ONENET
one network for Europe

Report on Cybersecurity, privacy and other business regulatory requirements

D5.8

Authors:

Magda Zafeiropoulou (UBITECH Energy)

Thanasis Bachoumis (UBITECH Energy)

Katerina Drivakou (UBITECH Energy)

Anastasis Tzoumpas (UBITECH Energy)

Ferdinando Bosco (ENGINEERING)

Denisa Ziu (ENGINEERING)

Aivo Toots (CYBERNETICA)

Andres Jõgi (CYBERNETICA)

Marko Petron (CYBERNETICA)

Distribution Level	PU
Responsible Partner	UBITECH Energy
Checked by WP leader	Date: 07/07/2021 [Ferdinando Bosco, ENG]
Verified by the appointed Reviewers	Date: 19/07/2021 [Maria Papadimitriou, CIN] 20/07/2021 [Vassilis Sakas, ED]
Approved by Project Coordinator	Date: 23/07/2021 [Stephan Gross, FHG]

Dissemination Level		
PU	Public	x
CO	Confidential, only for members of the consortium (including the Commission Services)	
CI	Classified, as referred to in Commission Decision 2001/844/EC	

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	31-07-2021
Actual date of delivery	28-07-2021
Status and version	Ready for submission, V1

Version	Date	Author(s)	Notes
0.1	01-06-2021	Magda Zafeiropoulou (UBE) Thanasis Bachoumis (UBE) Katerina Drivakou (UBE) Anastasis Tzoumpas (UBE)	First draft of the deliverable.
0.2	15-06-2021	Magda Zafeiropoulou (UBE) Thanasis Bachoumis (UBE) Katerina Drivakou (UBE) Anastasis Tzoumpas (UBE)	First draft of the chapters 3,4,5, and 6.
0.3	28-06-2021	Ferdinando Bosco (ENG) Denisa Ziu (ENG) Aivo Toots (CYB) Andres Jõgi (CYB)	Draft of chapter 7 and contribution to chapter 5.
0.4	02-07-2021	Thanasis Bachoumis (UBE) Anastasis Tzoumpas (UBE)	Refinements regarding the context and structure of the deliverable.
0.5	14-07-2021	Maria Papadimitriou (CIN) Vassilis Sakas (ED)	Official review receival
0.6	16-07-2021	Thanasis Bachoumis (UBE) Magda Zafeiropoulou (UBE) Anastasis Tzoumpas (UBE) Ferdinando Bosco (ENG) Marko Petron (CYB)	Refinements in the document based on the reviews
0.7	23-07-2021	Stephan Gross (FHG)	Quality check process
1.0	28-07-2021	Thanasis Bachoumis (UBE) Anastasis Tzoumpas (UBE)	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

OneNet 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.

The project OneNet (One Network for Europe) is funded through the EU's eighth Framework Programme Horizon 2020. It is titled "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)".

While the electrical grid is moving 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. For this reason, the two major associations of grid operators in Europe, ENTSO-E and EDSO, have activated their members to put together a unique consortium.

OneNet will see the participation of a consortium of over 70 partners. Key partners in the consortium include the already mentioned ENTSO-E and EDSO, Elering, EDP Distribution, RWTH Aachen University, University of Comillas, VITO, European Dynamics, UBITECH, Engineering, and the EUI's Florence School of Regulation (Energy).

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.

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

Contents

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

Figures

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

Tables

List of Abbreviations and Acronyms

Acronym	Meaning
ASVS	Application Security Verification Standard
CIP	Critical Infrastructure Protection
CSIRT	Computer Security Incident Response Team
GDPR	General Data Protection Regulation
DER	Distributed Energy Resources
DNS	Domain Name System
DoA	Description of Action
DPbDD	Data protection by design and by default
DPIA	Data Protection Impact Assessment
DPO	Data protection officer
DSO	Distribution System Operator
DSP	Digital service providers
EC	European Commission
ECCG	European Cybersecurity Certification Group
EDPB	European Data Protection Board
EEA	European Economic Area
EMS	Energy Management System
EnC CPs	Contracting Parties of the Energy Community Treaty
ENISA	European Union Agency for Cybersecurity
ESCOs	Energy Service Companies
ETSI	European Telecommunications Standards Institute
FACTS	Flexible Alternating Current transmission system
HMI	Human Machines Interface
IACS	Industry Automation Control Systems
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
MAC	Media Access Control
MO	Market Operator
MS	Member States
NCA	National Competent Authority
NCCA	National Cybersecurity Certification Authority
NERC	North American Electric Reliability Corporation

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

NISD	Network and Information Security Directives
NIST	National Institute of Standards and Technology
NISD	Network and information systems Directive
OES	Operators providing essential services
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
POPD	Protection of Personal Data
RTU	Real Time Unit
SCADA	Supervisory control and data acquisition
SbD	Security by Design
SCCG	Stakeholders Cybersecurity Certification Group
SGIS	Smart Grid Information Security
SIEM	Security Information and Event Management
SO	System Operator
SPOC	Single Points of Contact
SSCP	Secure SCADA Communication Protocols
TSO	Transmission System Operator
WP	Work Package

Executive Summary

Power markets are being completely transformed by the massive entry of Renewable Energy Sources and the electrical grid is moving towards being more decentralized. As a result, the consumer role is evolving towards a more active one. The mission of OneNet is to create the conditions for a new generation of grid services able to fully exploit demand response, storage and distributed generation while creating fair, transparent and open conditions for the consumer. WP5 aims to design and an open conceptual architecture for effective yet seamless operation of a smarter pan-European electricity system, and to provide requirements, functional and technical specifications, together with interoperable and standardizable interfaces for an open scalable decentralized platform, technology agnostic, adaptable and flexible IT reference architecture, which will fully support the concept of OneNet. In this context, this report entitled as "Cybersecurity, privacy and other business regulatory requirements" is related to the Task 5.8. The main objective of Task 5.8 is to cover the full range of possible societal, ethical, legal and business concerns related to the research, the development of the OneNet architecture and its operation.

The report provides the outcome of the work performed in the context of Task 5.8 of the OneNet project. Specifically:

- An initial review of important assets, SCADA systems and potential threats in those systems is conducted.
- Identification and assessment of cybersecurity requirements, regulatory frameworks, and best practices in EU and globally in terms of power industry, and the new era of smart grids is carried out.
- Identification of the security landscape in the energy sector. Therefore, a questionnaire has been generated and distributed amongst OneNet partners. Based on survey results, security threats critical to energy sector are identified and measures already implemented in industry are determined. Furthermore, participants' data privacy posture is surveyed, including engagement of Data Protection Officer (DPO) and conducting of Data Protection Impact Assessment (DPIA) for OneNet demonstrators.

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

- Six plus one privacy principles of GDPR should be seen as the guiding principles of regulation on compliant processing, especially so when dealing with customer data and other personally identifiable information.
- Data controller obligations and data subject's rights in terms of GDPR have been reviewed and considered.
- Establishment of comprehensive requirements provided in NISTIR 7628 are recognized as the most relevant guidelines for going forward with OneNet project. Based on this, more detailed recommendations and suggestions have been provided, also considering SGIS report, European Union Agency for Cybersecurity (ENISA) cybersecurity guidelines for smart grids and Open Web Application Security Project (OWASP) ASVS security verification standard.

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 Purpose of this 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), WP5 contributes to the direction of fulfilling the OneNet envision by striving to attain two objectives; First, to design an open conceptual architecture for effective yet seamless operation of a smarter pan-European electricity system where market and network technical operations are coordinated closer to real-time across countries, and second to provide requirements, functional and technical specifications, together with interoperable and standardizable interfaces for an open scalable decentralized interconnection of platforms, technology agnostic adaptable and flexible IT reference architecture which fully support the OneNet concept and provides the necessary backbone for the WP6 subsequent implementation of the OneNet data sovereignty-preserving working space.

This task contributes to the overall WP5-level objectives, by providing cybersecurity, privacy, and other regulatory requirements. 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. Special attention is given to issues surrounding data protection. Cybersecurity is an increasingly regulated environment that goes way beyond technical prevention measures; this does for example creates legal obligations. This task focuses on an assessment of relevant legal standards and regulations, by using as a starting point the global and European (EU as well as Council of Europe) standards.

As illustrated in Figure 1.1, a high amount of interdependencies amongst tasks in different WPs, involving T5.8, exists. The outcome of this report constitutes the foundations from a security perspective based on which the OneNet concept will be built upon. Regarding the horizontal WPs, WP4 will utilize the data privacy requirements declared in this deliverable to conduct a requirement analysis regarding cybersecurity measures for grid operators and customer integration. Moreover, other tasks of WP5, such as T5.2 and T5.6, which are responsible for the creation of the OneNet architecture, and the extended data and service interoperability in the OneNet platform of platforms, respectively, need as a knowledge from this deliverable all the presented standards for data security in energy sector. Finally, 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.

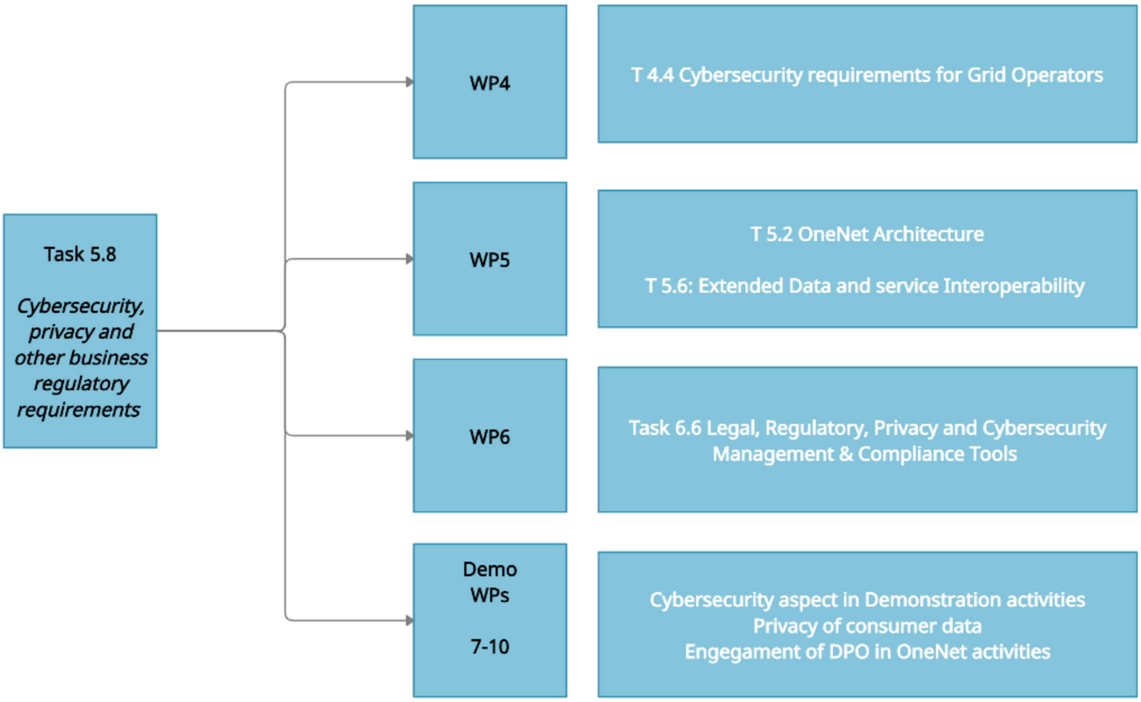

Task 5.8
Cybersecurity, privacy and other business regulatory requirements
WP4
T 4.4 Cybersecurity requirements for Grid Operators
WP5
T 5.2 OneNet Architecture
T 5.6: Extended Data and service Interoperability
WP6
Task 6.6 Legal, Regulatory, Privacy and Cybersecurity Management & Compliance Tools
Demo WPs 7-10
Cybersecurity aspect in Demonstration activities
Privacy of consumer data
Engegament of DPO in OneNet activities

Figure 1.1: Connection of D5.8 with the rest tasks and WPs of OneNet project.

1.2 Structure of this document

The structure of this deliverable is unfolded as follows: Chapter 2 includes the methodology introduced for the creation of this deliverable. Chapter 3 contains information regarding the regulatory environment in the energy sector along with the EU framework for data protection. Chapter 4 incorporates information about Cyber incident communication procedures and impact awareness. Moreover, chapter 5 contains details regarding cybersecurity standards in the energy industry. In chapter 6, the results of the survey distributed to the partners participating in the OneNet demonstrators are presented, providing important information regarding their perspective, knowledge, and expectations of cybersecurity in the context of OneNet. In chapter 7, by encapsulating all the previous presented information, we make cybersecurity recommendations for the OneNet architecture and relevant constraints. Finally, chapter 8 concludes the work conducted in this deliverable and acts as a connection point delivering the key outcomes needed by other OneNet tasks.

2. Methodology

In order to set the basis for the societal, ethical, legal, and regulatory landscape concerning data protection and cybersecurity, relevant information has been collected and processed following the next sequence of actions:

- Following the developments in WP1, where technical and organisational measures will be implemented to safeguard the rights and freedoms of the data subjects/research participants.
- Network and Information Security Directives (NISD).
- Cybersecurity Standards in power industry.
- Documents from regulatory authorities and collection on legal instruments.
- Survey: A questionnaire has been designed and distributed to the OneNet partners.
- Extensive research on European law using a thorough approach.
- Cybersecurity, privacy and other business regulatory requirements are derived.
- Recommendations in demonstrators about data privacy and security.

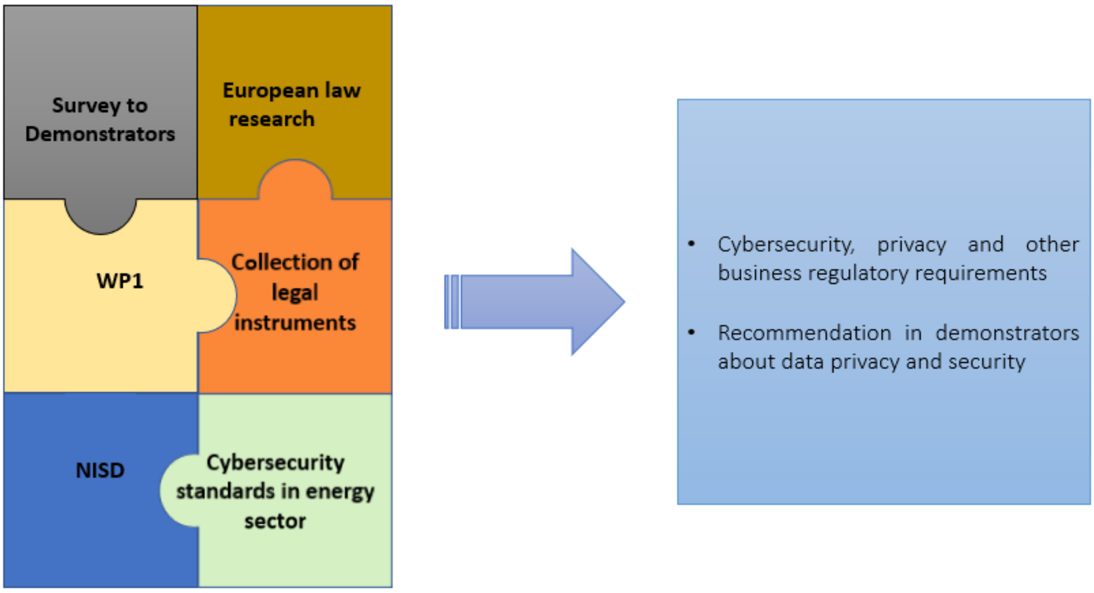
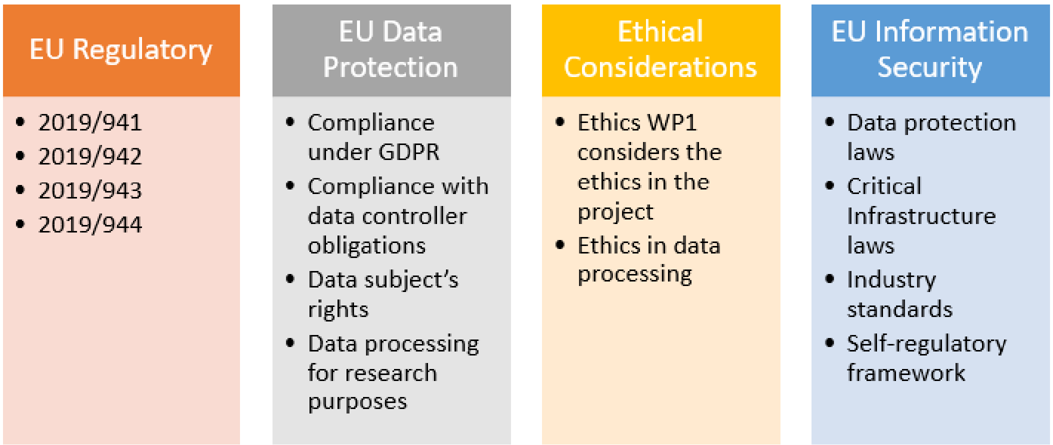

Survey to Demonstrators
European law research
WP1
Collection of legal instruments
NISD
Cybersecurity standards in energy sector
• Cybersecurity, privacy and other business regulatory requirements
• Recommendation in demonstrators about data privacy and security

Figure 2.1: Methodology used for the development of D5.8.

