements and standards**: Technical specifications for secure design, development, and operation of smart grid components and systems.

3 **Threat and vulnerability analysis**: Regular assessment of potential threats and weaknesses to the smart grid.

4 **Incident response and resilience**: Planning, training, and testing to effectively respond to and recover from cybersecurity incidents.

5 **Cybersecurity testing and evaluation**: Assessment of the security of smart grid components and systems to ensure they meet security requirements.

6 **Interoperability and compatibility**: Ensuring that smart grid components and systems can securely communicate and exchange data with each other, including new technologies and systems and foster collaboration between the public and private sectors.

7 **Situational awareness**: Real-time monitoring and analysis of smart grid systems to detect and respond to cybersecurity incidents.

8 **Information sharing and collaboration:** Sharing of information and best practices among stakeholders to enhance the overall security of the smart grid.

Figure 7: Framework for securing the electricity network from cyber threats.

The **Impact Level Allocation** identifies the security requirement and requirement enhancements at each impact level. The impact levels for a specific smart grid information system will be determined by the organization in the risk assessment process, as follows:

- Selecting the appropriate security requirements, including GRCs (Governance, risk and compliance).
- Identifying aspects of the selected security requirements that would need modifications or clarifications to apply to the smart grid information system.
- Identifying security policy issues in the GRCs to ensure they are covered in the appropriate security policies in the organization.

There is a general agreement in the cryptographic community that openly published and time-tested cryptographic algorithms and protocols are less likely to contain security flaws than those developed in secrecy, because their publication enables scrutiny by the entire community. The general concerns are that these additional techniques have not received a level of scrutiny and analysis commensurate with the standards development process of FIPS and recommendation practices of NIST. In that sense, well-understood, mature methods that have been extensively peer-reviewed by a community of cryptographers and an open standards process should be preferred over cryptographic compositions or protocols that are based on proprietary and closed development shall be preferred.

If a cryptographic algorithm implementation may not be upgradeable, due to costs, it is prudent to ensure that adequate planning is in place to treat affected devices/systems as less trusted in the infrastructure and, for

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

example, use enhanced network segmentation, monitoring, and containment (upon possible intrusion or tampering detection).

Data collection shall be limited to only the necessary for smart grid operations, including planning and management, improving energy use and efficiency, account management, and billing. Such data must be obtained by lawful and fair means and, when appropriate and possible, with the knowledge or consent of the customer. It is also highly recommended to de-identify information. Energy data and any resulting information, such as monthly charges for service, collected because of smart grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure that energy data from specific consumer locations is limited appropriately.

Smart grid equipment is designed to have an average of 20 years lifetime, which is longer than for typical IT and communication systems. Subsequently, a smart grid might be seen as a long-term and expensive resource that must be built future proof. It needs to be designed and built to adapt to changing needs, regarding scale and functionality and, at the same time, to tolerate and survive malicious attacks of the future.

4.6 ENISA

4.6.1 Supporting regulatory framework and process

ENISA (European Network and Information Security Agency) was established in 2004, with the aim to improve cybersecurity in the EU. The agency was established in response to the growing need for a coordinated EU-wide approach to address the increasing threat of cyber-attacks and to enhance the security of digital networks and systems. The establishment of ENISA aimed to help ensuring the protection of citizens, businesses, and governments from cyber threats and to contribute to the development of a secure and trustworthy digital society in the EU. Several reports have been released sharing information about the main concerns and good practices regarding cybersecurity in the energy sector (European Network and Information Security Agency., 2016; Marinos, 2022; Stergiopoulos et al., 2020) [15].

Electricity grids access all critical infrastructures**.** A smart grid offers great technical functionalities, but, thanks to the interconnected systems, can create vulnerabilities on the industrial sector. Cybersecurity refers to "the safeguards" and actions that can be used to protect the cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure" and it "strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein"

SCADA networks, which are being connected with traditional corporate IT systems to boost data visibility across operational and corporate IT assets, are widely used in the production, transmission and distribution of electricity. In major corporate IT systems and data centres, the energy supply and power exchange platforms process sensitive customer data, as well as crucial financial data. Therefore, all parts of the power subsector should be considered potential priority targets for cybercriminals and should be safeguarded as such. As such, the energy sector needs to increase the current maturity level on the management of cyber security [16].

4.6.2 Guiding principles and objectives

ENISA reports were developed to provide expert advice and support Member States on cybersecurity issues, by developing best-practices and standards and raising awareness on potential cybersecurity risks. This organization supports incident response and crisis management and conducts research and analysis on cybersecurity trends and threats.

In order to establish and promote European and international standards for risk management and the quantifiable security of electronic products, systems, networks, and services — which, along with software, make up the network and information systems — ENISA aims to support cooperation between stakeholders at the Union level.

The proposed standards aim to share knowledge and build consensus among technical experts nominated by interested parties and other stakeholders. Naturally, there is competition between the different players, but they also cooperate in many instances, in particular when there is a common interest. Although standards are voluntary, laws and regulations may refer to them and even make compliance with their obligatoriness.

Within the electricity subsector, ENISA encourages DSOs to perform risk management, by implementing structured and systematic approach to identifying, assessing and managing cybersecurity risks. It also recommends promoting a positive security culture among employees and stakeholders to enhance and manage cybersecurity risks. Manage the network's assets, to maintain an accurate inventory of assets including information and communication technology systems, to ensure that they are properly protected and secured. DSOs should implement appropriate access controls to make sure that only authorized personnel have access to sensitive information and systems. It is also of extreme importance for DSOs to have a well-defined and tested incident response plan in place to ensure that they are prepared to respond effectively to cybersecurity incidents. DSOs are also advised to perform monitoring and detection of systems continuously to identify and respond to cybersecurity incidents in a timely manner.

4.6.3 Guidelines for the electricity sector

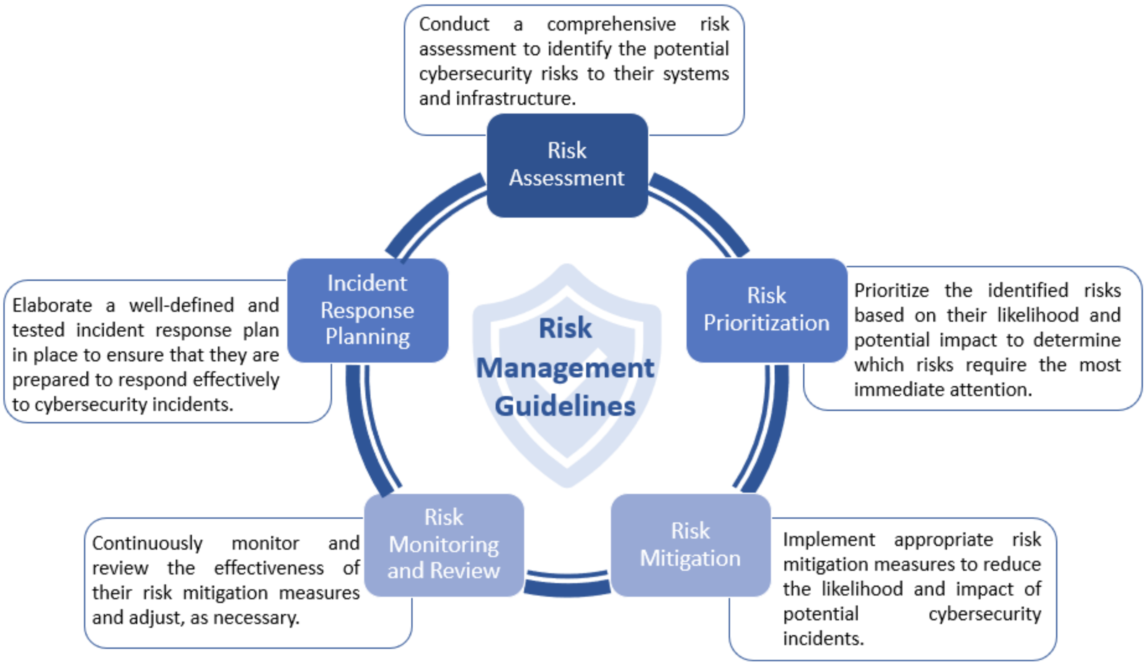

Conduct a comprehensive risk assessment to identify the potential cybersecurity risks to their systems and infrastructure.
Risk Assessment
Incident Response Planning
Elaborate a well-defined and tested incident response plan in place to ensure that they are prepared to respond effectively to cybersecurity incidents.
Risk Management Guidelines
Risk Prioritization
Prioritize the identified risks based on their likelihood and potential impact to determine which risks require the most immediate attention.
Risk Monitoring and Review
Continuously monitor and review the effectiveness of their risk mitigation measures and adjust, as necessary.
Risk Mitigation
Implement appropriate risk mitigation measures to reduce the likelihood and impact of potential cybersecurity incidents.