3. Legal Regulatory and Ethical Environment

This chapter contains information regarding the regulatory framework in the energy sector, along with the EU framework for data protection. Those two elements are of vital importance in order to define the cybersecurity requirements in the context of OneNet. Moreover, the ethical considerations that need to be considered in OneNet are also incorporated. Finally, the EU information security framework is presented in detail.



EU Regulatory	EU Data Protection	Ethical Considerations	EU Information Security
• 2019/941 • 2019/942 • 2019/943 • 2019/944	• Compliance under GDPR • Compliance with data controller obligations • Data subject's rights • Data processing for research purposes	• Ethics WP1 considers the ethics in the project • Ethics in data processing	• Data protection laws • Critical Infrastructure laws • Industry standards • Self-regulatory framework

Figure 3.1: Frameworks elaborated on this chapter.

3.1 EU Regulatory Framework in the Energy Sector

The EU has created standard rules for the energy industry within the scope of the single market, which are incorporated in a number of legal and non-legal instruments [1]. The Treaty on European Union, for example, contains explicit provisions on energy and lays out the goals for the internal market's functioning in terms of energy—supply security, efficiency, renewable energy, and infrastructure. It also gives Member States the power to choose the terms for exploitation of their energy resources and to develop their own energy structure (Art. 194). Various instruments, including those relating to electricity generation and distribution, consumer and critical infrastructure protection, and removing obstacles and discrimination in the electricity market, have been adopted in the electricity sector to achieve this goal (see, for example, the Electricity Directive (2009/72/EC)) [2].

It is worth noting that the EU's energy strategy prioritizes energy supply security and encourages research and innovation in this field, among other things. Recently, the "clean energy for everyone European package" program was launched. The program on "clean energy for all European package" [3] resulted into four legislative instruments adopted by the European Parliament:

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

- Regulation (EU) 2019/941 on risk preparedness in the electricity sector, which requires the EU Member States to prepare plans for how to deal with potential future electricity crises, and put the appropriate tools in place to prevent, prepare for and manage these situations [4].
- Regulation (EU) 2019/942 establishing an EU Agency for the cooperation of energy regulators, which recasts the regulation 713/2009 [5].
- Regulation (EU) 2019/943 on the internal market for electricity (recast), which establishes rules to ensure the functionality of the internal market for electricity [4].
- Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) [2].

Apart from putting a heavy emphasis on the EU's goal of producing clean energy, these instruments also address issues such as energy security, operational efficiency, consumer protection and involvement, and crisis management, amongst others. Given the rapid pace of innovation in the information technology sector and the significant impact it is having on the EPES, the synergy between the electrical sector's operational structure and the need for cybersecurity and data protection is a welcome development. This is especially true because this innovation introduces a new source of cybersecurity vulnerability into the operational framework, as well as privacy hazards such as profiling, mass surveillance, loss of control, violation of confidentiality, and transparency, etc. ENISA has detailed certain security-related aspects of microgrid security and made recommendations [6].

Cyberattacks are recognized as severe circumstances for the electricity power system in the “Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC” [4]:

“The consequences of electricity crises often extend beyond national borders. Even where such crises start locally, their effects can rapidly spread across borders. Some extreme circumstances, such as cold spells, heat waves or cyberattacks, may affect entire regions at the same time.”

The Regulation (EU) 2019/941 considers the Directive on Network Information Security (NIS) [7] and ensures that cyber-incidents are recognized as a risk and factored into risk management plans. Furthermore, Regulation (EU) 2019/941 mandates the establishment of National Competent Authorities (NCAs), as well as the development of a methodology by the European Network of Transmission System Operators for Electricity (ENTSO-E) to detect regional electricity crisis scenarios. The Methodology was proposed and recently approved by ACER (March 2020). Cyberattacks have been added to the Methodology as a risk that could lead to a power outage [8].

ENTSO-e must develop relevant regional electricity crisis scenarios within six months of the Methodology's approval, as required by Regulation (EU) 2019/941 and based on the Methodology, and submit the proposals to regional security centres, TSOs, competent authorities, and the Electricity Coordination Group (ECG). The NCAs should prepare national crisis scenarios within four months of identifying regional scenarios and discuss them with the necessary national authorities, including the TSOs. The risk-preparedness plans are built on the basis of regional and national electricity crisis scenarios. The NCAs should prepare national crisis scenarios within four months of identifying regional scenarios and discuss them with the necessary national authorities, including the TSOs. The risk-preparedness plans are built on the basis of regional and national electricity crisis scenarios. The Regulation (EU) 2019/941 recognizes the need of collaboration between EU Member States (MSs) and Energy Community Treaty Contracting Parties (EnC CPs) in identifying electrical crises, developing crisis scenarios, and developing risk preparedness plans. These actions must result in solutions that do not jeopardize the security of EU MS and EnC CP supply. The EC may invite EnC CPs to participate in the ECG for these purposes.

The "Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity" adds cybersecurity to ENTSO-E's and the EU Distribution System Operators (DSO) entity's responsibilities. Specifically, ENTSO-E is responsible for promoting cybersecurity, while the EU DSO entity's responsibilities include data management and protection, as well as cybersecurity, in collaboration with competent authorities and regulated organizations. In addition, Article 59 (2)(e) of Regulation (EU) 2019/943 mandates the creation of a Network Code for Cybersecurity in order to establish sector-specific rules to ensure cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting, and crisis management. Multiple stakeholders from the energy industry have offered public feedback as part of an open consultation process spearheaded by the European Commission, in which they expounded on the necessity for and scope of new cybersecurity electrical standards.

3.2 EU Data Protection Framework

The GDPR is the most important general legislation governing the privacy and protection of personal data of persons whose data is processed using both automated and manual means. It focuses on enforcing individual rights, boosting the EU internal market, assuring tighter rule enforcement, facilitating international personal data transfers, and establishing global data protection standards. As already stated, the GDPR applies once personal data is processed; these are defined by the GDPR as [9]:

> *"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*

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

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. [10]. 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.

3.2.1 Compliance requirements under the GDPR

3.2.1.1 Observance of the principles of data protection

The essential principles specified in Article 5 of the GDPR for defending the rights of data subjects are known as data protection principles. They are broad principles that convey the underlying purposes, obligations, and constraints of processing personal data without dictating precise ways in which data controllers and processors must comply. These ideas have been turned into “protection goals that the system must target” in systems engineering. These principles are:

- **Lawfulness, fairness, and transparency:** Personal data must be processed lawfully, fairly, and transparently in relation to the data subject, according to this principle. Data controllers must have valid reasons for processing personal data, and they must not use the data in ways that have unjustifiable

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

negative consequences for the individuals involved. The GDPR provides a number of other legal reasons on which the data controller can lawfully handle data:

- Consent,
- performance of a contract,
- compliance with a legal obligation,
- protection of the vital interest of the subject or another natural person,
- performance of public interest task, and,
- the legitimate interest of the controller or a third party (Art. 6).

- Fairness indicates that personal data must be processed fairly, and that following the other criteria suggests that the processing is fair. Under the GDPR, transparency is an overarching obligation that applies to three central areas: the provision of information to data subjects about the nature and purpose of processing; the provision of information to data subjects about the nature and purpose of processing; and the provision of information to data subjects about the nature and purpose of processing; data controllers' communication with data subjects about their rights; and data controllers' support of data subjects' exercise of their rights.
- Purpose limitation: Personal data must be acquired for specific, explicit, and legitimate objectives and not subsequently processed in a way that is incompatible with those aims, according to this principle. This means that the objective must be established before data processing can begin. Additional data processing is only permitted in certain circumstances and is subject to certain safeguards. (Art. 5(1)(b)).
- Data minimization: This principle stipulates that only the bare minimum of personal data be gathered and processed in order to achieve a given goal. It is necessary to erase data that is no longer required. (Art. 5(1)(c)).
- Accuracy: This principle mandates that personal data be accurate and, where applicable, kept up to date. This means that the data controller must take all reasonable measures to ensure that erroneous personal data is deleted or corrected. (Art. 5(1)(d)).
- Storage limitation: This means that personal data must not be retained in a form that allows data subjects to be identified for longer than is required for the purposes for which it is processed. This concept is intended to avoid the indefinite retention of personal data in a manner that allows data subjects to be identified. In order to comply with this concept, data that is no longer required must be erased or anonymized. Personal data may, however, be held for longer periods only for public interest archiving, scientific or historical research, or statistical reasons, provided that suitable technical and organizational safeguards are in place to protect the data subject's rights and freedoms. (Art. 5(1)(e)).

- **Integrity and confidentiality:** Personal information must be processed in a way that protects data security. This includes employing suitable technical or organizational means to protect against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. This principle is important to data security and establishes a requirement for proactive risk assessment of personal data in transit (Art. 5(1)(f); see also Art. 32 for some examples of technical and organizational measure).
- **Accountability:** This principle requires data controllers and processors to demonstrate how they adhere to the GDPR's principles and duties. This is an overarching criterion that can be proved in a variety of ways, depending on the complexity and nature of their data processing, such as by conducting a data protection impact assessment, documenting, and generating a personal data inventory, and so on; establishing a data privacy governance framework, which may involve designating a Data Protection Officer (DPO); and implementing data protection by design and default (Art. 5(2)).

3.2.1.2 Compliance with data controller obligations

As stated above, the accountability requirement of the GDPR implies inter alia that the data controller complies with the obligations imposed by the regulation. These obligations are various and depend on the context of the data processing. The most prominent of these obligations in the context of the OneNet project are the follows:

- Observe the data protection principles, particularly, having a lawful basis for data processing (Art. 5),
- Implement appropriate technical and organizational measures to ensure compliance (Art. 24),
- Implement data protection by design and by default (Art. 25),
- For joint controllers (who together determine the purposes and means of processing: Art. 26), they must by means of an "arrangement" between them, apportion data protection compliance responsibilities between themselves (Arts. 4(7), 26); of liability (Art. 26(3)),
- Appointment of representatives by controllers outside the EU (Art. 27),
- Obligations related to the appointment of processors (Art. 28),
- Keep a record of processing activities (Art. 30),
- Cooperate with the supervisory authorities (Art. 31),
- Ensure data security (Art. 32),
- Data breach notification (Arts. 33, 34),
- Carry out a Data Protection Impact Assessment (Art. 35),
- Enable the rights of the data subjects (Art. 12),

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

- Observe rules of data transfers to non-EU states (Arts 44 ff).

Again, the importance of integrating the requirement of data protection by design and by default (DPbDD) (also known as Privacy by Design) in the architectural design of the OneNet system should not be underestimated or overlooked. Data Protection by Design is a principle that promotes privacy and data protection compliance from the start; an alternative to bolting privacy considerations on as an after-thought or ignoring them altogether. The requirements to implement DPbDD are reflected in Article 25 of the GDPR, which requires data controllers to:

"both at the time of the determination of the means for processing and at the time of the processing itself, [to] implement appropriate technical and organizational measures to protect the rights of the data subjects".

This provision has been interpreted to mean "effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default".

Data protection by design has a technologically neutral posture and is implemented contextually based on the nature, scope, context, and purpose of data processing, so that stakeholders are able, on a case-by-case basis, to translate these principles into concrete measures for guaranteeing data protection. The GDPR does not explicitly describe any technical or organizational measures in this regard; however, any measure adopted by the controller must be effective, facilitate the enforcement of the rights of the data subjects, consider the risks involved in the processing and in addition should be regularly reviewed. Key performance indicators should be defined to demonstrate the effectiveness of the measures adopted to comply with Article 25 of the GDPR.

Another part of the DPbDD principle is that by default—whenever default settings are pre-configured—the settings must be carefully chosen so that the safest and strictest privacy settings should apply, so that only personal data necessary to achieve specific purposes shall be processed (emphasis on data minimization). Data subjects should also be able to reset these settings at their choosing, an approach that shall continue throughout the life cycle of the data processing operations.

There are several operational methodologies for implementing this notion of DPbDD. Recently, the European Data Protection Board (EDPB) published guidelines on how to implement data protection by design and by default by data controllers and technology providers. These guidelines provide examples of key design and default elements, and it is highly recommended that these guidelines are consulted during the design of the OneNet platform and its individual tools:

- ➢ Wherever personal data is processed throughout the OneNet project, a clear legal basis for this is identified prior to such processing.

- The amount of personal data—volume, type, categories, and level of details—processed in the project is limited to those necessary for achieving the identified purposes.
- There is a mechanism for the data subjects to enforce their rights such as a contact point for access request.
- Personal data is not retained for a period longer than necessary for the achievement of the identified purposes. Data no longer needed should be automatically deleted.
- Access to personal data throughout the entire lifecycle and data flow is limited to those who need it.
- The information provided to the data subjects about the data processing is clear and presented in a manner, and the language they will understand.
- An information security management system is incorporated into the platform for managing information security incidents and policies.

3.2.1.3 Enablement of data subjects' rights

The GDPR sets the key rights enjoyed by the data subjects regarding the processing that occurs with their data. A major aspect relates to the data subjects' right to information and access to the information processed about them, thereby contributing to transparency, lawfulness, and fairness, which are considered as key cornerstones of data processing. These rights, which data controllers are obliged to facilitate the subjects in exercising, include:

- the right to information (Arts. 13, 14),
- the right of access (Art. 15),
- the right of rectification (Art. 5 (1)(d), 16),
- the right to erasure (Art. 17),
- the right to restrict processing (Art. 18),
- the right of data portability (Art. 20),
- the right to object to certain processing (Art 21),
- the rights in relation to automated decision making and profiling (Art 22).

It should be noted that these rights are at a first site, not absolute in character. They are subject to potential derogations in various situations. This implies that the rights may be denied or limited if there are compelling countervailing reasons for doing so. Under the GDPR, one situation for example where this may occur is when the unrestricted exercise of a given right interferes with the scientific research activity by overly burdening researchers or putting the accuracy of the results at risk. The possibility for EU member states to include exemptions in their respective national law is provided for in Article 89(2) of the GDPR. These exemptions may be relevant for the project during the research phase.

3.2.1.4 Data processing for research purposes

The GDPR allows data processing for the purpose of scientific research. In general, consent is seen as the most appropriate basis for this data processing since it allows the data subjects to make an informed decision on whether to participate in the research or not. Article 5(1)(b) also includes scientific or historical research purposes as one of the instances of compatibility for further processing. However, this provision is subject to the implementation of appropriate safeguards such as pseudonymization, anonymization, encryption, among others, where necessary to protect the data subjects. Also, a research purpose may also justify more extended storage of data under Article 5(1)(e).

Furthermore, the GDPR also allows some variation between Member States in some aspects of data protection law. In this regard, the processing of data for scientific research is one of the areas, where the Member States are allowed, among other matters, to provide for exemptions from some of the rights accorded to the data subjects, if it is deemed necessary in the interests of the research (see Article 89).

3.3 Ethical Considerations Relevant for OneNet Project

The domain of research ethics over time has revolved around defining the moral obligations regarding the way in which organizations and researchers should handle human subjects during research. Certain fundamental principles—human dignity, autonomy, necessity, and proportionality, as well as common good—have emerged as crucial matters of ethical relevance in this context. In some cases, mainly in bio-medical research, ethics committee approvals must be obtained before commencing such research as a form of independent safeguard to ensure that researchers do not privilege – inadvertently or not – the research interest over the interests of the human subject. The Ethics Work Package (WP 1) deliverables have previously addressed these issues, in terms of defining general requirements for the involvement of human subjects in the project. In the present analysis, specific emphasis will be placed on data and information usages in non-invasive research—collection and processing of personal data—and the ethical implications for the OneNet project.