Figure 8: ENISA's risk management guidelines for the electricity subsector.

ENISA provides several good practices for DSOs to improve their cybersecurity posture, by performing a risk management, establishment of a security culture among employees and stockholders, appropriate asset controls and incident response. Figure 8 depicts risk management guidelines for the electricity sector, provided by ENISA. These guidelines aim to support DSOs in ensuring the security and resilience of their systems and infrastructure against cybersecurity threats and attacks.

Most widely known measures relevant to network security also apply to IT networks in power grids. Also, it should be noted that, apart from the scenario specific measures, common organizational security measures, such as security governance models, security policies and procedures, standards and certifications, training and **awareness-raising, risk management**, audits and assessments and contractual clauses, also apply to the power sector.

Technical measures include, among others, device and configuration management, network monitoring, patching and updating, network segmentation and authentication, and network security.

The energy sector needs to increase the current maturity level regarding the management of cybersecurity. In that sense, several stakeholders made a comparison with the financial sector, which has developed a considerably high level of maturity of cybersecurity, which is an example for management of cyber risks and sharing of cyber security incidents. This low maturity of the energy sector is explained by historical reasons, where physical security and safety threats have always been considered above all other threats by the sector. As the energy sector is experiencing a digital transformation, with the processing of digital data to monitor and process the critical infrastructure, safety and security, the sector needs to target high maturity levels on cyber threat management. Cybersecurity should be seen as one important component of the "multifaceted challenge" [17] of the energy security.

5 Related projects

Several projects within the H2020 programme are addressing cybersecurity issues in various aspects in the energy sector.

5.1 EnergySHIELD

The Electrical Power and Energy System (EPES) is of key importance to Europe's economy, as all other domains rely on the availability of electricity. A power outage can directly impact the availability of other services such as transport, finance, communication and water supply. Digital solutions have become essential to keeping the light on and the energy grid humming, but there is an increased risk of cyberattacks. As such, addressing cybersecurity is necessary. The EU-funded EnergySHIELD[1] project will attempt to develop an integrated toolkit that combines the latest technologies for vulnerability assessment, monitoring and protection, as well as learning and sharing. It will be tailored to meet the needs of EPES operators.

5.2 FORESIGHT

The effective management of cyber threats requires a set of proactive tools and the development of an entire security culture. The EU-funded FORESIGHT[2] project aims to develop a federated cyber range solution to enhance the preparedness of cybersecurity professionals at all levels and advance their skills towards preventing, detecting, reacting to and mitigating sophisticated cyber-attacks. Through an ecosystem of networked realistic training and simulation platforms, the project will extend the capabilities of existing cyber ranges and allow complex cross-domain/hybrid scenarios to be built jointly with the IoT domain.

5.3 CyberSANE

Europe's critical information infrastructure (CII) are those interconnected information and communication infrastructures essential for the maintenance of vital societal functions (health, safety, security, economic or social well-being of people). Any disruption or destruction would have serious consequences. In today's digital era, the increased usage of information technology in modern CIIs makes them vulnerable to cyber-related crime. The EU-funded CyberSANE[3] project will enhance their security and resilience by providing a dynamic collaborative warning and response system. This will support and guide security officers to recognize, identify, dynamically analyse, forecast, treat and respond to advanced persistent threats and handle their daily cyber incidents utilizing and combining both structured data and unstructured data coming from social networks and the dark web.

5.4 PHOENIX

PHOENIX[4] will realize 3 strategic goals:

(1) Strengthen EPES cybersecurity preparedness by employing security a) "by design" via novel protective concepts for resilience, survivability, self-healing and accountability, and b) "by innovation" via adapting,

[1] https://energy-shield.eu/
[2] https://foresight-h2020.eu/
[3] https://www.cybersane-project.eu/
[4] https://phoenix-h2020.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

upgrading and integrating a number of TRL5 developments to TRL7-8 and validating them in real-live large-scale pilots;

(2) Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level, a novel fully decentralized inter-DLTs/blockchain based near real-time synchronized cybersecurity information awareness platform, among authorized EPES stakeholders, utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group;

(3) Accelerate research and innovation in EPES cybersecurity by privacy preserving a novel deploy, monitor, detect and mitigate DevSecOps mechanism, a secure gateway, federated Machine Learning algorithms and establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.

5.5 CyberSEAS

The move towards more agile, connected, intelligent and data-driven energy systems, and their interconnection with our day-to-day lives, means that there is a major increase in cyber exposure of energy systems leading to major safety and privacy incidents. The EU-funded CyberSEAS[5] project improves the resilience of energy supply chains by protecting them from disruptions generated by complex attack scenarios. CyberSEAS delivers an open and extendable ecosystem of 30 customizable security solutions providing effective support for key activities, such as risk assessment; interaction with end devices; secure development and deployment; real-time security monitoring; skills improvement and awareness; and certification, governance and cooperation. CyberSEAS solutions will be validated through experimental campaigns consisting of numerous attack scenarios.

5.6 SDN

The smart energy ecosystem is the next step of the conventional electrical grid, offering increased reliability, augmented service quality and efficient exploitation of existing infrastructures. However, it generates significant security and privacy problems as it contains a combination of heterogeneous, coexisting smart and legacy technologies. The EU-funded SDN-microSENSE[6] project will provide secure, privacy-enabled and resistant-to-cyberattacks tools to ensure electrical power and energy system (EPES) operation and the integrity and confidentiality of communications. The project will adopt an SDN-based technology and implement risk assessment processes to identify the risk level of each EPES component, self-healing abilities to isolate the critical parts of the network, large-scale detection tools, prevention mechanisms and a privacy protection structure.

[5] https://cyberseas.eu/

[6] https://www.sdnmicrosense.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

6 Cybersecurity Survey

6.1 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a policy framework for assessing and improving the capabilities of private sector businesses in the United States to prevent, detect, and respond to cyber threats. It has been utilized by hundreds of organizations since its publication in 2014, providing a common vocabulary and framework for debating and improving security.

In the context of T4.4 Requirement analysis of cyber security measures for grid operators and customer integration, UBE has prepared a survey (Table 4) starting from NIST standard alongside [18] a maturity level, in order to assess the security maturity level of the grid operators participating in OneNet Consortium.

Table 3 Security maturity level matrix.

#LEVEL	DEFINITION	PROCEDURE	STANDARD	COMPLIANCE	UPDATES
INITIAL	■				
BASIC	■	■			
DEFINED	■	■	■		
MANAGED	■	■	■	■	
OPTIMISED	■	■	■	■	■

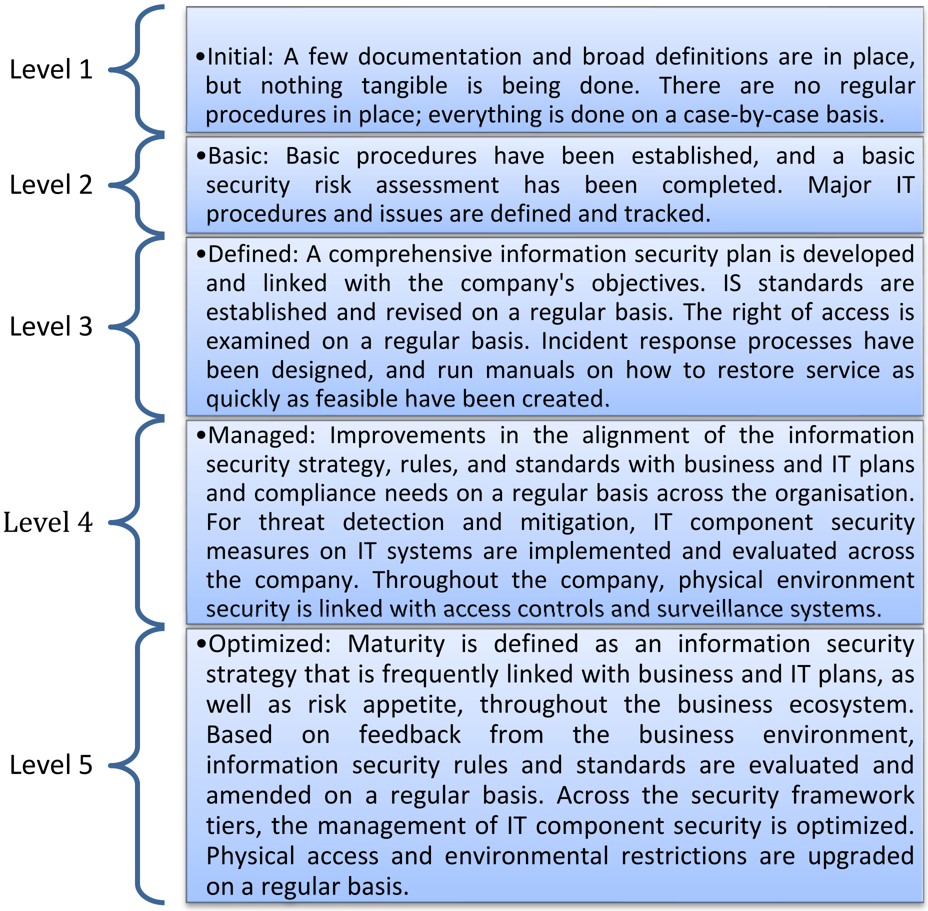
The following are the **criteria** that determine where the line between different stages of maturity is drawn:

- **Definition.** There is some understanding of cyber security inside the firm,
- **Procedure.** Cyber-security processes have been defined,
- **Standard.** Specific policies and standards are implemented,
- **Compliance.** Procedures are used to ensure that specified requirements are met,
- **Updates.** The security strategy is in line with the company's goals, and standards and rules are updated on a regular basis.

Five maturity levels defined but only 4 possible answers. This is because "level 5" is a security level very hard to achieve and maintain.

Maturity, as shown in Table 3, refers to an information security strategy that is frequently linked with business and IT plans, as well as risk appetite, throughout the business ecosystem. Based on feedback from the business environment, information security rules and standards are evaluated and amended on a regular basis. Across the security framework tiers, the management of IT component security is optimized. Physical access and environmental restrictions are upgraded on a regular basis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Level 1

•Initial: A few documentation and broad definitions are in place, but nothing tangible is being done. There are no regular procedures in place; everything is done on a case-by-case basis.

Level 2

•Basic: Basic procedures have been established, and a basic security risk assessment has been completed. Major IT procedures and issues are defined and tracked.

Level 3

•Defined: A comprehensive information security plan is developed and linked with the company's objectives. IS standards are established and revised on a regular basis. The right of access is examined on a regular basis. Incident response processes have been designed, and run manuals on how to restore service as quickly as feasible have been created.

Level 4

•Managed: Improvements in the alignment of the information security strategy, rules, and standards with business and IT plans and compliance needs on a regular basis across the organisation. For threat detection and mitigation, IT component security measures on IT systems are implemented and evaluated across the company. Throughout the company, physical environment security is linked with access controls and surveillance systems.

Level 5

•Optimized: Maturity is defined as an information security strategy that is frequently linked with business and IT plans, as well as risk appetite, throughout the business ecosystem. Based on feedback from the business environment, information security rules and standards are evaluated and amended on a regular basis. Across the security framework tiers, the management of IT component security is optimized. Physical access and environmental restrictions are upgraded on a regular basis.

Figure 9: Cybersecurity maturity levels.

To determine the security maturity level of the OneNet system platform users, a survey has been contacted based on NIST requirements [19]. As presented in Table 4, the questions revolve around five topics: governance, technical, data, risk and compliance.

- **Governance** ensures that security initiatives are aligned with the company's goals and legislation,
- **Technical** (Architecture, Infrastructure) acknowledges the architecture's assets as well as its infrastructure,
- **Data** (Information processing) protection from unauthorized or unintentional destruction, alteration, or disclosure,
- **Risk Management** examines the dangers that come with using information technology,
- **Compliance** refers to security in practice: standards and regulations that are available.

Questions with four prepared answers have been created for each topic. The stages of maturity are represented by the replies, which are graded from 1 to 4. Level 5 has no alternatives since it is extremely tough to acquire and maintain.

Table 4 Cybersecurity Survey raw text.

Security Level Assessment			
Governance	**1. Information security governance Strategy and Metrics**		**Maturity Level**
	a) Information Security Strategy and policies.	Informal Procedures. Ad hoc definition of an information security strategy. No budget.	1,00
		Processes for managing the security of data throughout its life cycle are emerging. Major security incidents are tracked and recorded. The security risk management is present but ad-hock without a clear process	2,00
		Information security policies and standards are developed and revised based on a defined process and regular feedback. Budget allocated. The security risk-management process is proactive.	3,00
		Security measures on IT systems are implemented and tested enterprise-wide for threat detection and mitigation. Physical environment security is integrated with access controls and surveillance systems across the enterprise. Detailed security budget requirements are incorporated into enterprise-wide business planning and budgeting activities. Cyber Security KPIs are regularly presented to the board of directors	4,00
	b) Strategic alignment of security	There are some discussions about the importance of cyber security	1,00
		Security objectives are mentioned in global objectives, but NO precise responsibilities.	2,00
		Security objectives are mentioned in global objectives with precise responsibilities.	3,00
		Audit procedures are defined to tests if security objectives were fulfilled. Cyber security KPIs are measured and tracked. Cyber incidents are systematically addressed enterprise-wide.	4,00
	c) Communication and Awareness	No awareness training for security objectives. Few communication rules circulated.	1,00
		No awareness training for security objectives. Communication rules defined.	2,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		Awareness training for security is organized at least once a year. Precise communication rules and procedures are established.	3,00
		Awareness training for security is organized at least once a year. Continues improvement for communication rules is present.	4,00
	d) People Roles and responsibilities	No special roles and responsibilities are defined. Security responsibilities are defined as part of other responsibilities.	1,00
		Responsibilities for security are defined as part of the definition of all roles.	2,00
		Security roles and responsibilities are defined and described.	3,00
		Security roles and responsibilities are defined and described. Audit organized for security roles and responsibilities regularly.	4,00
	e) Security performance assessment	No security performance controls are planned. Ad-hoc security assessments performed.	1,00
		Process for security control defined, but NO controls planned.	2,00
		Process for security control defined, at least two assessment controls planned for a year.	3,00
		Results of security controls used when assessing the performance of the company.	4,00
	f) Assessment of security budget and investments	No budget is specially allocated. If necessary, the budget is allocated for specific situations on a case-by-case basis.	1,00
		There is some consideration of security budget requirements within IT.	2,00
		IT budget processes acknowledge and provide for the most important information security budget requests in IT and some other business units.	3,00
		Security budget is provided yearly as a percentage of the IT budget of the organization. There is an audit for budget usage for security measures.	4,00
Technical	**2. Technical Asset Security Management**		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	a) Security architecture	The architecture of the system does not include a security perspective and is not built based on security standards and best practices. Some components describe security requirements.	1,00
		The architecture of the system contains a security perspective and is partly built based on security standards and best practices. Some components have separate security requirements.	2,00
		The architecture of the system contains a full documented security perspective, with specifications for each component, and is built based on security standards and best practices inc.	3,00
		The architecture of the system contains a full documented security perspective it is built based on security standards and best practices, and it is regularly checked with auditing tools.	4,00
	b) IT component security	Some component types have a security perspective defined.	1,00
		All component types have a security perspective defined and documented.	2,00
		All component types have a security perspective aligned with best practices and international standards for secure components.	3,00
		All components are checked on a regular basis for security compromises and issues. There is evidence of security requirements for all components.	4,00
	c) Physical infrastructure security	There are ad-hoc rules for physical access to the security infrastructure.	1,00
		Access to the security infrastructure is limited based on user roles and need to know.	2,00
		Access to the security infrastructure is defined in security procedures based on cyber security standards and best practices.	3,00
		There is permanent monitoring of the access to the security infrastructure.	4,00
	d) Please identify & describe potential legacy systems still in use		
Data	**3. Information Service/System/Data Security Management**		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	a) Incident Management	Incidents are managed ad-hoc based on the judgment of the employees of the organization.	1,00
		There is a tool used for incident management, where incidents are registered and tracked.	2,00
		There is a tool and well-defined procedures for incident management.	3,00
		There is a tool and well-defined procedures for incident management and results from the incidents are evaluated on a regular basis. The outcome of the evaluation is used for incident management process improvement	4,00
	b) Resource effectiveness	All incidents are treated in the same way.	1,00
		Incidents are treated based on the security level of the incident.	2,00
		Incidents are treated based on their severity level. Different roles are treating different severities.	3,00
		Incidents are treated based on their severity level. Different roles are treating different severities. KPIs are used to evaluate the effectiveness of the resources and enhance the performance.	4,00
	c) Data Identification and Classification	Access to systems is based on username and password, default username and passwords are not changed there is no password policy	1,00
		There is a domain where users are registered and have roles (LDAP-based). Access to components is based on the roles defined in the domain.	2,00
		There is a special Identity and Access Management system (IAM) defined for components. There is a single-sign-on system.	3,00
		The access to the systems is monitored and audited regularly. User access rights are being audited yearly.	4,00
	d) Access Management	Users are added or deleted to/from the system when necessary. No other steps and checks are performed.	1,00
		There are specific procedures defined to add, delete, activate, and disable users based on their roles.	2,00
		There are mechanisms for delegating the roles.	3,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		There is a monitoring and audit system for access management. Users on the systems are audited regularly	4,00
	e) System Acquisition, Development, and Maintenance Security Policy Access Management	There are no special security rules for security acquisition. There are some rules for system development.	1,00
		System acquisition and system development follows security rules. No process defined for checking the security.	2,00
		System acquisition and system development follows security rules. Detailed process is defined for checking the security.	3,00
		System acquisition or development is approved only after security checks.	4,00
Risk	**4. Vulnerability and Risk Management**		
	a) Security Threat profiling	There is no organized threat profiling.	1,00
		Vulnerabilities are known and documented as part of individual components documentation	2,00
		Vulnerabilities are documented for individual components and the whole system	3,00
		Proactive vulnerabilities assessment of the systems and components is conducted and documented.	4,00
	b) Security Risk Assessment	Risks assessments are ad hock. No define process for regular risk assessments.	1,00
		Risks are documented on a system level.	2,00
		Risks are documented the whole system and for each component of the system.	3,00
		There is a Risk Register updated regularly based on the company process.	4,00
	c) Security Risk Prioritization	There is no prioritization of risks.	1,00
		Risks are prioritized based on likelihood and potential impact.	2,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		There are procedures used to define the priority of risks that are based on best practices and international standards.	3,00
		There is a Risk Register is updated regularly based on the company process.	4,00
	d) Security Monitoring	Incidents are mentioned in regular reports.	1,00
		There is a tool (register) used to register the security incidents.	2,00
		There are defined procedures for monitor and following the resolution of security incidents.	3,00
		There is a monitoring mechanism that measures the unavailability of the system due to security issues.	4,00
Compliance	**5. Information Security Governance Control/Compliance/Continuity Management**		
	a) Compliance Control	Ad-hoc compliance control.	1,00
		Compliance with GDPR, NIS performed.	2,00
		Compliance control is defined in procedures, and budgeted is allocated for the implementation of controls needed for compliance.	3,00
		Compliance control is monitored and periodically reported to the regulatory body if needed.	4,00
	b) Security Testing and Auditing	Security tests organized ad-hoc.	1,00
		Security tests are performed for each new component or each new configuration change without a clear process or steps that should be performed.	2,00
		Security tests are performed based on processes and procedures based on international standards and best practices.	3,00
		Security tests are performed based on processes and procedures based on international standards and best practices and audits of the whole system for security problems are performed regularly.	4,00
	c) Business continuity planning	There is no clear Business continuity plan. Business continuity is considered only when an incident occurs.	1,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		There is a business continuity plan in case of security issues.	2,00
		There is a business continuity plan in case of a security issue that is being tested regularly.	3,00
		There is a business continuity plan in case of a security issue that is being tested regularly. KPIs are used to evaluate the tests and are used for the improvement of the plan. Proactive actions are performed for business continuity.	4,00
Additional Questions			
	Procurement contract language cybersecurity requirements for IT and OT assets	No cyber security language is included in asset procurement	1,00
		Some cyber security language is included in asset procurement, but it is done ad-hock and there is no policy and procedure	2,00
		Security language is included in the asset procurement process	3,00
		Security language is included in the asset procurement process and cyber security is of the main consideration in the decision-making process for the procurement of assets	4,00
	Cyber Security Training for key employees	No specialized cyber security training is provided.	1,00
		Specialized cyber security training is provided to some of the IT engineers.	2,00
		Specialized cyber security training is provided to all the It engineers and there is a cyber security group in the organization.	3,00
		Cyber Security is an integral part of the DNA of the organization. Yearly cyber security training is mandatory for the IT, Cyber Security team, and all key employees.	4,00
	Priority to systems is assigned when implementing new cybersecurity measures	Prioritization is not available	1,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