It is notable that the GDPR also brings to the force the ethical aspect of data processing by stating (in Recital 4) that the processing of personal data should be designed to serve mankind. Advanced data processing mechanisms such as artificial intelligence, profiling, and the intended or unintended consequences of such processes have shown the need for ethical data and information management in systems development. Based on the scenarios and proposed outcome of the OneNet project, the following ethical issues should be considered as part of the system's development requirements.

3.4 EU Information Security Framework

Information security requirements are imposed by various legislative and non-legislative instruments within the EU and the Member States, such as data protection laws, critical infrastructure protection laws, industry standards and self-regulatory frameworks. The concept of information security as a term is commonly used to capture both the data security (aspects 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.

An important legal source of information security requirements relating to the protection of critical infrastructure is the EU Directive on security of network and information systems (NISD)[1] is an important legal source of information security requirements relating to the protection of critical infrastructure. It establishes measures to achieve a high common level of NIS among operators providing essential services (OES) and digital service providers (DSP). The NISD is the first horizontal instrument of its kind in the EU, and the EU Member States are obliged to ensure its implementation. OES are entities which provide essential services in the energy, transport, banking, financial markets, health, drinking water and digital infrastructure sectors. In a similar way to the GDPR (in respect of personal data processing), the NISD imposes key obligations on OES in the energy sector and the electricity subsector in respect to adopting appropriate and proportionate technical and organizational measures to manage the security risks of the network and information systems they operate (NISD, Art 14). Those measures shall ensure a level of security of network and information systems appropriate to the risk posed, having regard to state of the art.

To facilitate the implementation of the Directive, the NIS Cooperation Group has issued a "Reference document on security measures for Operators of Essential Services" [11], which concretizes key security measures for OES for enhancing their network and information security. The key recommendations of this document include:

- **Regular risk assessment** of the system as part of the Information System Security Risk Analysis to identify any security related risks, assess them and define appropriate risk treatment actions (mitigation, acceptance, avoidance, transfer),

[1] For more information about NIS Directive, please consult this link: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

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

- **Systems Configuration:** Configuring systems following industry hardening standards Installing only services and functionalities or connecting equipment which is essential for the functioning and security of the information system,
- **System Segregation:** Segregating logically or physically the systems to limit the propagation of IT security incident within the system or subsystem,
- **Traffic Filtering:** Filtering traffic flows circulating in the system and forbidding traffic that is not needed for the system and that is likely to facilitate attacks,
- **Cryptography:** Establishing and implementing a cryptography policy and related procedures to protect data confidentiality, authenticity and/or integrity,
- **IT Security Administration**: Restricting administrative accounts to authorized employees for only "need-to-know" tasks,
- **Identity and Access Management:** Authentication and Identification and Access Rights,
- **IT Security Maintenance:** Developing and implementing a security maintenance procedure to ensure that the latest versions of hardware and software are installed. Security requirements should also be enforced in Industrial Control Systems,
- **Physical and Environmental Security**
- **Security Incident Management process:** Such a process should include details on the below points:
    - **Detection:** Detection, Logging & Monitoring, Logs Correlation and Analysis,
    - **Computer Security Incident Management**: Information System Security Incident Response, Incident Report and Communication with Competent Authorities and Computer Incident Response Teams (CSIRTs),
- **Continuity of Operations**: Ensuring Business Continuity including Disaster Recovery Management,
- **Crisis Management:** Crisis Management Organization and Crisis Management Process.

Information security relating to the protection of personal data is part of the requirements under the GDPR's Article 32. It requires the data controller to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with the data it processes, particularly regarding the confidentiality, integrity, and availability attributes. These measures, however, include the protection of the data as well as the information system through which the data is processed. Two types of measures are considered:

- **Technical:** pseudonymization and encryption of personal data where appropriate; data minimization, regular testing of the systems, ensuring confidentiality, integrity, availability and resilience of processing systems and services through back-ups, authentication, among others; implementing data protection by design and by default, implement security by design and by default, regular update of the systems where necessary and logical access control, among others,

- **Organizational:** appropriate data protection and security policies, conducting a risk assessment, transparency in presenting information about the data processing, enabling data subjects to enforce their rights, physical access control, staff training, ensuring that only data processors with appropriate technical and organizational measures are used, among other measures.

From the EDPB guidelines on DPbDD, key design and default elements suggested in the guidelines can be translated to security requirements for developing information processing systems [12]. To this extent, the approach of Security by Design (SbD) must be embedded in OneNet as well. SbD is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attacks as possible through certain measures as continuous testing, authentication safeguards and adherence to best programming practices, among others throughout the SDLC lifecycle. The objectives of SbD can be accomplished by following and applying the ten principles proposed by OWASP [12] that are related to the three pillars of information security, namely: Confidentiality, Integrity and Availability (sometimes also referred to as the 'CIA triad').

It is essential to highlight that under both the GDPR and the NISD, data breach notification to the relevant authorities or data subjects is a requirement, which the affected stakeholders need to implement if there is a data security breach within the context that requires such notification. Further significant development regarding cybersecurity in the EU is the introduction of an EU-wide cybersecurity certification framework for ICT products, services, and processes under Regulation (EU) 2019/881 (the Cybersecurity Act) [13]. This framework aims to enable a harmonized approach at EU-level to cybersecurity certification schemes, to create a digital single market for ICT products, services, and processes. This Act, which makes ENISA's mandate permanent, also tasks ENISA with supporting and promoting the development and implementation of the EU policy on cybersecurity certification of ICT products, services, and processes. ENISA has recently published the relevant documents [14].

4. Cyber-incident communication procedures and impact awareness

The operation of complex systems as contemporary power systems requires new ICT-based tools and applications. While the strong synergy between the electricity and ICT infrastructure facilitates the transition of the power systems towards smart grids, it also increases the concerns for the cybersecurity of these systems. The electricity industry, technology providers, vendors, deployment, and system integrator companies are all facing threats that are evolving very fast and jeopardize the functioning of the products, services, and operation of systems they design or use. This is the main reason why stakeholders from electricity and ICT sectors are developing frameworks to assess risks of threats, increase security and build up systems' resilience. The efforts combine setting adequate legislation framework to enable stakeholders to assess risks and mitigate consequences; establishing international standards for the entire chain starting from products to systems; setting up risk-management processes based on good practice for the electricity sector and enabling cooperation between various stakeholders. In fact, these efforts should help in building up trust between stakeholders, improving procedures for cyber incidents reporting, increasing systems preparedness, and raising awareness on cyber hygiene.

4.1 Assets and threats

4.1.1 Assets

The assets that are related to information and control systems include[15]: physical components of the electricity system (cables, relays, transformers, switches, automation, sensors, Flexible Alternating Current Transmission System (FACTS) devices, etc.); operational information about electrical assets (status indicators, alerts, events, disturbance information); historical information (data that is stored for further use/or as legislation requirement); trending information (all information related to commercial issues); information system configuration (communication network topology, internet protocol (IP) addresses, media access control (MAC) addresses, user credentials & permissions, con-figuration files, location data). The information systems and industry automation control systems (IACS) used in power systems include software applications, various services for these applications, supervisory control, and data acquisition (SCADA) and other hardware components. Their operation is based on ICT and exchange of data.

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

4.1.1.1 Industrial Automation Control Systems – SCADA

IACS-SCADA are amongst the essential assets existing in power systems as they enable remote acquisition and control of other assets or infrastructures. The basic building blocks of SCADA system are:

- the remote terminal units (RTUs),
- the communication system,
- the master station/ central computer system and the human machines interface (HMI).

Modern SCADA systems also contain intelligent electricity devices (IEDs), data concentrators, various sensors, programmable logic controllers (PLCs) and other hardware. Apart from the hardware components, SCADA systems include software, which provides functionalities regarding data acquisition and control, databases, analytics generation, as well as HMI visualization. Furthermore, advanced software functions are implemented in SCADA systems used by both ESCOs and SOs. Because of their central role in power system control as building blocks of Energy Management Systems and Distribution Management Systems, as well as due to their interdependencies to other systems and infrastructure, provision of sufficient level of safety and security for these systems is crucial. The security requirements of the IACS-SCADA should be considered during the entire phase of the installation and operation, namely development, design, implementation, and operation phase.

Due to their architecture, communication systems and software applications, SCADA systems are subject to many vulnerabilities. According to [16], there were 135 public vulnerabilities notified for Industry Automation Control Systems (IACS) in 2015, compared to 35 for the previous year. This is also highlighted by the fact that attacks against SCADA systems are becoming more and more frequent on a global level, with factories, refineries and power plants being the most targeted. According to Dell, the number of SCADA attacks has increased from 91,676 in 2012 to 675,186 in 2014 and the countries with the most incidents were Finland, United Kingdom and United States of America (USA) [17]. The most often exploited vulnerability was buffer overflow, followed by the lack of input validation and the information exposure. The full spectrum of exploited vulnerabilities in this period is illustrated in Figure 4.1.

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

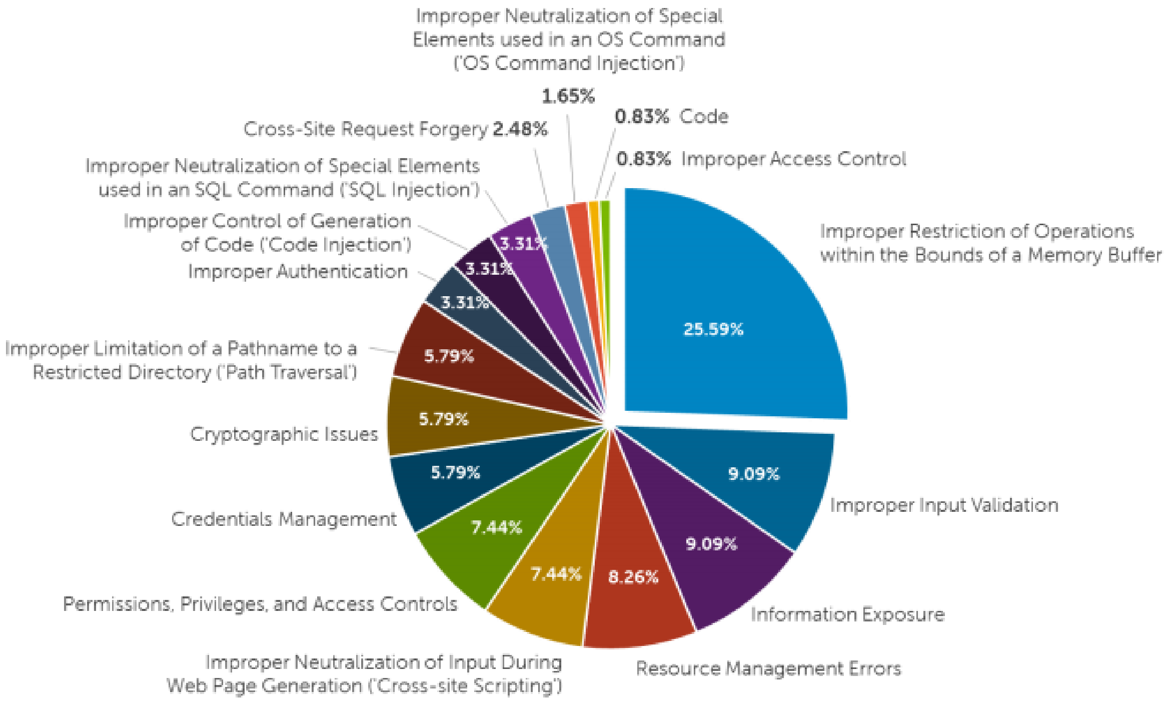


Figure 4.1: Exploited vulnerabilities between 2012 and 2014 [17].

4.1.2 Threats

Critical information systems are exposed to various threats that can be both of a cyber or a physical nature, as well as accidental or malicious. As such, their threat landscape consists of intrusions during data transfer, software and communication equipment malfunctions, field assets malfunctions, physical attacks (physical destruction of equipment), system intrusion, user errors and abuse of data. The reference documents provide lists of frequent threats that are relevant for the electricity sector which include physical attacks, accidental damage, natural or environmental disasters, failures or malfunctions of devices, systems and services, outages, interception, nefarious activity, and legal threats [18].

Considering IACS-SCADA, the threat landscape includes SCADA communication hacking, communication systems outages, user (insider) incidents, malware, exploit-kits, rootkits, distributed denial of service and data leakage. The threats of SCADA systems are related to vulnerabilities such as low use of intrusion detection systems, common vulnerabilities of ICT systems, low maintenance of firmware and software, legacy RTUs security vulnerabilities, weak authentication methods in place, general lack of understanding of SCADA system processes and operation and lack of training on cybersecurity by users, physical security of assets and other vulnerabilities.

Threats, of any nature, can often result in data exfiltration, alteration, removal, and system maloperation. Human error or bugs can occur due to poor training, applications development loopholes, monitoring issues, lack of maintenance. However, cyber threats are usually associated with malicious attacks, for example using malware or exploiting an inside error. Table 1 summarizes the types of cyber threats, their frequency, and their impact.

Hackers may want access for harmful purposes, although they are usually motivated by sordid gain. System control, extortion, theft, and intrusion are all connected with the term "hacking". On the other hand, terrorist attacks are usually associated with overt attacks as they are typically driven to cause damage to critical systems of particular services. Identification of threats also requires identification of possible actors that are capable to perform the attacks, have the available resources and the potential interest for the attack.

Table 1: Cyber threat types [19].

TYPE	OBJECTIVE	FREQUENCY	IMPACT
Overt attacks	Disrupt, destroy, frighten	LOW ↓ HIGH	HIGH ↑ LOW
Gain System Control	Remotely modify and operate the system		
Extortion	Criminal motivation for monetary gain		
Theft	Criminal motivation for monetary gain		
Intrusion	Unauthorized access to information and potential to exploit information		

Threats, which are typical for the electricity sector, include web-based attacks, malware, phishing, denial of service, insider threat, cyber espionage, ransomware, and botnet. According to [20], the TSOs are at high risk from malware, social engineering, including phishing and spam, insider threats, espionage, ransomware and botnet. The risks of web-based attacks are medium, while the denial-of-service threat risks are considered low. Besides web-based and denial of service, all other threats pose high risks for cascading. The risks for generation are relatively lower, with only high risks of ransomware, medium risks of espionage, ransomware, botnet and phishing and low risks of malware, denial of service and web-based attacks.

4.1.3 Current cyber incidents communication procedures

The company/system under attack should alert immediately the relevant national entities about the threats that become attacks. The NIS Directive sets the principles of cyber incidents notification and reporting as a crucial step in increasing the incident response capability on national and EU level. The main actors and roles in the process are entities designated as NCAs and Single Points of Contact (SPOCs) and national/sectoral CSIRTs who should cooperate with the OESs following a notification of an incident.

Three are the main steps for the mandatory notification and reporting requirements as defined in the NIS Directive [7]:

- OES shall notify the NCA and/or the national CSIRT on incidents that have a high impact.
- SPOC informs the SPOC of another EU MS when the incident has a high impact on that other EU MS.
- NCAs sent annual report to the NIS Cooperation Group on the incident notifications by OESs.

The principles on incident notification and reporting are also illustrated in Figure 4.2.

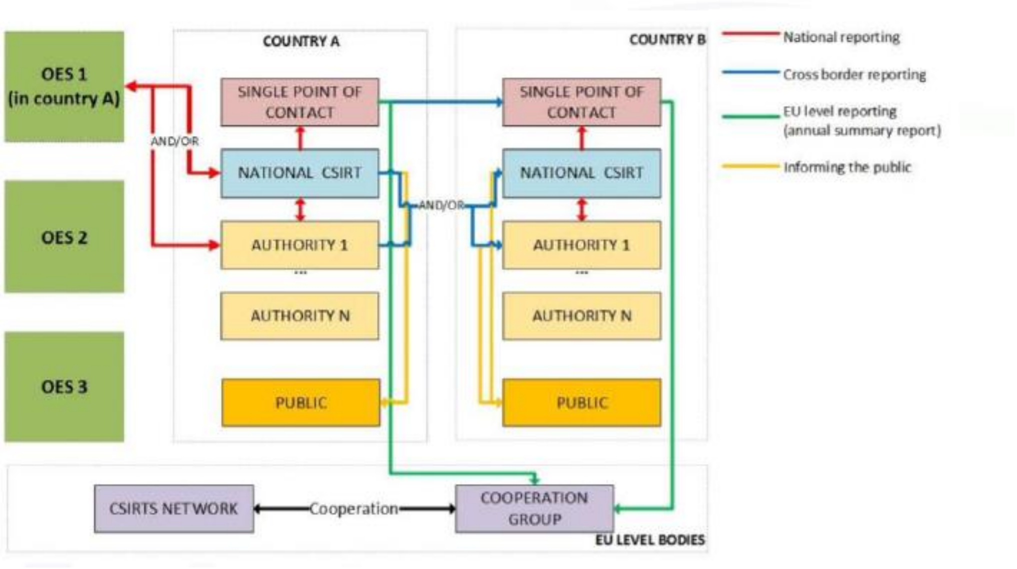


Figure 4.2: Incident reporting process for OESs [21].