		Cyber security measures are implemented depending on the importance of the systems ad-hock	2,00
		Process and procedure are available for asset prioritization. Cyber security measures are implemented depending on the priority of the system	3,00
		Process and procedure are available for asset prioritization. Cyber security controls are implemented based on the priority of the system and a cost-based analysis of all available controls	4,00
	Cyber Security information is shared with industry partners	No, we don't collect cyber security information	1,00
		Cyber Security information is collected but not shared	2,00
		Cyber Security information is collected and shared with industry partners rarely.	3,00
		Cyber Security information is shared in sector-specific information sharing and analysis centers (ISAC)	4,00
	The organization has alternative locations ready should it be necessary to relocate operational control to ensure service delivery	No, we don't have a backup facility	1,00
		There is a cold site that is used for backup facility	2,00
		The organization has a hot site that is used for backup facility	3,00
		The organization mirrors all the system data to an alternative data facility, operations can continue without interruption if the primary location experience outage and the switch over is tested regularly.	4,00

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

6.2 Survey Results Analysis

Five relevant topics regulated by NIST: Governance, Technical, Data, Risk and Compliance and their characteristics (Information security governance Strategy and Metrics, Technical Asset Security Management, Information Service/System/Data Security Management, Vulnerability and Risk Management and Information Security Governance Control/Compliance/Continuity Management) were scored and rated to outline the average level of security maturity of the OneNet participants (Figure 10).

According to the findings of the security study, all practitioners have done the bare minimum of efforts to comply with applicable requirements. Figure 10 shows that on average all five proposed topics are above level 3. This means that comprehensive information security plan is developed, and incident response processes have been designed. Governance, technical and data topics have the highest values while compliance and risk aspects have lower values indicating that overall, the group of practitioners investigated display a reactive behaviour.

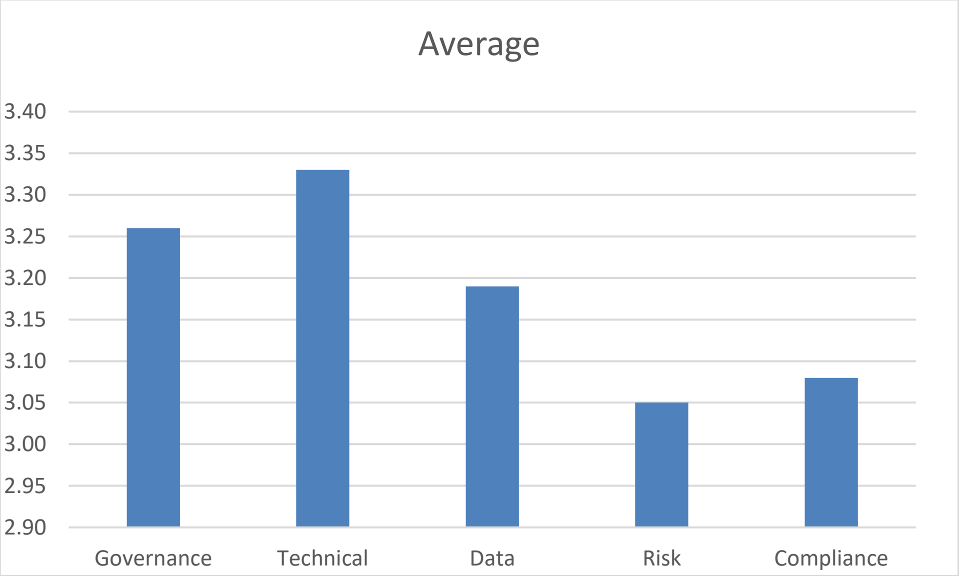
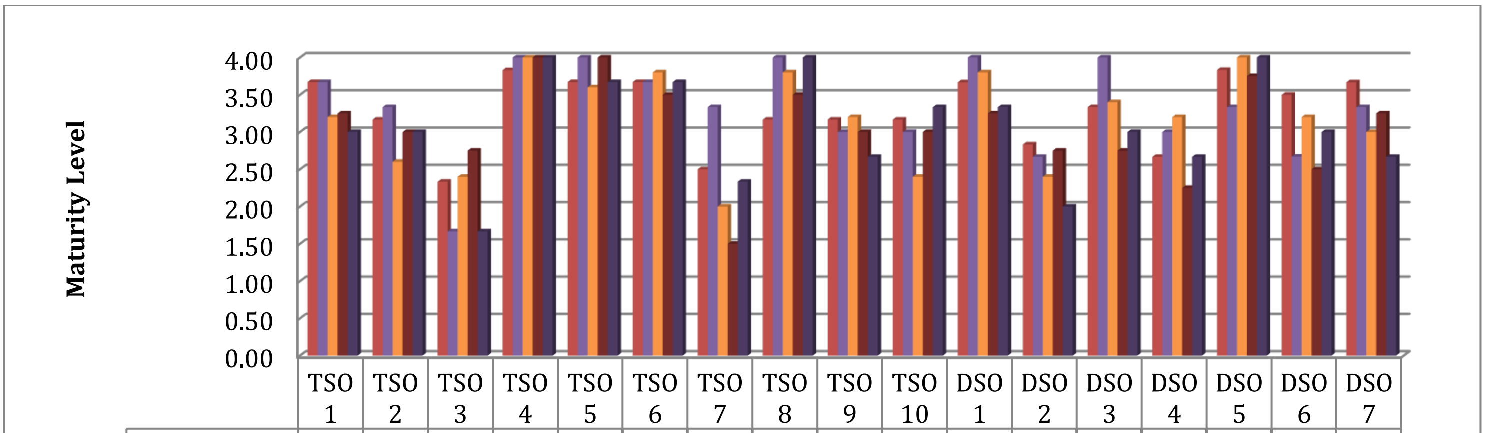


Figure 10 Average security level.