It is essential that each EU MS appoints NCA or CSIRT to which an OES sends incidents notifications. The OES should comply with this requirement for the incidents that compromise the provision of their essential ser-vices. Furthermore, the OESs should be able to determine the significance of the incident based on several key parameters. These parameters include:

- the number of affected users by the incident, which actually means the number of users who have been affected by the disruption of the essential service provided by the OES,
- the duration of the incident, and

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

- the geographical area that is affected by the incident.

As presented in Figure 4.2, the national CSIRTs may send the OES technical information that could help the OES in responding to the incident. The national CSIRT or NCA may inform the public about an incident should it help in handling an existing, ongoing incident or help in preventing other incidents in the future.

However, the institutional set-up of the notification procedures depends on national circumstances and traditional governance models. The organizational set-up can be centralized, where a single entity is notified about the cyber incident. The decentralized approach is based on incident reporting by sectors – OESs report to a sectoral authority and the SPOC is the central location that collects information and contacts all authorities involved. Additionally, a mix of the previous approaches is implemented by some EU MSs, with one authority being responsible for several sectors and the rest of the sectors having their own sectoral authorities. The set-up influences the overall incident response capability on national level and should be built on previous experiences on crisis management and experiences on dealing with past incidents, which may not necessarily be cyber incidents. Relating incident communication requirements and practices is a complex task due to the variety of incidents and the split responsibilities among actors. The national legislation should clearly define roles and actors involved to provide unobstructed information flow and fast response upon incident notification.

The Guidelines on notification of OESs incidents published by the NIS Cooperation group provide notification methods, technical considerations, guidelines on cross-border information notification, procedures of annual reporting, information of the public and templates for notification. The overview of the general consecutive notification steps is presented in Table 2, and are based on the reference documents published by the NIS Cooperation Group [21].

Table 2: Incident communication procedures based on recommendations from [11], [21].

Cyber Incident notification steps		Actions
Determine significance (options)	Parameters	Use the set of three parameters proposed by NIS Directive: number of users affected by the disruption of the essential service; time duration of the incident; geographical area affected by the incident
		Use the set of three parameters proposed by NIS Directive: number of users affected

		by the disruption of the essential service; time duration of the incident; geographical area affected by the incident Use extended set of parameters
		Use sectoral parameters
	Threshold	General threshold (> of certain number of affected citizens)
		Sectoral/subsector thresholds
		No threshold
Alert notification	Notification method	Phone call, email, email w/o attachment, online form, web service, paper, multiple options
	Technical and security considerations	Encryption, authentication, confirmation
	Reporting template information (developed by NCA/CSIRT)	Nature of the cyber incident: type of threat (system failure, malicious actions)
		Impact - describe the severity including affected critical infrastructure and essential ser-vice, scale of the incident (for example use Traffic Light Protocol); geographic spread; number of affected citizens and duration (star of significant incident until the incident is no longer significant)
		Contact information: organization, contact point in the organization); other parties that may be involved
		Operational information: time of discovery; status (ongoing/resolved); incident details (malware, source (inside/outside)); ongoing/taken mitigation actions; support requests from national entities
		Information sharing: affected IT assets
		Ex-post sharing: mitigation actions taken; lessons learned
Notification confirmation	A system to confirm the notification should be in place at the relevant authority	
Follow-up notification	Using the same and/or additional means for notification the OES updates the NCA/CSIRT with relevant information during the incident. An ex-post incident is generally a requirement and should be submitted by the OES.	

Prior reporting the incident, the OES should assess the significance of the incident based on national set-up related to incident notifications. The challenge for operators might arise from the requirement to develop processes that will include fast incident impact analyses that should be applied together with the processes for incident handling. In fact, the procedures, and practices on organizational (TSO) level are essential to provide information on the ongoing incidents without undue delays. Based on the conducted activities for assessment of the significance and threshold of the incident, the OES notifies the relevant entity on national level.

The notification method may differ and depends on the set-up, but it is advisable to provide more than one notification method. This is especially important because during cyber-attacks, some of the IT systems might become unavailable, while traditional means of conveying notifications as telephone calls, may face overload of lines. All of the notification methods should be assessed together with the technical considerations for encryption, authentication, and confirmation. For example, on one hand, telephone networks have generally lower level of protection of information that is sensitive for the operator, but on the other hand they offer the possibility for direct communication and confirmation that the notification is received. The actual template depends on the national entity and the means of notification. It can be a checklist with questions that are answered over the phone or an online form that is checked/filled in. The process of confirmation is important to clarify that the notification has been received and to follow-up on the incident.

In the case of cross-border cyber incidents, the SPOC is obligated to communicate with the SPOCs of the other affected EU MSs. There is no proposed approach on the notification and exchange of information. However, there are several factors to be considered when developing cross-border notification procedures. These factors include:

- timely sharing of information which should get to the stakeholders that may be affected.
- establishing clear common procedures.
- coordination of the process by one of the actors involved.

The exchange of bilateral information may be based on the template used on national level and the procedures of information exchange should depend on the impact of the incident. The information exchange should be done carefully to preserve the confidentiality and the commercial interests of the OESs that have been affected. If not included as a part of a common procedure, the sender SPOC should provide detailed instructions on information handling to the receiver SPOC in order to ensure confidentiality.

For the purpose of increasing cybersecurity on EU level, the NIS Cooperation Group collects annual reports on notified incidents from EU MSs. The reports contain the information required in the notification template already described in *Figure 4.2*. The reports provide the basis to analyse trends in cybersecurity, improve incident response on EU level on the bases of aggregated data and create strategic overview of incidents [22].

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

4.2 Cyber incidents and threats impact analyses

The successful cyber-attacks in power systems have multi-fold effects. The disruption of the essential service is the first and most significant effect. The interdependencies with other sectors and services significantly increase the effects of cyber-attacks on power systems and energy systems in general. However, these effects cannot be easily quantified and qualified. The assessment of internal costs associated with a cyber-attack should be done by the companies that have been victims of the attacks and then, the analyses should be expanded to all other affected sectors and services. However, the companies are reluctant to disclose details of cyber-attacks as those damages their reputation, so the costs and the economic and societal effects of cyber-attacks can be accessed only roughly in most of the cases. The financial effects of undelivered electricity and potential equipment damage may be considerable, depending on the geographical spread of the incident and the targeted systems. The financial effects can be also measured by the downtime of equipment and the affected related services dependent on electricity supply. As the transmission networks are interconnected, a cyber-attack on one system can have a cascading effect and spread on neighbouring systems. The sense of insecurity and panic is the underlying element of many cyber-attacks, but the effect of cyber-attacks on power systems is even greater as many people may be affected. These events may diminish the trust in power systems and their capability to maintain continuous operation.

Table 3 depicts general vulnerabilities of the electricity sector and the potential impacts, based on the review conducted in [23]. With the general objective to increase the overall incident handling capability, the risk assessment of threats should also incorporate an assessment of the potential impacts that the attacks would have on the system. This approach would enable the companies to prioritize their cybersecurity investments and develop countermeasures that would mitigate the impacts of future attacks with high likelihood.

The attacks may have financial motives, especially industrial espionage, and data theft. Industrial espionage can be done by software that can copy plant configurations. Data theft and attacks on IACS may be motivated by financial gains, but they require significant technical knowledge in IT, automation, and energy (electricity) systems. The attacks through corporate networks using ransomware could possibly bring more financial benefits than attacks to IACS.

Table 3: Vulnerabilities and impacts in power systems, based on [23]

System segment	System	Risk	Potential Financial Impact	Other impacts
Electricity production units	Monitoring and dispatch systems	Medium	Equipment replacement	Loss of production unit, market disruption and loss of potential revenue for the producer

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

	SCADA	High	Investment loss, possible equipment replacement	Interrupted control functions, remote access to primary equipment for the attackers, loss of revenue.
Transmission /distribution system	Digital interfaces	High	Investment loss, equipment accountability, loss of revenue, possible equipment replacement	Unavailability to access various systems.
	IACS-SCADA	High	Investment loss, equipment accountability, loss of revenue, possible equipment replacement	Interrupted control functions, remote access and control of primary and secondary equipment in substations, possibility to cause equipment damage.
	Energy/Distribution Management systems	High	Investment loss, loss of revenue	Interrupted system operation and control, power outages and possibility for cascading effects, penalties.
	Smart metering systems	High	Loss of revenue for the affected trader/supplier	Meter tampering, possibility of faulty controls and outages, breach of data privacy for customers
Supply	Billing systems	High	Costs for lawsuits and dispute settlements	Damaged reputation for the company, breach of data privacy for customers

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

5. Cybersecurity Standards and practices in power industry

More important data is crossing communication networks, needing tighter security, thanks to intelligent distributed technologies that offer remote control, monitoring, and advanced analytics. Serial communications or a dedicated and isolated control and automation network were once the only options for utilities. More data have to be transported from the field to a central site, as device technologies progress and support for more advanced data processing methods are installed at field and central sites [24]. In a world with separate systems connected by a dedicated infrastructure, the electrical grid is far more vulnerable to cyber-attacks. As a result of changes such as energy deregulation and the growth of distributed energy resources (DER), a huge number of different actors are now involved in the operation of electric power networks, relying on both Operational Technology (OT) and ICT. Business and operational processes increasingly use standard ICT components, standardized IP-based protocols, and public communication infrastructure to communicate across the boundaries of OT actors and ICT assets [10].

5.1 National Frameworks for EPES relevant to OneNet project

The scope of the analysis in this section is limited to the national frameworks of countries participating in the four clusters of OneNet project will be conducted, i.e., Northern Cluster Demonstrator, Southern Cluster Demonstrator, Western Cluster Demonstrator, Eastern Cluster Demonstrator, particularly as they relate to the processing of personal data, information security and ethical requirements for conducting the demonstrators.

In the context of WP1 Ethics requirements, involved partners were asked to identify how all of the data they intend to process is relevant and limited to the purposes of the OneNet project (in accordance with the 'data minimization' principle). Consequently, as stated in D1.2 POPD-NEC-Requirement No.2:

"The OneNet partners from non-European countries can guarantee that all European data regulation are applied during the processing of personal data.

- Energoinfo (Serbia) develops an application as part of WP8. The application will exclusively process data that can be considered uncritical in the context of Protection of Personal Data (POPD).
- Piclo (United Kingdom) with their flexibility platform will process personal data of their residential flexibility provider. The United Kingdom as a former member of the EU applies the same data protection regulation as the EU.
- Nord Pool AS (Norway) is localized in Lysaker, Norway. Norway is not part of the EU but of the European Economic Area (EEA). The EEA applies equivalent data protection regulation as the EU. "

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

5.2 Global and European cybersecurity standards in energy automation

Interoperability of different vendors' products depends on cyber security standards to guarantee seamless interconnection and information exchange across the many actors and roles in energy automation systems. On the one hand, there are organizational and technical security needs, and on the other hand, there are technical security standards that provide specific technology solutions and methods for organizational and management components of the working environment.

Apart from standardization, another essential aspect is law, which is often country specific and addresses the safe operation of infrastructure. Existing Guidelines and Recommendations also detail recommended practices for the safe implementation and operation of energy automation systems. In an ideal world, standardization, regulation, and guideline activities all work together.

There is an extensive list of Cybersecurity standards specifically related the energy sector but not all the relevant standards are relevant for OneNet and in particular for data exchange.

Amongst those that should be considered and approached in the context of OneNet are:

- IEC 62351: Power systems management and associated information exchange – Data and communication security. This standard has been published to provide security recommendations for different power system communication protocols including IEC 61850,
- IEC 62443: This family of standards represents and international agreement on best practices regarding processes, techniques, and requirements for securing industrial automation and control systems,
- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Specifically, it defines the requirements for ensuring that systems are designed, implemented, operated, and maintained to provide the required safety integrity level,
- ISO/IEC 270xx: Information Security Management System; It includes a series of standard for the information security managements. Some of these, very generic and applicable to all kind companies (e.g., ISO/IEC 27001:2013 and ISO/IEC 27002:2013) but some others specialized in specific sectors, such as the ISO/IEC 27019, based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil, and heat, and for the control of associated supporting processes,

- **IEEE 1686:** Intelligent Electronic Devices (IED) Cyber Security Capabilities. This standard defines the functions and features to be provided in IEDs to accommodate critical infrastructure protection programs,
- **IEEE 1711.2-2019:** IEEE Standard for Secure SCADA Communications Protocol (SSCP). SSCP is primarily intended to protect serial SCADA communications, but can be applied to other serial communications, such as the maintenance ports of IEDs. SSCP is independent of the underlying communications link and protocol (e.g., Modbus, DNP3, IEC 60870- 5), and is appropriate for serial communications over leased lines, dial-up lines, multi-drop links, radio, power line carrier, fibre optic, etc.
- **IEEE C37.240**: Cyber Security Requirements for Substation Automation, Protection and Control Systems. It defined engineering practices that shall be achieved for high levels of cybersecurity of automation, protection, and control systems independent of voltage class or criticality of cyber assets. Cybersecurity includes trust and assurance of data in motion, data at rest, and incident response.
- **CEN/TR 17167:** Communication system for meters. This includes a standardization of communication interfaces for systems with meters and remote reading of meters for all kind of fluids and energies distributed by network. Secure communication covering data privacy as an inherent property, providing a scalable mechanism for security services, data integrity, authentication, and confidentiality.
- **NERC-CIP.CIP-002 and CIP-003 to CIP-009:** Critical Infrastructure Protection (CIP) cybersecurity Standards to protect bulk electrical systems. This family of the standards sets the requirements for cyber security categorization, security management control, personnel and training, electronic security parameters, physical security of power systems, system security management, incident reporting and response planning, and recovery plans.
- **IEEE P1402:** IEEE Draft Guide for Physical Security of Electric Power Substation. This guide describes recommended practices for the physical security of electric power substations. It addresses a number of threats, including unauthorized access to substation facilities, theft of material, and vandalism. It describes options for positive access control, monitoring of facilities, and delay/deter features which could be employed to mitigate these threats. The convergence of physical and cyber security means that IEEE Standard P1402 also is referenced in cyber security requirements. In fact, virtually all cyber security standards reference physical security.

5.3 Cybersecurity guidelines and recommendations examples

Below guidelines on how to address secure communication in certain application environments, in addition to rules and standards.

5.3.1 NISTIR 7628

The Cyber Security Working Group, which is part of the SG Interoperability Panel, is specified by the US National Institute of Standards and Technology (NIST). The "Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements" NIST Interagency Report (NISTIR 7628) offers a complete set of cyber security requirements. The paper is divided into three sections: strategy, security architecture and requirements, as well as supporting analysis and references. It specifies the standards for the smart grid information system as well as communication security [25].

5.3.2 SGIS Report

The document Smart Grid Information Security (SGIS) was prepared by European Committee for Standardization (CEN) - European Committee for Electrotechnical Standardization (CENELEC) - European Telecommunications Standards Institute (ETSI) Smart Grid Coordination Group under the Mandate M/490 [26] given to CEN, CENELEC and ETSI by the EC and the European Free Trade Association [27]. The goal of this report is to aid SG adoption in Europe by providing Smart Grid stakeholders with SG Information Security recommendations and standards.

SG services will be enabled by a secure information and communication system built into the key infrastructure of transmission and distribution networks, all the way down to connected properties SGIS paper outlines an analytic method that can be used to a variety of use cases and matched to standards development to fulfil security concerns. The security inquiry was closely linked to SGAM, which was developed by a different working group. The security subgroup's final report presents recommendations for security measures to be used in SGAM's various zones and domains.

Selected security standards are mapped to security standard areas, as shown in *Figure 5.1*, under the following terms [27]:

- **Details for Operation:** The standard focuses on organizational and procedural tools that can be used by all or a subset of actors. It may contain implicit system and component requirements without addressing implementation possibilities.

- **Relevance for Products:** The standard has a direct impact on component and/or system functionality, and it should be considered throughout product design and development. It is concerned with the technology that will be utilized to integrate a security measure.

- **Design Details:** For standards on a technical level, the standard outlines the implementation of security means in sufficient detail to achieve interoperability between different vendor's products, and/or processes to be followed for standards addressing organizational means.