From the 31 TSO, DSO and market operators, 10 TSO and 7 DSO partners have participated in the survey. The low participation is due to the cybersecurity alert raised due to the situation in the east of Europe and those partners weren't allowed to transfer any information regarding cybersecurity.

When examining the data supplied by each participant, it is clear that big TSO and DSO partners have adopted security measures and adhere to applicable standards to a greater security level.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



	TSO 1	TSO 2	TSO 3	TSO 4	TSO 5	TSO 6	TSO 7	TSO 8	TSO 9	TSO 10	DSO 1	DSO 2	DSO 3	DSO 4	DSO 5	DSO 6	DSO 7
■ Governance	3.67	3.17	2.33	3.83	3.67	3.67	2.50	3.17	3.17	3.17	3.67	2.83	3.33	2.67	3.83	3.50	3.67
■ Technical	3.67	3.33	1.67	4.00	4.00	3.67	3.33	4.00	3.00	3.00	4.00	2.67	4.00	3.00	3.33	2.67	3.33
■ Data	3.20	2.60	2.40	4.00	3.60	3.80	2.00	3.80	3.20	2.40	3.80	2.40	3.40	3.20	4.00	3.20	3.00
■ Risk	3.25	3.00	2.75	4.00	4.00	3.50	1.50	3.50	3.00	3.00	3.25	2.75	2.75	2.25	3.75	2.50	3.25
■ Compliance	3.00	3.00	1.67	4.00	3.67	3.67	2.33	4.00	2.67	3.33	3.33	2.00	3.00	2.67	4.00	3.00	2.67

Figure 11: Maturity level of security.

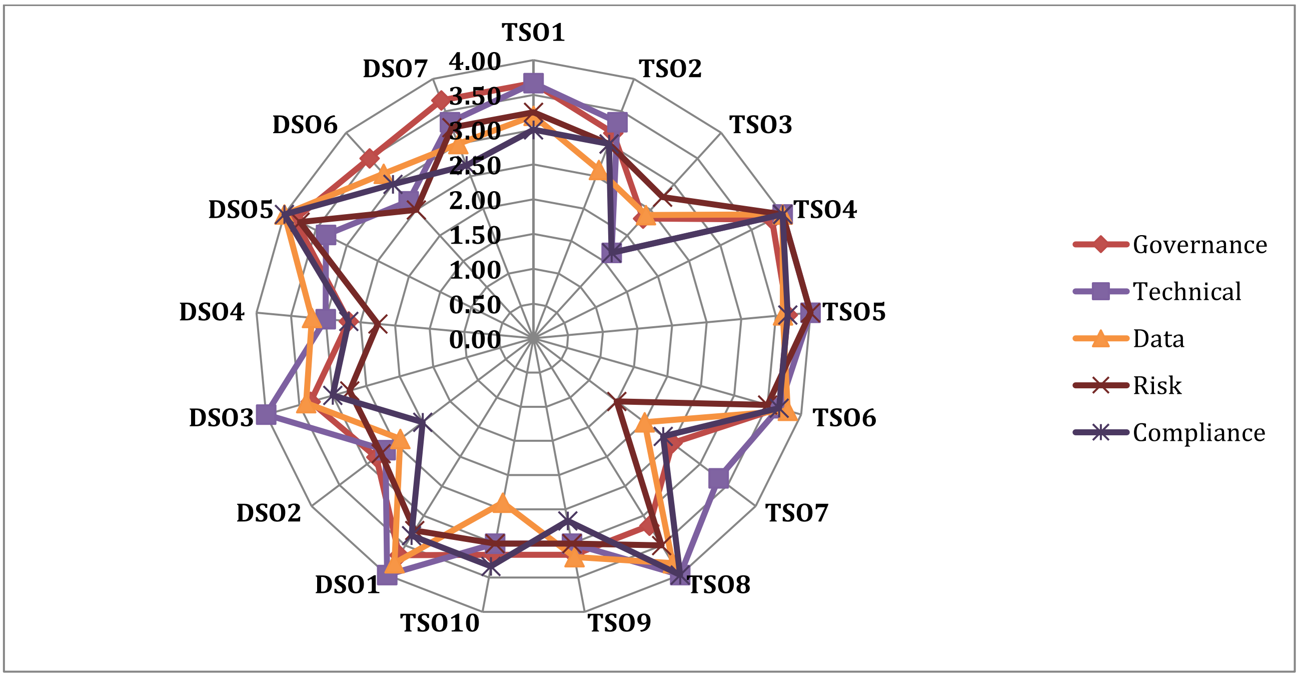


Figure 12: Spatial presentation of security maturity level.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

7 Cybersecurity requirements for Cross Stakeholder Data Governance

Cross-stakeholder data governance refers to a collaborative approach to managing and sharing data among multiple stakeholders, including organizations, government agencies, individuals, and other entities. The goal of cross-stakeholder data governance is to ensure that data is used and shared in a way that is ethical, secure, and in compliance with relevant regulations and standards.

In a cross-stakeholder data governance model, stakeholders collaborate together to define policies and procedures for data collection, use, and sharing. This can involve creating a data governance framework that outlines the roles and responsibilities of each stakeholder, as well as the processes and procedures for managing data across different organizations and systems.

The benefits of cross-stakeholder data governance include increased transparency, accountability, and trust among stakeholders, as well as improving data quality and security. Addressing the data governance in a clear and structured way, stakeholders can minimize the risks of data breaches, privacy violations, and other data-related issues, while also maximizing the value and potential of data for research, innovation, and other purposes.

Data Security and Cybersecurity are crucial aspects for cross-stakeholder data governance, since the protection of sensitive information is essential to maintain the trust and credibility of all stakeholders involved. The security impact of cross-stakeholder data governance can be significant, as it involves managing and sharing data across different organizations, systems, and jurisdictions.

To ensure the security of data in a cross-stakeholder data governance model, stakeholders must establish clear policies and procedures for data protection, access control, and incident response. This imply to implement encryption, authentication, and authorization mechanisms to ensure that data is only accessed and used by authorized parties. It may also involve implementing data masking or anonymization techniques to protect the privacy of individuals whose data is being shared.

In addition, stakeholders must monitor and assess the security of their data management practices and systems and consider prompt action to solve any security vulnerabilities or incidents that may arise. This requires a well-defined security commitment to ongoing security awareness training, risk management, and incident response planning.

Overall, the security impact of cross-stakeholder data governance cannot be overstated, as data breaches and other security incidents can have serious consequences for individuals, organizations, and society. As such, stakeholders must prioritize security in all aspects of their data management practices and work together to establish a strong, collaborative approach to data governance.

The International Data Spaces Association (IDSA) is an organization that is dedicated to promoting secure and trustworthy data sharing through a collaborative approach to data governance. The IDSA approach includes several aspects that are designed to address the security challenges associated with cross-stakeholder data governance.

More in details, the IDSA framework includes a set of security and privacy principles that are designed to ensure that data is protected and managed in a secure and trustworthy manner. These principles include [20]:

- Data sovereignty: ensuring that data is owned and controlled by the data provider.
- Interoperability: enabling secure and seamless data exchange across different systems and domains.

- Security and trustworthiness: ensuring that data is protected from unauthorized access, tampering, and other security threats.
- Privacy: ensuring that the privacy of individuals is protected, and that personal data is processed in compliance with relevant regulations and standards.

The IDSA also provides a set of technical specifications and guidelines for implementing secure data sharing solutions based on the principles outlined in the framework, within the IDS Reference Architecture Model (IDS RAM) [21]. These specifications cover various aspects of data management, including data access control, authentication, and encryption.