- **Completeness:** The standard covers the entire security framework, including technical and organizational measures, rather than just one specific security measure.

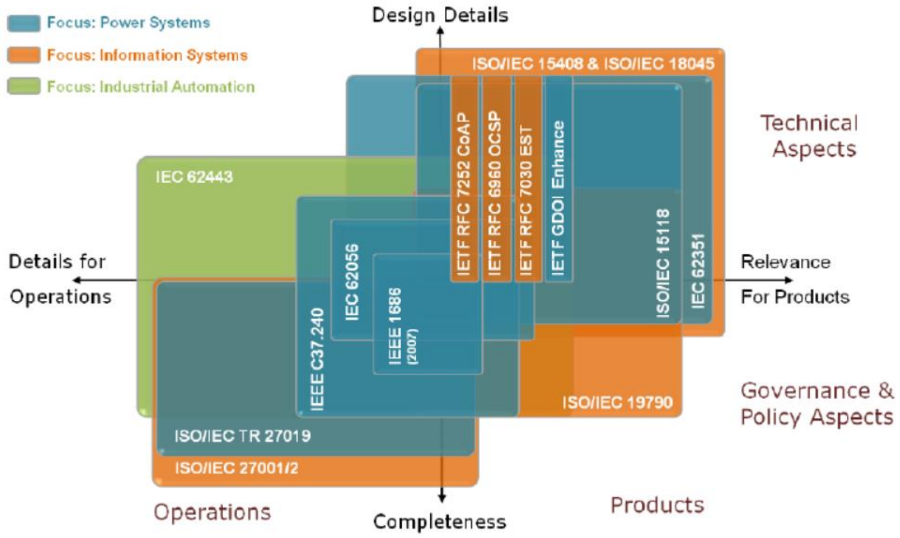


Figure 5.1: Security Standard Coverage Source: CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, 2014 [27].

The origin domain of the considered standards is indicated by the colour code in the Figure 5.1 based on the colouring, it is clear that for SGs, standards from many domains are applicable. Figure 5.1 depicts the application and scope of each of the standards examined by the SGIS during this working period from a somewhat different perspective. The following are the differences in the drawing:

- **Guideline:** The document contains security implementation guidelines and best practices. This could also include pre-requisites that must be met before the implementation can begin.

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

- **Requirement**: The paper contains generic product, solution, or process requirements. There is no implementation information available.
- **Realization**: The document explains how to put security measures in place (specific realizations). If possible, note how the document's level of detail rises from the left to the right side of the column.
- **Vendor**: Technical features of products or components are addressed in the standard.
- **Integrator**: Integration elements that have repercussions on technical design, are relevant for vendor procedures (need particular features to be supported) or require product interoperability are addressed in the standard (e.g., protocol implementations).
- **Operator**: The standard addresses operational and/or procedural features that are primarily concerned with the realization and provisioning on an operator's site.

Some standards only cover a portion of a vertical region. Partially covered means that the standard may not contain explicit requirements for the vendor, integrator, or operator. On an abstract level, standards covering many horizontal areas address requirements and propose solution options. Additional standards or guidelines may be required for implementation.

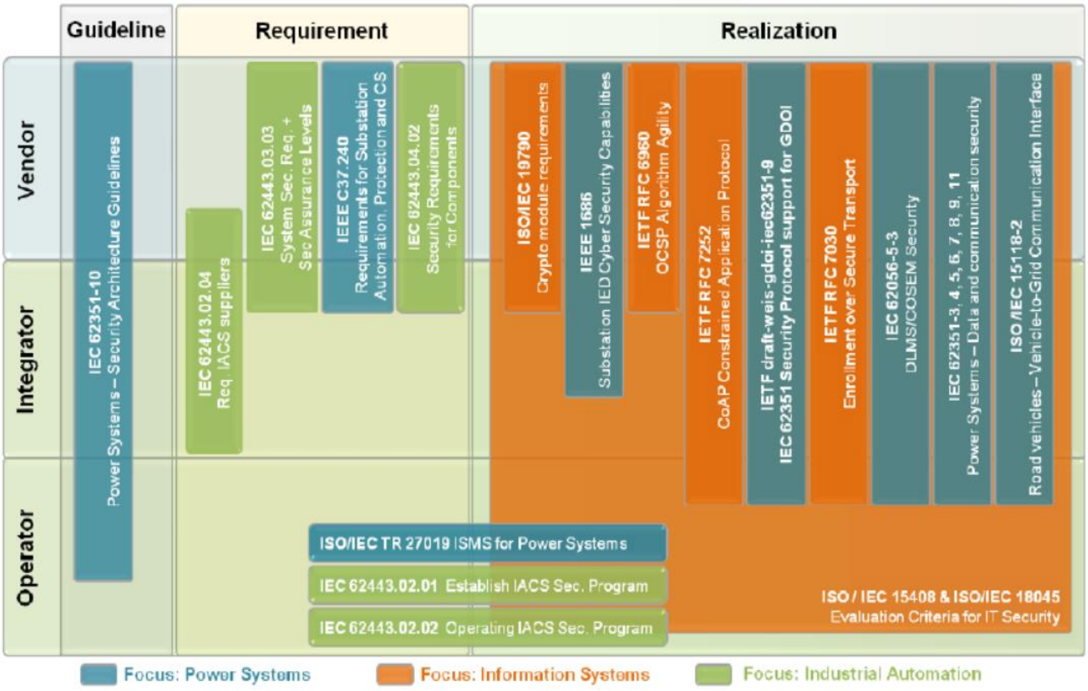

Guideline
Requirement
Realization
Vendor
Integrator
Operator
IEC 62351-10 Power Systems – Security Architecture Guidelines
IEC 62443.02.04 Req. IACS suppliers
IEC 62443.03.03 System Sec. Req. + Sec Assurance Levels
IEEE C37.240 Requirements for Substation Automation, Protection and CS
IEC 62443.04.02 Security Requirements for Components
ISO/IEC 19790 Crypto module requirements
IEEE 1686 Substation IED Cyber Security Capabilities
IETF RFC 6960 OCSP Algorithm Agility
IETF RFC 7252 CoAP Constrained Application Protocol
IETF draft-weis-gdoi-iec62351-9 IEC 62351 Security Protocol support for GDOI
IETF RFC 7030 Enrollment over Secure Transport
IEC 62056-5-3 DLMS/COSEM Security
IEC 62351-3, 4, 5, 6, 7, 8, 9, 11 Power Systems – Data and communication security
ISO/IEC 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface
ISO/IEC TR 27019 ISMS for Power Systems
IEC 62443.02.01 Establish IACS Sec. Program
IEC 62443.02.02 Operating IACS Sec. Program
ISO / IEC 15408 & ISO/IEC 18045 Evaluation Criteria for IT Security
Focus: Power Systems
Focus: Information Systems
Focus: Industrial Automation

Figure 5.2: Security standard applicability. Source: [27].

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

Some standards only cover a portion of a vertical region. Partially covered means that the standard may not contain explicit requirements for the vendor, integrator, or operator. On an abstract level, standards covering many horizontal areas address requirements and propose solution options. Additional standards or guidelines may be required for implementation. Furthermore, the use case specific analysis permits pointing to additional standards that are appropriate but not explicitly included in the study.

5.4 Key actors and roles

The key actors identified in the cybersecurity aspect are the following ones:

ENISA: ENISA is the EU cybersecurity agency entrusted with assisting and promoting the development and implementation of EU cybersecurity certification policy, including the development of candidate certification schemes and the publication of guidelines in this field. ENISA is in charge of creating several cybersecurity certification schemes and has released the Common Criteria for the European candidate cybersecurity certification scheme (EUCC scheme) [28]. It is also launching a public consultation on a draft EUCC scheme for Cloud Services, which focuses on cybersecurity certification throughout the cloud services chain. ENISA is also responsible for the upkeep of a dedicated website with information on European cybersecurity certification systems.

Conformity Assessment bodies: After being accredited by national accreditation organizations in accordance with Regulation (EC) No 765/2008, conformity assessment organizations will immediately execute certification operations. Only if the conformity assessment body achieves the requirements will it be granted accreditation, which will be valid for a maximum of five years and can be renewed [28]. When a certifying organization violates or fails to meet accreditation conditions, accreditation may be suspended or revoked.

Stakeholders Cybersecurity Certification Group (SCCG): The Stakeholder Cybersecurity Certification Group is an advisory and support group comprised of fifty organizations representing various industries. The group provides strategic cybersecurity certification advice to the European Commission and ENISA, as well as assisting the Commission in the preparation of the URWP [29].

European Cybersecurity Certification Group (ECCG): Within the cybersecurity certification system, the European Cybersecurity Certification Group serves as an advising and supportive body, including adopting an opinion on a candidate scheme produced by ENISA. Representatives of national cybersecurity certification authorities or other relevant national authorities make up the group. Stakeholders and other interested parties may be invited to ECCG meetings and to participate in its activities [29].

European Commission (EC): The European Commission has a number of responsibilities under the certification framework, including publishing a Union rolling work program for European cybersecurity certification. A list of ICT products, services, and processes that could be included in the scope of a European cybersecurity certification scheme will be included in the rolling work program, which will define strategic priorities for future schemes (CSA Art. 47). On the basis of the Union's rolling work program, the EC may ask ENISA to create a candidate scheme or assess an existing European cybersecurity certification scheme. The Commission will assess the efficiency and use of the adopted European cybersecurity certification schemes on a regular basis, as well as whether a specific European cybersecurity certification scheme should be made mandatory through relevant Union law in order to ensure an adequate level of cybersecurity and improve the internal market's functioning (CSA, Art. 56(3)).

Ad hoc working groups: ENISA has the option of forming ad hoc working groups to address specific difficulties in scientific, technical, legal, or socioeconomic topics, such as the development of a specific candidate European cybersecurity certification scheme. Members of these ad hoc working groups will be chosen based on their competence in network and information security from both the public and commercial sectors, including Member States competent authorities or bodies, industry, users, and academic experts. Some ad hoc working groups have been established so far, such as the ad hoc working group on the SOGIS-MRA certification framework's transposition and the ad hoc working group on cloud services. Some ad hoc working groups have been established so far, such as the ad hoc working group on the SOGIS-MRA certification framework's transposition and the ad hoc working group on cloud services.

National cybersecurity certification authority (NCCA): Each MS must appoint one or more national cybersecurity certification agencies to carry out supervisory functions, including those relating to certification schemes. These authorities must be self-contained in carrying out their responsibilities. The NCCA is a member of the ECCG. The NCCA's responsibilities include monitoring and enforcing the duties of manufacturers or providers of ICT products, services, or processes within their jurisdiction that conduct conformance self-assessment and the appropriate European cybersecurity certification schemes, as well as deal with complaints from natural or legal persons about European cybersecurity certificates within their authority. They also have the authority to conduct investigations, such as audits of conformity assessment organizations, holders of European cybersecurity certificates, and issuers of EU statements of conformity, as well as to revoke certificates and levy penalties.

Manufacturers and providers of ICT products, services, and processes: The Cybersecurity Act (CSA) addressees who can apply for certification are listed here. Manufacturers of ICT equipment and devices, developers, ICT service providers such as cloud service providers, integrators, and process developers are among them.

5.5 Conclusion regarding cybersecurity standards, guidelines, and regulation in energy automation

Over the last few decades, power systems' reliance on ICT has grown significantly, transforming them into complex infrastructures that transfer data in order to apply advanced control functions that, in turn, improve the security of operation and the continuity of electricity supply for customers. Although the process of digitalizing power systems is still ongoing, its consequences have altered the cybersecurity landscape and increased the risks of disruptions in critical infrastructure services.

Crucial infrastructure, according to EU legislation and specifically Directive 2008/114/EC, refers to assets and systems that are critical to citizens' well-being. These systems' failure would have a substantial influence on citizens' safety and security, as well as their health, economic, and social activities. Electricity transmission systems are regarded as vital since their operation has a direct impact on all of the functions listed above. Furthermore, breakdowns in interconnected transmission systems may affect multiple countries, escalating the system's and society's repercussions and costs.

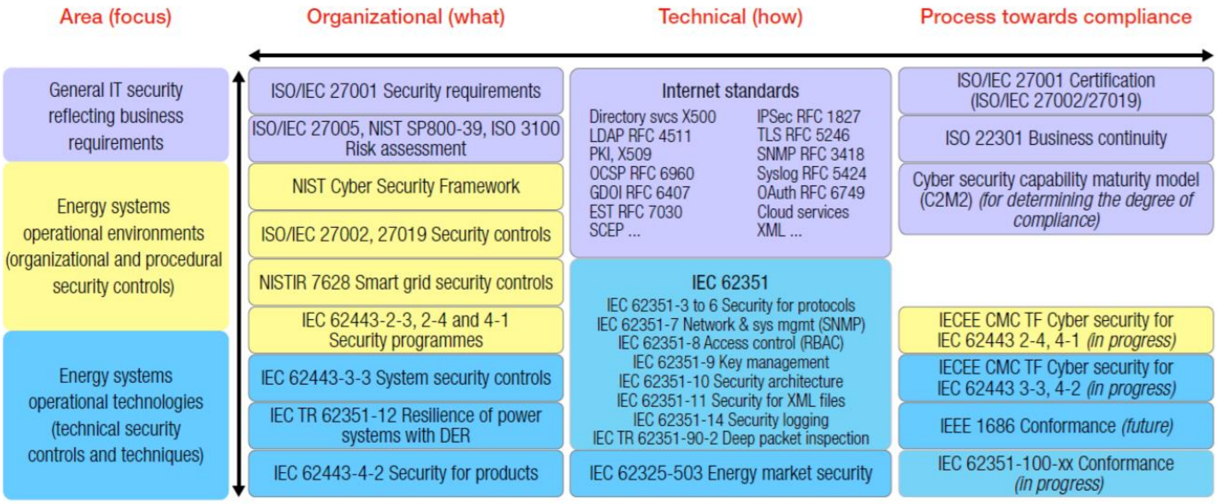
Successful cyber-attacks on power systems have a multiplicity of consequences. The first and most severe effect, given the interdependencies with other services, is the disruption of the critical service that electricity utilities provide. Depending on the spatial effect of the incident and the targeted systems, the cost effects of undelivered electricity and probable equipment damage could be significant. Due to the interconnected nature of the transmission networks, a cyber-attack on one system can have a cascading effect and spread to neighbouring systems. Many cyber-attacks are fuelled by a growing sense of vulnerability and terror.

Transmission systems rely on both legacy systems and modern technology to operate safely and reliably. To maintain the secure and reliable operation of the transmission systems, the current power infrastructure is coupled with sophisticated control systems and intelligent components with bi-directional communication capabilities. Cyber security threats are evolving, necessitating the deployment of sufficient protective mechanisms that match the multi-actor environment of today's power systems. To provide seamless interconnection and information exchange between the many players and roles in energy automation systems, Cyber Security Standards are a requirement for interoperability of different vendors' products. On the one hand, there are organizational and technical security requirements, and on the other hand, there are technical security standards that provide specific technology solutions and methods for organizational and management components of the operating environment [10], as indicated in the preceding subsections of this deliverable. Also, there are a number of cyber security-related regulations and guidelines that apply to energy automation, focusing on technological and organizational security measures. Despite the fact that there is no single comprehensive

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

standard or norm encompassing all aspects of cyber security, the industry is converging on a small number of standards that are gaining increased acceptance worldwide, as shown in Figure 5.3.

The North American Electric Reliability Corporation (NERC), that is presented in this section of the document, confirms the strong link between cyber security and power system resilience when they state that resilience is a component of reliability in relation to an event, and that cyber security is a key issue to reliability as stated in the NERC CIP regulation CIP-008-5 stating requirements for "Cyber Security - Incident Reporting Response Planning", for example. The Cyber Security Task Force of the IEC System Committee Smart Energy has chosen a set of international standards that apply to smart energy operational environments to assist energy operators in implementing their cyber resilience. A series of standards are illustrated in Figure 5.3. System integrators and device manufacturers must combine organizational security controls with technical controls to be implemented at both the system and product level. Technical controls (third column in Figure 5.3) are implemented based on standards published by Internet-related organizations and energy-related committees. This demonstrates the convergence of IT and OT technologies, as well as the necessity to make them interoperable, an issue that is becoming increasingly important as open platforms based on IoT technologies, as well as edge and cloud-based services, are deployed.