In addition, the IDSA promotes a collaborative approach to data governance that involves multiple stakeholders, including industry, academia, and government. This approach is designed to facilitate the sharing of best practices, knowledge, and resources across different domains and sectors, in order to maximize the benefits of data sharing while minimizing the risks.

Overall, the IDSA approach to data governance emphasizes the importance of security and trustworthiness in cross-stakeholder data sharing, and provides a set of principles, specifications, and guidelines that are designed to address these challenges.

The OneNet system is strongly based in the IDSA framework for the cross-stakeholder collaboration and data governance aspects, following the IDS RAM with a focus in data security, governance, and trust.

In particular, the data security and cybersecurity aspects are fundamental for the OneNet cross-stakeholder governance.

Data security refers to safeguarding data throughout its lifecycle. Data Security should implement the process for ensuring data is safe from cyber-attacks, unauthorized access, data breaches, and theft. It should also establish a clear plan of action to respond to all potential threats.

The OneNet system takes into high considerations both the data security (relating to the protection of data in terms of confidentiality, integrity and availability) and cybersecurity aspects (relating to the protection of the systems and networks infrastructure), although they overlap in many instances.

The OneNet Data Governance Framework, described in D6.2 [22] relies on 5 pillars and 10 building blocks that covering all the cross-stakeholder governance aspects. In particular, the Data Security building block, under the Data Access pillar, addresses the data security aspects expected in the cross-stakeholder governance.

Following the European Interoperability Framework [23], which recommends defining a common security and privacy framework (for cross-stakeholder data exchange), the OneNet System implements a specific cybersecurity layer for ensuring at any level to:

- Apply “know-your-data-user” principle by making data usage information available to data owners easily and free of charge.
- Harmonise authentication and authorization schemes across Europe and sector.

Figure 13 and Figure 14 show how the OneNet Cybersecurity layer intervenes both in the central communication with the OneNet system and at any data exchange between OneNet Participants, within the OneNet Connector (see D5.2 [24] for architectural details).

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

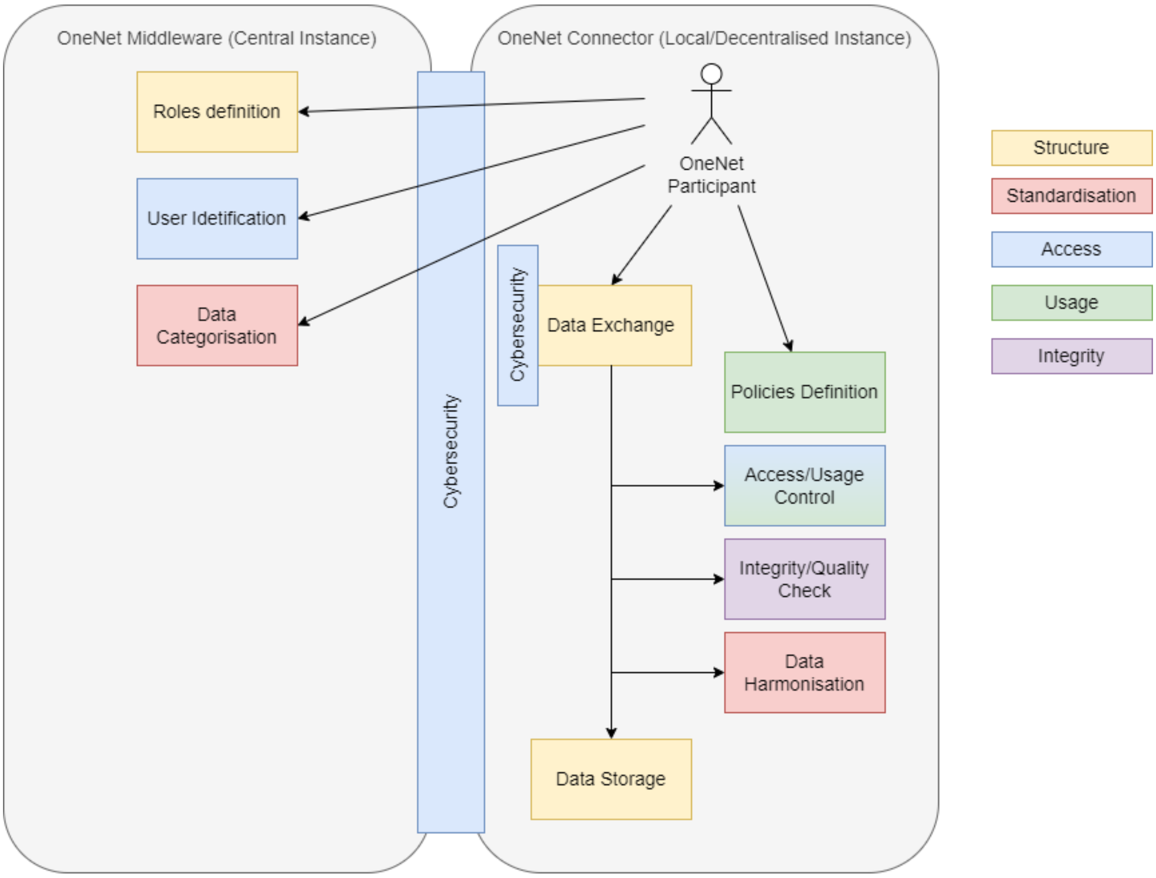


Figure 13: OneNet Cybersecurity layer - central communication.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

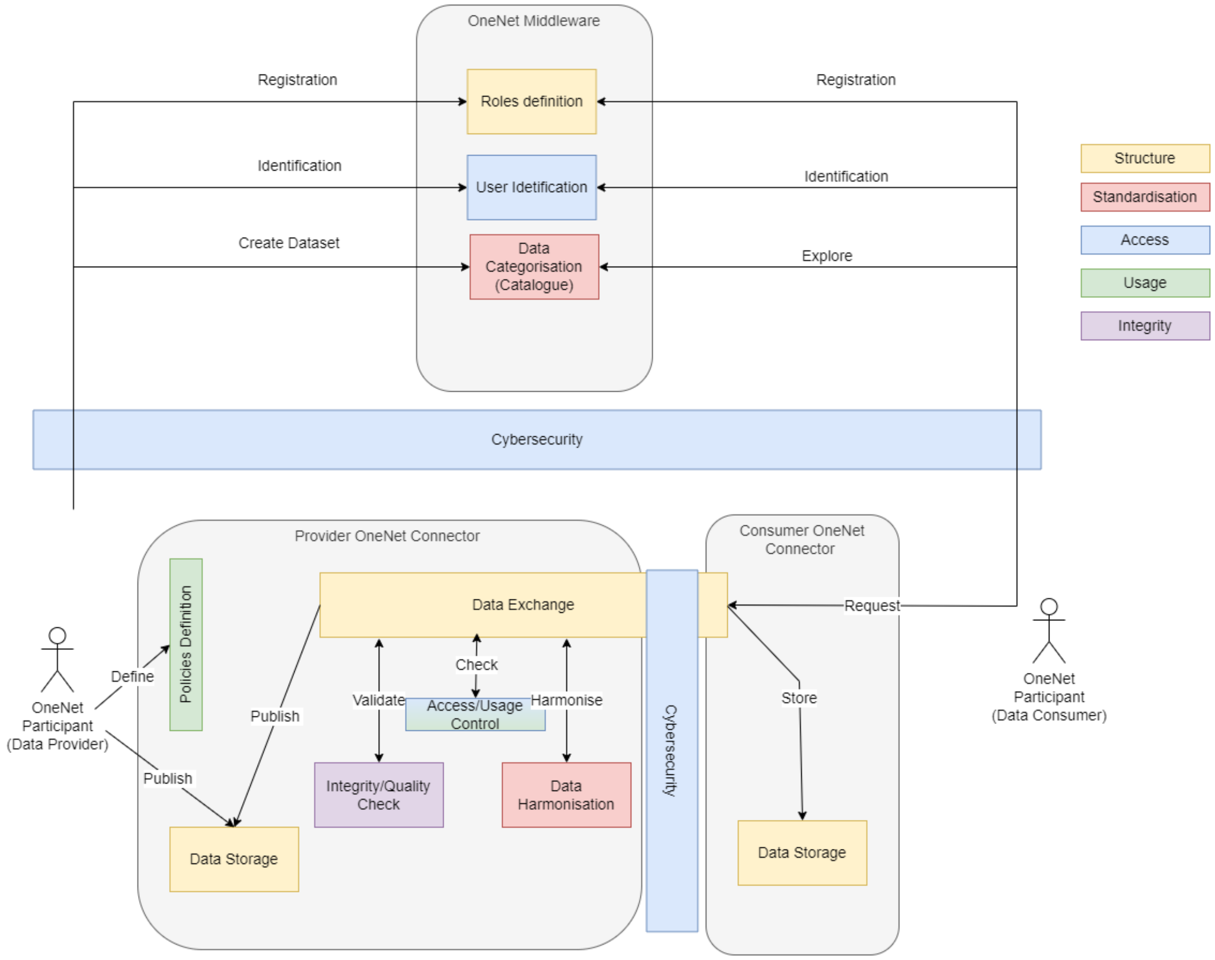


Figure 14: OneNet Cybersecurity layer - data exchange.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

8 Measures and Processes

This chapter presents key Network Security terms, operational scenarios and policy recommendations for grid operators. Based on the above, in conjunction with the D5.8 “Report on Cybersecurity, privacy and other business regulatory requirements” the OneNet cybersecurity proposed measures are identified are thoroughly presented.

8.1 Network Security Terms

1. Syslog

Computer systems use the Syslog protocol to send event data logs to a central location for storage. Logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT operational tasks.

2. Audit

A network audit is a formal or informal inventory, assessment, and analysis of your network’s hardware, software, operating systems, servers, and users. Network audits typically check:

- All network infrastructure and internet-accessible systems,
- The security mechanisms activated to protect the network,
- The practices used for day-to-day network management.

3. File Integrity Monitoring

File Integrity Monitoring (FIM) is a widely used security control mechanism in IT organizations. It examines the integrity of sensitive files, registry keys, and folders within the host operating system and checks whether files have been altered or compromised by tracking logs and comparing the current version to a known baseline. Companies can monitor file integrity by leveraging advanced file integrity monitoring (FIM) tools that help automatically track and alert IT admins to unauthorized modifications across critical files.

4. Security Configuration Assessment (SCA)

Security Configuration Assessment (SCA) is a lightweight cloud service which can perform the configuration assessment of IT assets, and track compliance centrally the status of IT assets on based on the Centre for Internet Security (CIS) hardening benchmarks. It also takes into consideration standards like PCIDSS, HIPAA, NIST and many more.

5. Vulnerability assessment

It is the testing process in order to identify and assign severity prioritisation levels to all security defects in a specific timeframe. It uses automated and manual techniques with an emphasis on comprehensive coverage.

6. Threat Intelligence and Malware Detection

Threat intelligence is the process of data analysis for the purpose of understanding a threat actor’s motives, targets, and attack behaviours. Threat intelligence lead to faster, more informed, data-backed security decisions and influences positively behaviour from reactive to proactive in relation to cybersecurity threats. Malware detection is a set of defensive techniques and technologies required to identify, block and prevent the harmful effects of malware.

7. Offline Analysis Assessment

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

Security assessment performed in a way that guarantees that sensitive data does not leave leak.

8. **Security**

   The protection of the networking infrastructure from unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.

9. **Command Execution Mode**

   Usually refers to synchronous and asynchronous command execution modes

10. **Mitigation**

    Mitigation, or Attack Mitigation, is process of severity reduction of a threat event. Usually is centered around strategies to limit the impact of a threat against data in custody.

8.2 Cybersecurity Operational Scenarios

The below list presents the most usual Cybersecurity operational scenarios:

- Ransomware detection and response at End Point Level: is meant to represent complex attack chain, ultimately targeting at the deployment of a ransomware in the victim host.
- Data Leak Attempt: USB devices are a common tool for malicious users and attackers to infiltrate a system by opening backdoors, retrieving data that they are not authorized to, deleting sensitive data that can cause large losses to their owners or generally speaking to achieve their goals.
- Network Analysis Outlier Detection with statistical analysis: Statistical analysis is relevant in the detection of anomalous behaviour which could indicate an adversary, at the level of the network. Network-based attacks that could be spotted using outlier detection include volumetric attacks, rare connection connections (ports / sources / destination combinations), the use of novel and suspicious protocols used for exploitation, and more.
- Windows Registry Attack: These types of attacks provide the persistency access to the malicious attackers.

8.3 OneNet Cybersecurity Recommendations

Recommendations deriving from cybersecurity requirements for grid operators listed in Table 5 are based on the nineteen chapters of NISTIR 7628 Smart Grid Cyber Security standard [14] (also presented in D5.8 in the related chapter). Each line represents a condensed description of standard chapter with additional more specific recommendations (measures). Included, relevant results of the cybersecurity survey are taken into account. In addition to listed guidelines, relation to CIA (Confidentiality (C), Integrity (I), Availability (A)) triad security model is shown and GDPR privacy principles are listed for each generic recommendation in order to highlight how data privacy is supported.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 5: Security related constraints and non-functional requirements based on NISTIR 7628.

NISTIR 7628 requirements	Description & Recommendations	CIA	GDPR privacy principles
SG.AC Access Control	Ensure resources are only accessed by authorized personnel. Recommendations: • Separation of duties should be enforced to eliminate conflicts of interests. (NISTIR 7628 SG.AC-6) • Principle of least privilege should be implemented. (NISTIR 7628 SG.AC-7) • For critical systems with higher security levels consider using of multi-factor authentication, cryptographic devices, or client-side certificates for higher impersonation resistance. (OWASP ASVS 2.2.4) Notes: According to survey results, most reported security breaches were spam and phishing emails, further reinforcing the need for separating less critical office systems from mission critical ones.	C, I, A	• Lawfulness, fairness and transparency • Purpose limitation • Data minimization • Integrity and confidentiality (security) • Accountability
SG.AC Access Control	Ensure resources are only accessed by authorized personnel. Recommendations: • Separation of duties should be enforced to eliminate conflicts of interests. (NISTIR 7628 SG.AC-6) • Principle of least privilege should be implemented. (NISTIR 7628 SG.AC-7) • For critical systems with higher security levels consider using of multi-factor authentication, cryptographic devices, or client-side certificates for higher impersonation resistance. (OWASP ASVS 2.2.4) Notes: According to survey results, most reported security breaches were spam and phishing emails, further reinforcing the need for separating less critical office systems from mission critical ones.	C, I, A	• Lawfulness, fairness and transparency • Purpose limitation • Data minimization • Integrity and confidentiality (security) • Accountability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

SG.AU Audit and accountability	Security of OneNet information system should be validated by conducting periodic audits and logging of critical activities. Recommendations: - Detect and record security relevant events. (OWASP ASVS 7.1.3) - Non-repudiation measures should be implemented. (NISTIR 7628 SG.AU-16) Notes: According to survey results insider attacks were considered one of the most critical threats for Energy industry.	I	- Lawfulness, fairness and transparency - Integrity and confidentiality (security) - Accountability
SG.CA Security assessment and authorization	Compliance of OneNet information system should be regularly assessed. In case of nonconformance appropriate corrective actions should be implemented. Recommendations: - Conduct routine self-assessments. (ENISA Smart Grid Threat Landscape and Good Practice Guide 9.1.9).	C, I	Integrity and confidentiality (security)
SG.CM Configuration management	Policies and procedures must be set in place to manage and document all configuration changes to information system. All updates and patches should be thoroughly tested on a non-production environment. Recommendations: - System components should be configured to provide only essential functionality with unnecessary functions, ports, protocols and services disabled. (NISTIR 7628 SG.CM-7) - Baseline configuration for smart grid information system should be developed, documented and maintained as well as keeping previous baselines for possible rollback (NISTIR 7628 SG.CM-2) Notes: Establishment of configuration management process is recommended. (ENISA Smart Grid Threat Landscape and Good Practice Guide 9.1.3)	I, A	- Integrity and confidentiality (security) - Accountability
SG.CP Continuity of operations	Capacity to continue or resume operations after disruptions should be documented. Security measures necessary for maintaining required continuity level must be guaranteed.	A	N/A

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	Recommendations: • OneNet systems should integrate fail-safe response procedures upon the loss of communications with other systems. (NISTIR 7628 SG.CP-11) • Use of backup telecommunication provider(s) (NISTIR 7628 SG.CP-8) and alternate control centre(s) should be considered. (NISTIR 7628 SG.CP-9) Notes: • Distributed/decentralized architecture would increase availability and reliability of OneNet information system (Based on the experience from UXP [33]). • Load balancing should be used for critical components to guarantee continuous functioning of the infrastructure (Based on experience from UXP). • It should be possible to increase the reliability and performance of all components by adding redundancy (Based on experience from UXP).		
SG.IA Identification and authentication	Identity of users must be verified before granting them access to OneNet information system. Recommendations: • Authentication mechanism should obscure feedback during authentication process. (NISTIR 7628 SG.IA-6) Anti-automation measures should be implemented to mitigate breached credential testing, brute force and account lockout attacks. (OWAPS ASVS 2.2.1)	C, I	Accountability
SG.ID Information and document management	Important and sensitive information and documentation must be protected and retained. Recommendations: Communications with devices outside OneNet system should be limited only to the devices that need to communicate. (NISTIR 7628 SG.ID-4).	C, I, A	• Lawfulness, fairness, and transparency • Integrity and confidentiality (security) • Accountability
SG.IR Incident response	Capability to maintain or resume operations of information system in the event of disruption must be maintained. Recommendations:	C, I, A	Accountability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