Area (focus)	Organizational (what)	Technical (how)	Process towards compliance
General IT security reflecting business requirements	ISO/IEC 27001 Security requirements ISO/IEC 27005, NIST SP800-39, ISO 3100 Risk assessment	Internet standards Directory svcs X500 LDAP RFC 4511 PKI, X509 OCSP RFC 6960 GDOI RFC 6407 EST RFC 7030 SCEP ... IPSec RFC 1827 TLS RFC 5246 SNMP RFC 3418 Syslog RFC 5424 OAuth RFC 6749 Cloud services XML ...	ISO/IEC 27001 Certification (ISO/IEC 27002/27019) ISO 22301 Business continuity Cyber security capability maturity model (C2M2) *(for determining the degree of compliance)*
Energy systems operational environments (organizational and procedural security controls)	NIST Cyber Security Framework ISO/IEC 27002, 27019 Security controls NISTIR 7628 Smart grid security controls IEC 62443-2-3, 2-4 and 4-1 Security programmes	IEC 62351 IEC 62351-3 to 6 Security for protocols IEC 62351-7 Network & sys mgmt (SNMP) IEC 62351-8 Access control (RBAC) IEC 62351-9 Key management IEC 62351-10 Security architecture IEC 62351-11 Security for XML files IEC 62351-14 Security logging IEC TR 62351-90-2 Deep packet inspection	IECEE CMC TF Cyber security for IEC 62443 2-4, 4-1 *(in progress)*
Energy systems operational technologies (technical security controls and techniques)	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 62325-503 Energy market security	IECEE CMC TF Cyber security for IEC 62443 3-3, 4-2 *(in progress)* IEEE 1686 Conformance *(future)* IEC 62351-100-xx Conformance *(in progress)*

Figure 5.3: Key cyber security standards and guidelines (source: IEC Technology Report: Cyber security and resilience guidelines for the smart energy operational environment).

6. Cybersecurity Survey

This section presents the results of a cybersecurity survey distributed amongst ONENET partners directly engaged in the demonstration activities, i.e., partners contributing to demonstration WPs 7 to 10. The questionnaire can be found in Appendix.

6.1 Rationale

The purpose of this survey is to contact various industries to address what is the current status of the organizations regarding the business and legal standards, and regulations in the aspect of cybersecurity. The results presented below, give us an insight into the information security maturity of organizations participating mainly in the demonstration clusters (WP7-WP10), with a focus on cybersecurity, and how this aspect is incorporated in the OneNet project. For the distribution of the questionnaire, the google docs tool was leveraged. Due to the criticality of this domain, it has to be explicitly mentioned that during the answers collection and analysis process, the identity of respondents as well as the organization's name they represent, remained unknown. Hence, vulnerable information, such as the organization's identity and personal data of the respondents, are not revealed in this document. Most of the presented questions gave the opportunity to the respondents to select multiple answers, and to provide any additional input they thought was applicable for each question, in order to enrich the outcome of this work. In total 24 responses were received, representing 24 different organizations directly engaging in the demonstration activities of the OneNet project.

6.2 Results about organizations view on cybersecurity

In the beginning of the survey, each participant was asked to provide information, regarding the domain that the company he/she represents belongs to, and the amount of the employees in the IT department. As can be seen in *Figure 6.1*, 66% of the participants in this survey represent System Operators (SOs), i.e., either Transmission System Operators (TSOs) or Distribution System Operators (DSOs), followed by technology providers in the energy domain, Market Operators (MOs), Energy Service Companies (ESCOs), and research organization. Besides this information, no other sensitive identity data was requested. More than 60% of the companies have an IT department employing more than 15 employees, highlighting the expertise that the companies participating in OneNet Demos have.

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

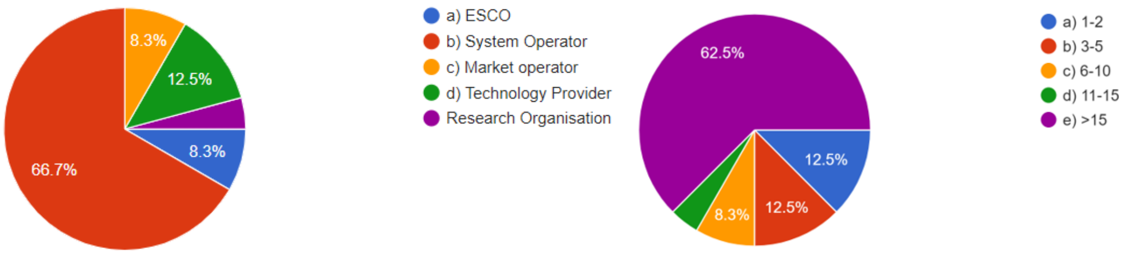
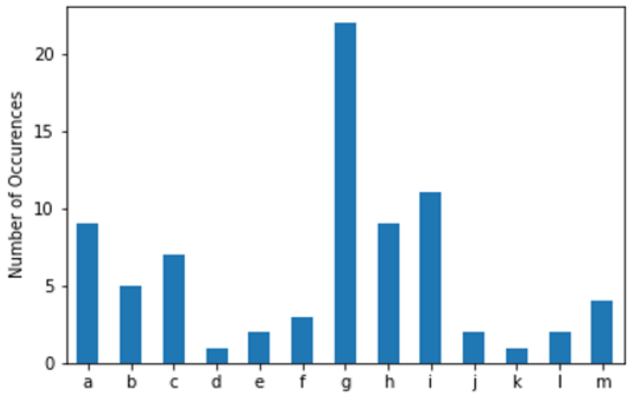


Figure 6.1: Left: Profile of the participants in the questionnaire. Right: answers to the question "How many people does your IT-department employ?".

In order to assess the level of knowledge regarding cybersecurity issues, and to showcase how frequent and crucial is security aspect in organizations, regardless the magnitude of the organization and the engaged domain, the participants were asked about the incidents occurred in their organizations the last year timespan. Figure 6.2 depicts that more than 90% and 50% of the participants stated that spam emails and emails impersonating organization, respectively, were the most common identified security breaches. Other occurrences that reported were weakness highlighted during testing, redirection to fraudulent websites, and malware/viruses. It is important to highlight that only 16% of the respondents answered that under their knowledge, their organization has not been exposed to hacking the last year.



a) Weaknesses highlighted during testing

b) Lost assets (lost/stolen laptops or memory cards)

c) Malware or viruses

d) Hacker attacks

e) Ransomware

f) Denial-of-service attacks

g) Spam emails

h) Redirection to fraudulent websites

i) Impersonating organisation in emails

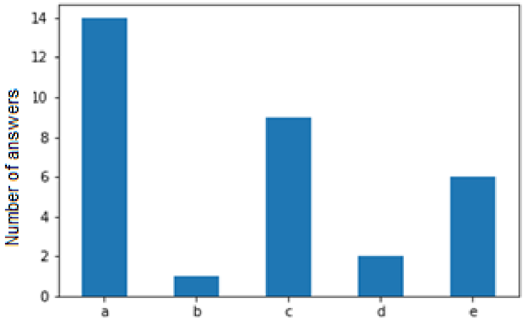
j) Unauthorised use of computers networks or servers by outsiders

k) Unauthorised use of computers, networks by staff

l) Any other breaches or attacks

m) We were not exposed to hacking

Figure 6.2: Number of security breaches occurred in the last 12 months in the respondents' organization.



a) ISO/IEC 27019

b) Critical Infrastructure Protection
IEC62443
ISO 27001
ISO 27001/27002, NIST CSF
In the process of getting ISO27001 certification
NIST DP 800-53
NIST Framework
Outsourcing these services
Yes, COSO ERM
Yes, IEC 62351
Do not know
Yes, NISTIR 7628
No

c) Regulatory standards

d) ISO 31000
COBIT

e) ITIL

Figure 6.3: Management and risk assessment processes organization of the respondents utilize for security.

In order to tackle the above-mentioned security breaches, the organizations participated in the survey apply multiple methods. As can be seen in Figure 6.3 , almost 60% of the organizations respond that they utilize the ISO/IEC 27019. In addition to that, 40% of the organizations use regulatory standards as a procedure for management and risk assessment.

Regarding the assessment of the most vulnerable parts of the organization towards cybersecurity attacks, 90% of the respondents replied that OT, ICT, and policies are the most sensitive. Other parts such as supply chain and people recognized as the most vulnerable. Figure 6.4 illustrates that the employees in 95% of the organizations feel secure at least to a certain extent. Potentially this can be explained also from the analysis of the bottom graph in Figure 6.4, which depicts that in 20 out of the 24 examined organizations, there exists a training process which aims to increase the cybersecurity awareness of the employees. Several methods were identified by the partners and incorporated in Table 4. Significant part of the increased awareness regarding cybersecurity subjects in the organizations participating in the survey, is also due to the fact that several ways are used in order to be informed for new forms of information security attacks and threats. As observed in Figure 6.5, the most used ways are information deriving directly from vendors, external consultants, news from media, associations etc., and participation in security conferences.

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

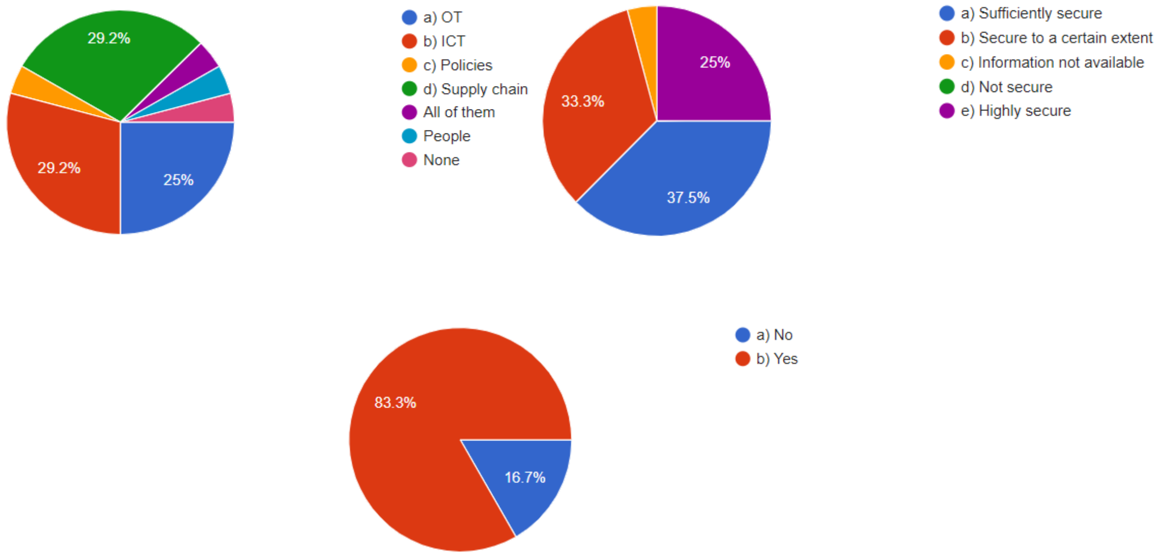
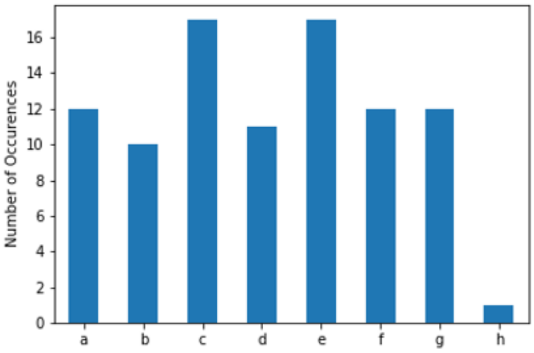


Figure 6.4: **Upper Left:** Identification of the organizations' biggest vulnerabilities; **Upper Right:** Level of security in the organizations; **Bottom:** Answers to the question regarding existence of training process in the organization to enhance cybersecurity awareness.

Table 4: Training methods about enhancement of cybersecurity awareness in the organizations participating in the demonstration activities.

Cybersecurity awareness training methods
SANS newsletters
ISACA tutorials
No standard methodology, just following recommendation by the national organisms, such as INCIBE, CCNCERT
NIST
Online courses, such as walk-in-centre etc.
Cyber circle
In-house methodology is used



a) Consulting firms/ external consulting

b) Scientific publications

c) Providers (vendors)

d) Social network

e) News on websites / blogs / from professional associations

f) Security conferences

g) Mailing lists

h) No, I do not get regular updates regarding security attacks and threats.

CERT Network

CIRT, Forums

Cybersecurity is dealt with by other branches of our organization

National cybersecurity agency

Figure 6.5: Participants answers regarding the way they are informed about new forms of information security attacks and threats.

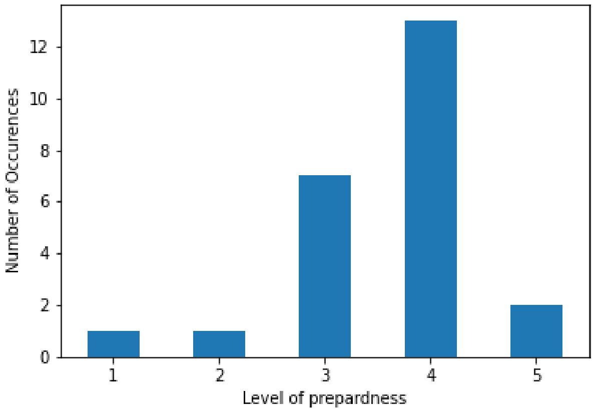
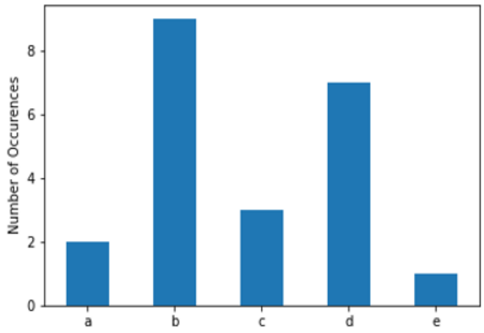


Figure 6.6: Answers to the question: " On a scale of 1 (“lowest”) to 5 (“highest”), how prepared is your organization to respond to a cybersecurity incident?".

Besides the analysis regarding the cybersecurity awareness of the organizations, it is important to point out at this point, that 60% of the respondents replied that their company is at least 80% prepared to respond properly to a cybersecurity incident. From the plethora of the industrial protocols used in Utilities and ESCOs to manage their infrastructure, IEC 61850 protocol was identified as the most vulnerable towards potential cyber-attacks. Figure 6.7 illustrates the responds of the partners for this subject.



a) IEC 62351
IEC 61850-7-410
IEC 61850-7-420
IEC 60850-5-102

b) IEC 61850
IEC 60870-5-101/104

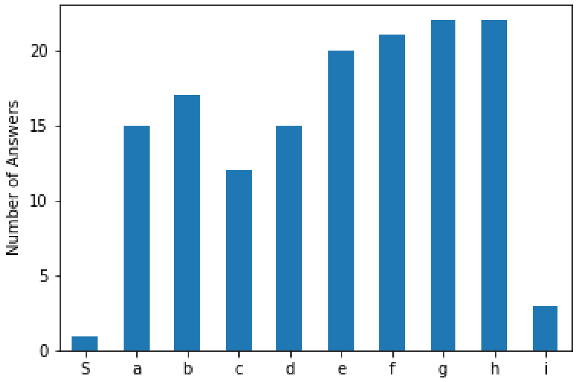
c) DNP3

d) Modbus

e) DNS
NA
Confidential
IT-focused

Figure 6.7: Answers to the question "Which industrial protocols used by your organization/environment are considered as vulnerable".

As Figure 6.8 illustrates, more than 85% of the organizations under question use firewalls, antivirus, intrusion detection systems and anti-spam solutions for protection against attacks. Other solutions such as Security Information and Event Management, data loss prevention and safety endpoints were also broadly used amongst the organizations.



a) Safety endpoints

b) Managing event logs (solutions SIEM (Security Information and Event Management))

c) Data Loss Prevention / file encryption (memory)

d) Vulnerability Management

e) Intrusion Detection Systems / Intrusion Prevention Systems

f) Anti-spam / spyware / phishing solutions

g) Firewalls

h) Antivirus

i) Information not available

Figure 6.8: Security measures implemented by the organizations.

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

One important aspect that has to be considered during the process of the cybersecurity requirements definition, is which threats/attacks the experts of the energy industry think are the most critical. From the pie chart presented in Figure 6.9, 30% of the replies concerned ransomware as the most critical threat, followed by insider attack, which was selected by a quarter of the respondents. Other threats, such as denial of service and spear phishing were also identified.

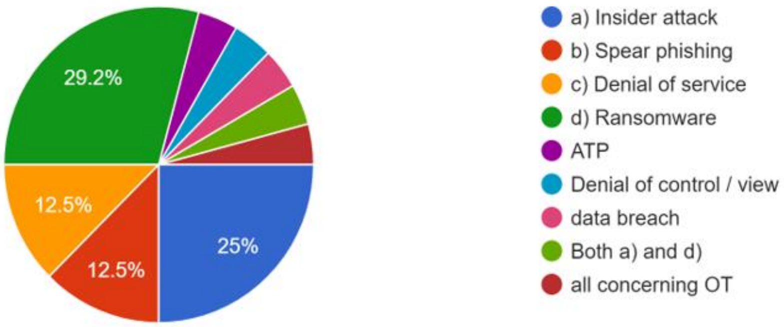


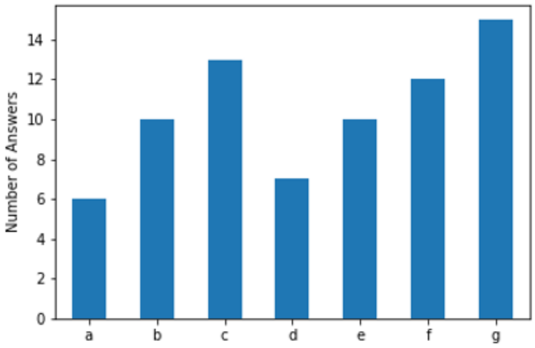
Figure 6.9: Threats/attacks identified as the most critical for the industry.

6.3 Cybersecurity view of organizations about OneNet DEMOS

In order to create a concrete list of cybersecurity requirements for the OneNet project, it is important to grasp the view of the organizations directly engaging in the demonstration activities, regarding the cybersecurity aspect. Therefore, the partners asked to assess which area of the energy domain they consider as the most vulnerable to cyberattacks. More than 60% of the respondents think that data management platforms are the most exposed to attacks. As depicted in Figure 6.10, all the different parts of the power system from the very low voltage level (distribution grid) to the very high voltage level (transmission system), were considered to be weak to cyberattacks. Control and automation processes in the Utilities and ESCOs were identified as the areas in high danger. A crucial aspect that has to be highlighted is also the security in the end-customer premises, due to the

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

fact that many respondents recognized it as a vulnerable area in the energy domain, along with the energy markets (platforms, data storage, data exchange amongst the participants etc.).



a) Generation

b) Transmission

c) Dispatching, control, and supervision (SCADA, RTU, PLS)

d) Distribution

e) Energy Market

f) End-customer premises

g) Data management platform

Figure 6.10: Areas recognized as the most vulnerable to cyber-attacks.

Table 5: Assets identified by respondents as the most critical in the demonstration activities.

Assets identified as critical regarding cybersecurity in the Demos	
SCADA / EMS	Databases in general and client data
Grid monitoring equipment	User Behaviour Analytics (UBA)
Domain Controllers	Mobile device management (MDM)
APIs and Interfaces between operations and external applications.	Availability of web platforms and trading data managed in those platforms
Software, such as flexibility platform which shall be accessible from Internet	Energy management software and messaging
Substation automation	Telecommunication network
Billing system	Smart metering system

In addition to the previous question, an important exercise was conducted in the context of this survey. The respondents had to identify specifically the assets that will be used in the demonstration activities and are critical regarding the cybersecurity. As can be observed in Table 5, both software and hardware infrastructures communicating with/be part of the OneNet architecture or will be developed as a component of the cluster demonstrators, were reported (see chapter 7 for more information about the OneNet architecture). Regarding the software developments, the security of flexibility platforms and the interfaces between the intrinsic operations in each demo and external platforms (applications), were highlighted as the most crucial. Regarding the hardware infrastructure, legacy systems utilized by the Operators and ESCOs for the proper operation of their networks and energy assets, respectively, such as automation in substations, SCADA, domain controllers, and smart metering system, were reported as the most critical. Besides those, the criticality of the database infrastructures was pointed out, due to the sensitivity of the data stored, such as smart metering data, end-customer personal data, market-related data etc.

Malicious cyber-attacks may target power system balancing and frequency control mechanisms, generating anomalies in real-time measurements of several variables in the power system. Most of the participants in the survey considered anomalies due to cyber-attacks as the most critical.

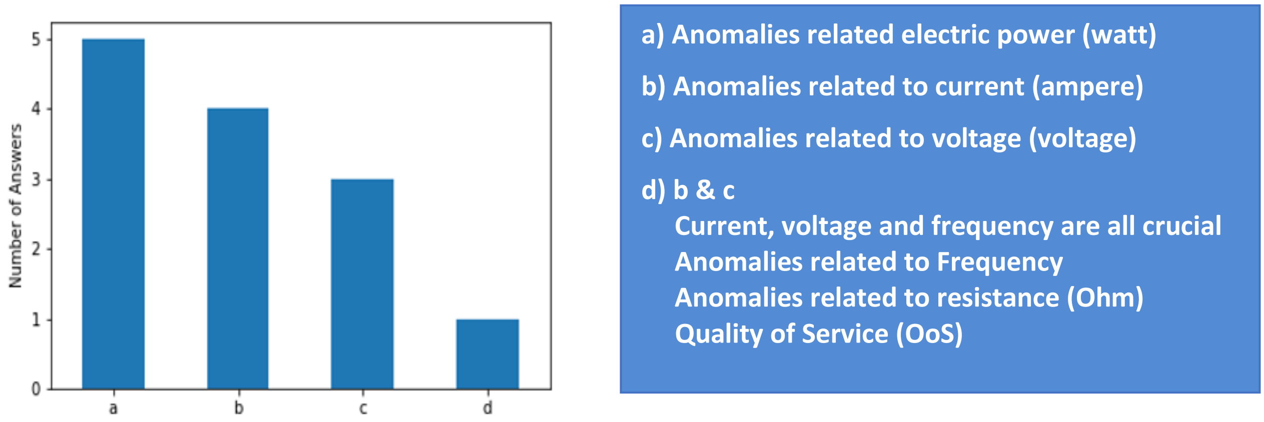


Figure 6.11: The anomalies considered by the partners as the most critical in the electrical grid.

In order to assess the importance of intrusion detection in the power systems, the response time of the organizations in the power industry was questioned. Stability and security are critical elements for the proper operation of the power system, and this must be ensured through the quick response to attacks. As Figure 6.12 illustrates, almost 50% of the organizations replied that the intrusion detection systems shall be able to respond from seconds to minutes time scale. The rest 30% of the participants answered that intrusion detection shall take place in hours after the threat occurs.

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

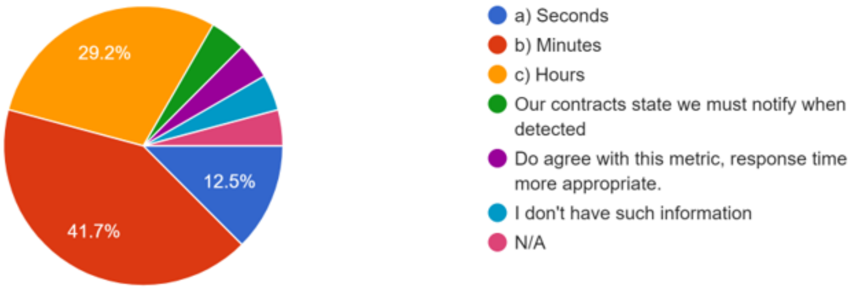


Figure 6.12: Maximum time scale interval in which an intrusion must be detected inside the organization.

Firewalls and access control lists were recognized as the most dominant ways that organizations utilize to mitigate network attacks in the infrastructure and their customers. Almost 80% of the organizations leverage commercial products for attack detection, showcasing the preference to established and guaranteed practices. Open-source software and in-house developed tools are also leveraged in about a half of the companies participating in the demonstration activities of the OneNet.

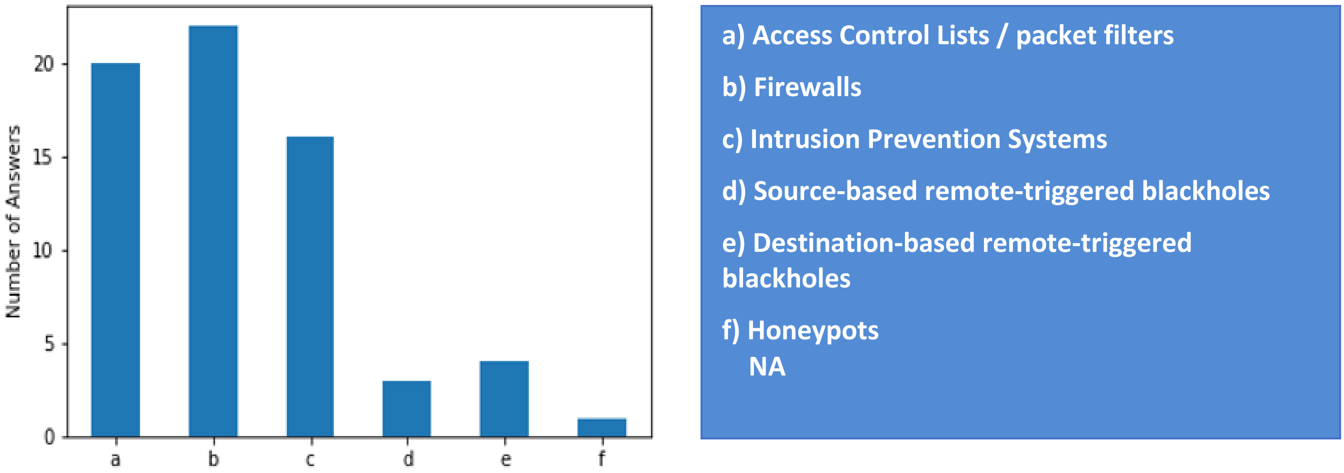


Figure 6.13: Measures used to mitigate network attacks in the organization's infrastructure/customers.

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

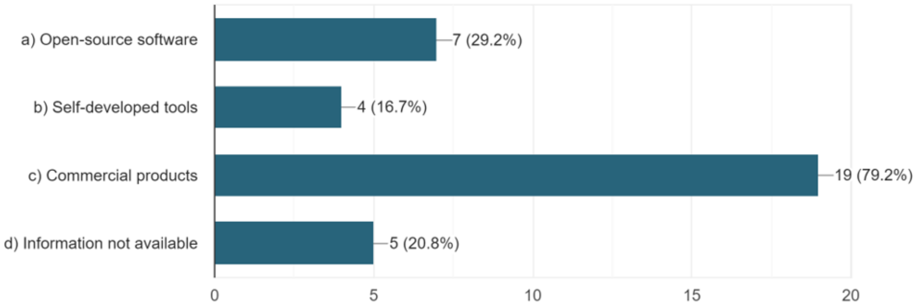


Figure 6.14: Tools used for attack detection, as identified by the partners.

6.4 DPO in OneNet project

Besides the previous parts of the survey that mainly strive to address the issue of cybersecurity, additional information was requested to identify whether a data protection officer (DPO) will follow up the activities of the companies in the OneNet project.

As mentioned by European Data Protection Supervisor [2]:

"The primary role of the DPO is to ensure that her organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. In the EU institutions and bodies, the applicable Data Protection Regulation (Regulation (EU) 2018/1725) obliges them each to appoint a DPO. Regulation (EU) 2016/679, which obliges some organizations in EU countries to appoint a DPO, will be applicable as of 25 May 2018."

From the answers received, 14 out of 24 replied either that they already engage, or they are willing to engage a DPO for the activities of the OneNet project. Moreover, several national data protection supervisory authorities of the companies participating in the Demos are incorporated in Table 6. An additional information that was requested from the partners is whether they are informed about DPIA, which stands for Data Protection Impact Assessment; a process that provides sufficient help about identification and minimization of the data protection risks in the context of the project, and guidance to help ensure the fundamental rights to protection of personal rights. Specifically, for projects closely related to energy domain, the Smart Grid task force has created the DPIA Template, an evaluation and decision-making tool which helps entities engaging in smart grids planning or executing investments to identify and anticipate risks to data protection, privacy and security. Regarding the

[2] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

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

demonstrators of OneNet, only one of the respondents replied positively to that request, showcasing the lack of awareness regarding this process.

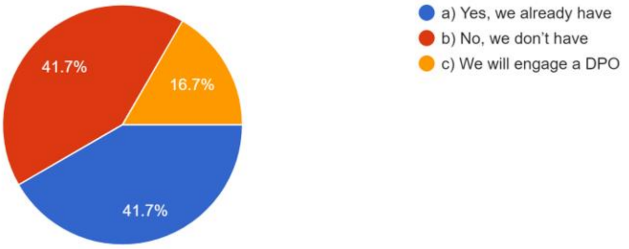


Figure 6.15: Engagement of DPO from partners to follow up the activities of OneNet project.

Table 6 National data protection supervisory authorities.

Authority	Link
Valstybinė duomenų apsaugos inspekcija	https://vdai.lrv.lt/lt/
CNPD - Centro Nacional de Proteção de Dados	www.cnpd.pt
Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti) ("DPA") 'The Serbian data protection authority is the Commissioner for Information of Public Importance and Protection of Personal Data'	https://www.poverenik.rs/sr/
CNPD - Centro Nacional de Proteção de Dados	https://www.cnpd.pt/
Data protection - Data Protection Ombudsman's Office	'https://tietosuoja.fi/en/home'
AEPD: Spanish Data Protection Agency	https://www.aepd.es/es
NISZ: Nemzeti Infokommunikációs Szolgáltató Zrt	https://www.nisz.hu/
AKI: Republic of Estonia, Data Protection Inspectorate	'https://www.aki.ee/en'
NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság	'www.naih.hu'
ANSSI: Agence nationale de la sécurité des systèmes d'information	https://www.ssi.gouv.fr/en/
ICO: Information Commissioner's Office	https://ico.org.uk/
UODO: Urząd Ochrony Danych Osobowych	'https://uodo.gov.pl/

7. Cybersecurity recommendations for the OneNet architecture and relevant constraints

This chapter includes initially an introduction to the OneNet architecture in order to facilitate the reader to have a clear view of it and understand properly its objectives and functionalities. Afterwards, the cybersecurity requirements and the constraints identified are thoroughly presented.

7.1 Introduction to the OneNet Architecture

One of the main objectives of OneNet project is to design an open conceptual architecture that will enable the European electrical system to operate as a single system in which a diversity of markets, network technical operations, energy platforms allow global participation of stakeholders regardless of their physical location, at all levels, from TSOs to DSOs, from small consumers to large producers. The high-level architecture is focusing on these two main aspects: firstly, to enable collaboration between different platforms targeting different domains; and secondly, to simplify the management of elements within platforms. The OneNet project does not provide a platform itself but an architecture that allows platforms to work together, in fact a key element considered for the design of such architecture is to make a data interoperability mechanism available to all platforms to support data exchange.

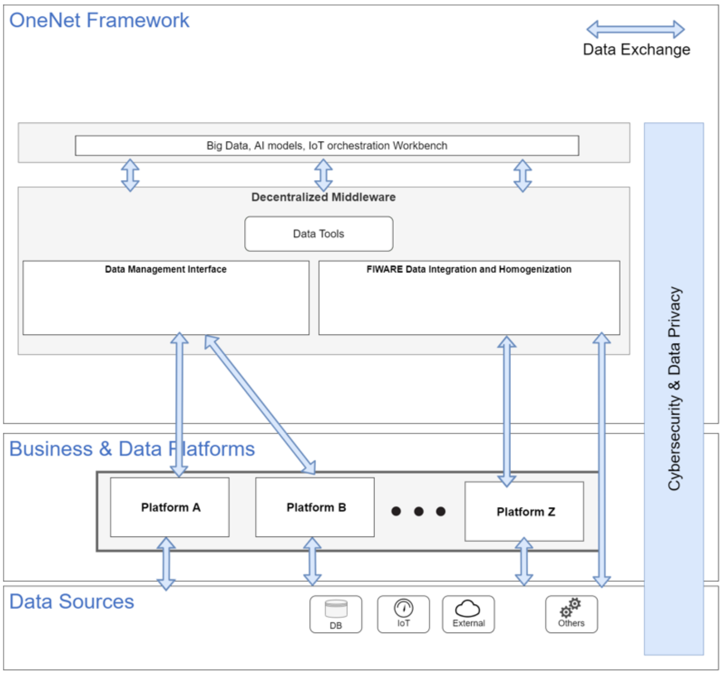

OneNet Framework
Data Exchange
Big Data, AI models, IoT orchestration Workbench
Decentralized Middleware
Data Tools
Data Management Interface
FIWARE Data Integration and Homogenization
Cybersecurity & Data Privacy
Business & Data Platforms
Platform A
Platform B
Platform Z
Data Sources
DB
IoT
External
Others

Figure 7.1: High-level diagram of the OneNet architecture. Extensive description of this diagram can be found in D5.2.