	- In case of wider adaptation of technologies developed during OneNet need for European Organization similar to US ICS-CERT has been identified. (SGIS Report) Notes: Based on survey results over 50% of OneNet stakeholders require intrusion detection for power systems from second to minutes timescale.		
SG.MA Smart grid information system development and maintenance	Security measures should be sustained and improved through effective maintenance of OneNet information system. Recommendations: - Administration and management functions should be limited to authorized administrators. (OWASP ASVS 13.1.2). Authorized administrators should be able to verify integrity of all security relevant configurations. (OWASP ASVS 14.1.5).	C, I, A	Integrity and confidentiality (security)
SG.MP Media protection	Access to physical media should be limited only to authorized users. Recommendations: - Passwords, integrations with databases and third-party systems, API keys should resist offline attacks. (OWASP ASVS 2.10.4) Regulated private data should be stored encrypted. (OWASP ASVS 6.1.1).	C, I	- Lawfulness, fairness and transparency - Purpose limitation - Data minimizations - Accuracy - Integrity and confidentiality (security) - Accountability
SG.PE Physical and environmental security	Physical access control and surveillance mechanisms should be implemented to ensure only authorized access to system components.	C, I, A	- Integrity and confidentiality (security) - Accountability
SG.PL Planning	Security planning should be utilized to prevent undesirable interruptions to continuity of operations.	C, I, A	N/A
SG.PM Security program management	Security program management should be utilized throughout life cycle of information system in order to guarantee adequate security policy. Recommendations:	C, I	- Integrity and confidentiality (security) - Accountability

	• Senior management authority should be appointed to coordinate, develop, implement and maintain security program. (NISTIR 7628 SG.PM-3) Framework of management accountability should be defined so that it establishes roles and responsibilities related to cybersecurity across the organization. (NISTIR 7628 SG.PM-8).		
SG.PS Personnel security	Procedures for background checks, employee and contractor onboarding and offboarding should be documented.	C, I, A	• Lawfulness, fairness and transparency • Integrity and confidentiality (security) • Accountability
SG.RA Risk management and assessment	Risk identification and classification process should be continually performed to ensure information system's compliance to necessary requirements.	C, I, A	Integrity and confidentiality (security)
SG.SA Smart grid information system and services acquisition	Detailed procedures for reviewing acquisitions of new system components should be enforced in order to avoid introduction of additional vulnerabilities into the OneNet information system. <u>Recommendations:</u> • Security engineering principles should be applied in specification, design, development and implementation of all OneNet information systems. (NISTIR 7628 SG.SA-8) • Information system documentation should include guides on how to install, configure and use security features built into the system. (NISTIR 7628 SG.SA-5) System development lifecycle methodology should include security. (NISTIR 7628 SG.SA-3)	C, I, A	Integrity and confidentiality (security)
SG.SC Smart grid information system and communication protection	Measures should be considered to protect information system components and communication links against cyber intrusions. <u>Recommendations:</u> • Industry proven or government approved cryptographic algorithms and libraries should be used. (OWASP ASVS 6.2.2).	C, I	Integrity and confidentiality (security)

	Recommendations on cryptographic algorithms and key sizes should be updated frequently. (OWASP ASVS 6.2.3).		
SG.SI Smart grid information system and information integrity	Integrity of sensitive data should be maintained. Recommendations: - Security functions should be verified on system start-up, restart and at defined frequency when tasked by user with appropriate privileges. (NISTIR 7628 SG.SI-6) Announced software and firmware flaws as well as flaws discovered during security assessments need to be addressed. (NISTIR 7628 SG.SI-2).	I	Integrity and confidentiality (security)

9 Conclusions

This document showcases a comprehensive examination of the legal and security aspects relevant to OneNet, incorporating key references such as NISD, GDPR, NISTIR, ENISA, and Electricity Network Codes and Guidelines. This examination's results establish a conceptual framework that serves as a basis for outlining essential recommendations and measures regarding privacy, data protection, and security.

Additionally, a methodology for identifying and evaluating potential concerns within operators and their specific use case scenarios, including likelihood and impact assessments is proposed. Through this methodology operators will be able to identify cybersecurity potential issues and act accordingly since an ordered data-gathering and self-assessment process is essential for safeguarding any system. The analysis conducted and the measures proposed demonstrates a strong emphasis on cybersecurity awareness within the consortium and highlights how adherence to principles, guidelines, and legal frameworks in system development helps address security concerns. The entire development of the OneNet project has been framed by cybersecurity considerations and influenced by these guidelines.

While the OneNet Reference Architecture IT implementation (as per WP5 "Open IT Architecture for OneNet" and WP6 "Reference IT Implementation for OneNet") has addressed cybersecurity aspects that refer to it as it is documented in D5.8 and D6.6, there are cybersecurity considerations that need to be addressed from the side of the platforms that act as counterparties of the OneNet system. In this regard this deliverable is presenting recommendations deriving from cybersecurity, privacy, and other regulatory requirements from the operators' perspective.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

References

[1] "General Data Protection Regulation," [Online]. Available: https://gdpr-info.eu/.

[2] "EU policies aim to deliver secure, sustainable and affordable energy for citizens and businesses.," [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/report_final_eg1_my_energy_data_15_november_2016.pdf.

[3] "European Commission, Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast)," 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R.

[4] "ACER, Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)," July 2022. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20CS/Revised%20Network%20Code%20on%20Cybersecurity%20(NCCS)_1.pdf.

[5] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[6] "European Commission, Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union," 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union.

[7] "IEC, Security Standards and Best Practices for the Smart Energy Operational Environment," 2023. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/.

[8] "ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en.

[9] "ISO/IEC 27002:2022(en) Information security, cybersecurity and privacy protection — Information security controls," 2022. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en.

[10] "ISO/IEC 27019:2017(en) Information technology — Security techniques — Information security controls for the energy utility industry," 2017. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27019:ed-1:v2:en.

[11] "IEC 62351 – Cyber Security Series for the Smart Grid," 2023. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/.

[12] "CEN-CENELEC-ETSI Smart Grid Coordination Group, SG-CG/M490/H_ Smart Grid Information Security," 2014. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/7_sgcg_sg.

[13] "ENISA, Proposal for a list of security measures for smart grids," 2013. [Online]. Available: https://energy.ec.europa.eu/system/files/2014-11/20140409_enisa_0.pdf.

[14] "NISTIR Guidelines for Smart Grid Cybersecurity," [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final.

[15] "ENISA, Stergiopoulos G., Power Sector Dependency on Time Service: attacks against time sensitive services," [Online]. Available: https://www.enisa.europa.eu/publications/power-sector-dependency/.

[16] "ENISA, Ferrara D., Marianos L., Portesi S., Tsekmezoglou E., EU cybersecurity market analysis," 2022.

[17] "ENISA, Report on Cyber Security Information Sharing in the Energy Sector," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector.

[18] "National Institute of Standards and Technologies, NIST-800," [Online]. Available: https://csrc.nist.gov/publications/sp800.

[19] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016.

[20] "Identity Defined Security Framework," [Online]. Available: https://www.idsalliance.org/identity-defined-security-101/.

[21] "Let's Get Real: The IDS Reference Architecture Model," [Online]. Available: https://internationaldataspaces.org/offers/reference-architecture/.

[22] K. Kukk, F. Bosco, M. Lacerda, V. Sakas , A. Kapetanios and K. Kotsalos, "Cross stakeholder Data Governance for Energy Data Exchange," 2023. [Online]. Available: https://onenet-project.eu/wp-content/uploads/2023/04/D6.2-OneNet-v1.0.pdf.

[23] "ISA², Interoperability solutions for public administrations, businesses and citizens," [Online]. Available: https://ec.europa.eu/isa2/eif_en/.

[24] F. Bosco, D. Ziu , A. Triveri, V. Croce, V. Sakkas, A. Kapetainos, K. Kotsalos , M. Haghgoo , J. Campos, T. Alves, N. Samovich , C. D. Silva, A. Lucas and K. Kukk, "OneNet Reference Architecture," 2021.