The core of the OneNet architecture, as illustrated in *Figure 7.1*, will be the Decentralized Middleware. This middleware will enable the exchange of information between all assets and various components that will be integrated in the OneNet ecosystem. This middleware includes mainly two sub-layers:

- the Data Management Interface enables the handling and management of data between involved actors,
- the FIWARE Data Integration & Homogenization[3] manages and provides standard access to the information coming from different sources belonging to different actors in the energy ecosystem.

Other low-level modules could be included in the middleware to manage semantic models for assisting in the interpretation of exchanged information, to handle and enforce data access policies, and to provide data quality control. All these modules will be indispensable to achieve OneNet's main goal: enabling a technology agnostic cross-platform, cross-stakeholder, and cross-country interoperability.

In addition to the fundamental aspect of the integration and management of the data exchanged by different platforms, the OneNet architecture take also into account the integration and orchestration of AI, Big Data, and IoT Apps for near real-time grid services.

Specifically, OneNet will include the OneNet workbench orchestration of Big Data, AI-based analytics models, IoT/edge computational/edge nodes technological enablers with a view to enable smart grid service/applications developers to deliver scalable near real-time cross-stakeholder cross-country market and coordinate network management services.

Finally, OneNet will allow the connection of data providers and data consumers to the middleware via specific interfaces and can provide applications to the App store of the AI, Big Data, IoT Apps for grid services layer. Moreover, it will allow to data owners and their assets to stay connected with the OneNet ecosystem.

Starting from these considerations, which give us a vision of the concept and the objectives of the OneNet architecture, we can certainly say that all the cybersecurity aspects linked to data exchange and in particularly the data privacy, must be considered during the implementation of the OneNet architecture.

All risks associated with unsafe data exchange therefore play a fundamental role together with the regulatory and legal aspects of data privacy. In this context, for example, it is crucial to follow the EU Data Protection Framework and the EU Information Security Framework guidelines and requirements. In next paragraph, we will see in more detail what are the guidelines, recommendations, and standards to be implemented in the OneNet architecture. They will provide the basis for the definition of non-functional requirements.

[3] FIWARE is a curated framework of open-source platform components to accelerate the development of Smart Solutions. More information about FIWARE concept can be found at: https://www.fiware.org/.

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

7.2 Cybersecurity, privacy and regulation guidelines for the OneNet architecture

The OneNet ecosystem connects critical infrastructure and public networks, enabling to combine cross-platform, cross-stakeholder, and cross-country interoperable technology. The integral function is secure data exchange between relevant actors in the energy ecosystem and beyond. As described in the previous chapter, in order to achieve this, the core of the OneNet architecture will be the Decentralized Middleware, which consists of two fundamental components — the Data Management Interface and the Firmware Data Integration & Homogenization. The Data Management Interface enables to manage data between involved actors and the Firmware Data Integration & Homogenization allows to access information from different sources belonging to different actors in the energy ecosystem.

In terms of security of these two components, smart grid security, information security and data privacy protection must be considered. Firstly, it is vital to protect the critical infrastructure and other components of smart grids from threats deriving from the access to public networks. Secondly, it is important to protect data privacy and guarantee confidentiality, integrity, and availability of the information. Due to long lifecycle of technical equipment used in energy ecosystem and constantly evolving processes and threats in cyberspace, ensuring information security and data privacy of a smart grid is not a one-off effort but continuous process.

Considering smart grid security, NISTIR 7628 [25] recommends defense-in-depth approach for protecting smart grid infrastructure. This means that multiple layers of defence measures should be implemented to protect OneNet and its components. This requires balanced approach focusing on defensive measures implemented in multiple layers and equipment distributed between multiple locations in order to protect system against all attack vectors. In terms of information security, ISO 27001 Information Security Management standard [30] proposes the following definition: "preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved". "Confidentiality, Integrity and Availability (CIA) are thus the key essential requirements of Information Security" [27]. Regarding data privacy, six plus one privacy principles of the GDPR [9] are acknowledged — these are the guiding principles of the regulation and compliant processing. Explanations of these principles are provided in Chapter 3.2.1.1.

Regarding CIA triad, a CIA vs. AIC paradigm of Smart Grid Information Security, should also be considered. "Confidentiality, Integrity and Availability are usually presented as parameters of information security model where order of these parameters does not hold any meaning on its own. However, depending on the context, these parameters might have different weight associated with them. For instance, in energy sector availability is traditionally considered as most important parameter, with integrity second and confidentiality last. However,

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

with the introduction of smart grid and its services weight of Confidentiality, Integrity and Availability may vary depending on stakeholder activities" [27]. Also, it should be noted that although in energy sector availability is traditionally the first priority, in some functionalities of smart grids, confidentiality and data integrity might be more important — protecting customer data, personally identifiable information etc.

7.3 Cybersecurity guidelines and recommendations

In terms of cybersecurity, privacy and regulatory aspects of OneNet architecture, NISTIR 7628 Smart Grid Cyber Security standard, SGIS Report (described in section 5.3) are considered to be the most relevant. In addition, Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) [31] and ENISA Smart Grid Threat Landscape and Good Practice Guide [32] are included. Global and European cybersecurity standards in energy automation (described in Section 4.1.1.1) are not in the focus of this chapter.

Recommendations listed in *Table 7* are based on nineteen chapters of NISTIR 7628 Smart Grid Cyber Security standard. Each line represents a condensed description of standard chapter with additional more specific recommendations. Included, relevant results of the cybersecurity survey (see Chapter 6) 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.

Table 7: 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	C, I, A	• Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • 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

	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.		
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 minimisation • Integrity and confidentiality (security) • Accountability
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. 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	A	N/A

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

	alternate control center(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: • In case of wider adaptation of technologies developed during OneNet need for	C, I, A	Accountability

	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 minimisation • 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.	C, I	• Integrity and confidentiality (security)

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

	Recommendations: • 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).		• Accountability
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. Recommendations: • 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	Measures should be considered to protect information system components and communication links against cyber intrusions.	C, I	Integrity and confidentiality (security)

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

communication protection	Recommendations: • Industry proven or government approved cryptographic algorithms and libraries should be used. (OWASP ASVS 6.2.2). 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)

As previously mentioned, cybersecurity of such a complex system as OneNet cannot be a one-time effort but must be a continuous process. It requires constant monitoring and assessment. For this purpose, it is advised to use test-driven development and maintain OneNet using regular functionality testing, code reviews, vulnerability scanning, 3rd party risk assessments and penetration testing. Penetration testing could be done according to widely accepted security verification standard in EU, OWASP ASVS. Also, in order to avoid security incidents related to misconfigurations, service providers in OneNet ecosystem should provide testing environment(s) in order to test new services before their production rollout. Due to the fact that data security and privacy is of high importance, the curation, processing, and transmission of the data will be conducted under the principles set out in the GDPR and any other applicable national legislation. In addition, for the derivation of the DPIA for the proper guidance to help ensure the fundamental rights to protection and personal data, the eight-step process documented in [34] shall be used, by leveraging the DPIA Template established by Smart Grid Task Force.

In conclusion, cybersecurity of OneNet requires continuous effort. To limit the required effort and share liabilities, it should be considered whether to cover previously listed guidelines and recommendations with new developments specially tailored for the needs of OneNet. Alternatively, already existing, and tested solutions could be used. For example, to cover the core functionality of OneNet ecosystem, secure data exchange, FIWARE

Context Broker [35], or similar industry proven solution like Estfeed [36] or Unified eXchange Platform® (UXP) [UXP] could be considered. Using 3rd party solutions, it is important to remember that new security risks could be introduced, and these must be analysed and considered.

8. Conclusions

OneNet seeks to provide a seamless integration of all the actors in the electricity network across Europe. The goal is to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure. Supporting this goal, this report provides an overview of relevant cybersecurity, privacy and other regulatory requirements that lay the basis for designing the architecture of OneNet ecosystem. Based on this overview, key takeaways and recommendations have been provided for the next development phases of OneNet.

In order to establish requirements for OneNet's ecosystem, current state and practices of energy ecosystem must be understood. With this purpose, important assets, SCADA systems in use and potential threats to these systems have been reviewed. Threats impact in terms of cyber incidents has been analysed. With this in mind, a thorough overview and suggestions for necessary response procedures in case of incidents have been provided. Relevant standards, principles, regulatory frameworks, and best practices in EU and globally in terms of power industry (smart grids) and related cybersecurity requirements were identified and assessed. These include requirements for power systems management, industrial automation and controls systems security, information security management and cybersecurity (both in terms of smart grids and considering the proposed architecture of OneNet ecosystem).

According to results described in this report, pan-European innovation in grid operations via platform federation as proposed in OneNet is a complex technical challenge. Building it requires special attention to cybersecurity, privacy and other business regulatory requirements. To identify security landscape relevant to sector, survey was conducted amongst OneNet partners. Based on survey results security threats critical to energy sector were identified and measures already implemented in industry were determined. In addition, participants' data privacy posture was surveyed, including engagement of DPO and conducting of DPIA for OneNet demonstrators.

Due to the nature of smart grid network which connects critical energy infrastructure components with consumer facing technology and services, cybersecurity and data privacy principles must be considered. Thus, six plus one privacy principles of GDPR should be seen as the guiding principles of regulation on compliant processing, especially so when dealing with customer data and other personally identifiable information. Also, data controller obligations and data subject's rights in terms of GDPR have been reviewed and should be considered. From ethics perspective, collection and processing of personal data should be non-invasive.

In terms of security recommendations, comprehensive requirements provided in NISTIR 7628 are recognized as the most relevant guidelines for going forward with OneNet project. Based on this, more detailed

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

recommendations and suggestions have been provided, also taking into account SGIS report, ENISA cybersecurity guidelines for smart grids and OWASP ASVS security verification standard. In addition, it is suggested to consider whether to develop everything needed for OneNet from the ground up or alternatively, use already existing components. A potential solution for data exchange in OneNet ecosystem could be Unified Exchange Platform (UXP) or similar proven data exchange solution. It must be kept in mind that both options pose different risks. Owing to evolving nature of security threats, on-going respect of good security practices is vital to the success of OneNet.

In conclusion, the cybersecurity, legal and privacy topics take on a fundamental aspect in the OneNet architecture and its operation. In particular, analysing the OneNet concept, the main important goal is to secure data exchange between relevant actors in the energy ecosystem and beyond.

In these terms, it becomes of fundamental importance to follow the specifications provided by the EU in the Data Protection Framework and in the Information Security Framework. For this reason, the approach and guidelines recommended in this document leverage on the Smart Grid Security (NISTIR 7628), Information security (CIA: Confidentiality, Integrity and Availability) and Data Privacy Protection (EU Data Protection Framework and GDPR).

From a technical and implementation point of view, it will be crucial for OneNet providing specially tailored cybersecurity requirements based on the recommendations collected in this document and in particular focusing on the threats/attacks the experts of the energy industry think are the most critical. Furthermore, OneNet ecosystem should provide a testing environment(s) in order to test new services (and platform integration) before their production rollout.

The outcome of this report constitutes the foundations from a security perspective based on which the OneNet concept will be built upon. Regarding the horizontal WPs:

- WP4 will utilize the data privacy requirements declared in this deliverable to conduct a requirement analysis regarding cybersecurity measures for grid operators and customer integration.
- Tasks of WP5, such as T5.2 and T5.6, which are responsible for the creation of the OneNet architecture, and the extended data and service interoperability in the OneNet platform of platforms, respectively, need as a knowledge from this deliverable all the presented standards for security in data exchange, collection and process in 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 raise their awareness regarding cybersecurity and

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

data privacy and protection issues in the demonstration activities that will be conducted in the context of the OneNet project.

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

9. References

[1] "Overview of the secondary EU legislation that falls under the legislative competence of DG ENER and that is currently in force.", 19 December 2019, [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/2014-12-19-ener-legislation.pdf (accessed Jun. 14, 2021).

[2] "L_2009211EN.01005501.xml.", [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0072 &from=EN (accessed Jun. 14, 2021).

[3] "Clean energy for all Europeans package | Energy.", [Online]. Available: https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en (accessed Jun. 14, 2021).

[4] "REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 5 June 2019 - on risk-preparedness in the electricity sector and repealing Directive 2005/ 89/ EC," 2019.

[5] "L_2019158EN.01002201.xml.", [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:320 19R09 42&from=en (accessed Jun. 14, 2021).

[6] "Smart Grid Security.", [Online]. Available: http://www.enisa.europa.eu (accessed Jun. 14, 2021.)

[7] EU, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016," 2016., [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=GA (accessed Jun. 15, 2021).

[8] "Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC."

[9] "General Data Protection Regulation (GDPR) Compliance Guidelines.", [Online]. Available: https://gdpr.eu/ (accessed Jun. 14, 2021).

[10] F. Buchi, S. Fries, and D. Kroeselberg, "Cyber Security Standards and Regulations in Energy Automation Systems," 2015, [Online]. Available: https://www.siemens.com/download?DLA20_43

[11] "Reference document on security measures for Operators of Essential Services," 2018, [Online]. Available: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures__0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed Jun. 14, 2021).

[12] "Making the web secure by design.", OWASP, [Online]. Available: https://owasp.org/www-pdf-archive/Skfpptx-design-workshop.pptx.pdf (accessed Jun. 14, 2021).

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

[13] “REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL”, 17 April 2019, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R088 1&from=EN (accessed Jun. 14, 2021).

[14] “Standards and Certification — ENISA.”, [Online]. Available: https://www.enisa.europa.eu/topics/standards?tab=publications (accessed Jun. 14, 2021).

[15] “EG2 deliverable on security measures for smart grids — ENISA.”, [Online]. Available: https://www.enisa.europa.eu/events/security-measures-for-smart-grids (accessed Jun. 14, 2021).

[16] “Communication network dependencies for ICS/SCADA Systems — ENISA.”, [Online]. Available: https://www.enisa.europa.eu/publications/ics-scada-dependencies (accessed Jun. 14, 2021).

[17] “Dell report revealed attacks on SCADA system are doubled Security Affairs.”, [Online]. Available: https://securityaffairs.co/wordpress/35967/hacking/dell-attacks-on-scada-doubled.html (accessed Jun. 14, 2021).

[18] “ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends – Cybersecurity Observatory.”, [Online]. Available: https://www.cybersecobservatory.com/2018/01/16/enisa-threat-landscape-report-2017-15-top-cyber-threats-trends/ (accessed Jun. 14, 2021).

[19] M. Keogh and S. Thomas, “National Association of Regulatory Utility Commissioners Cybersecurity A Primer for State Utility Regulators Acknowledgments and Disclaimers,” 2017.

[20] A. Stefanini, D. Benintendi, U. Finardi, and D. K. Holstein, “EVALUATING THE PRUDENCY OF CYBERSECURITY INVESTMENTS: Guidelines for Energy Regulators Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators EVALUATING THE PRUDENCY OF CYBERSECURITY INVESTMENTS: Guidelines for Energy Regulators Project Title: Europe and Eurasia Cybersecurity Partnership Sponsoring USAID Office: USAID Bureau for Europe and Eurasia Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators,” 2020.

[21] “Reference document on Incident Notification for Operators of Essential Services.”, [Online]. Available: https://ec.europa.eu/information society/newsroom/image/document/2018-30/reference document incident reporting 00A3C6D5-9BDB-23AA-240AF504DA77F0A6 53644.pdf (accessed Jun. 14, 2021)

[22] “NIS Cooperation Group’s guidelines for implementing the NIS Directive and addressing wider cybersecurity policy issues | Shaping Europe’s digital future.”, [Online]. Available:

https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-groups-guidelines-implementing-nis-directive-and addressing-wider-cybersecurity (accessed Jun. 14, 2021).

[23] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Economic Impacts of Cyber Security in Energy Sector: A Review," *International Journal of Energy Economics and Policy*, vol. 7, no. 5, pp. 250–262, 2017, Accessed: Jun. 14, 2021. [Online]. Available: https://ideas.repec.org/a/eco/journ2/2017-05-28.html

[24] Kalkitech, "Standards-based Security for Energy Utilities.", Whitepaper, 2019, Accessed: Jul. 19, 2021. [Online]. Available https://kalkitech.com/wp-content/uploads/2020/12/WP030017_-Standards-Based-Security-for-Energy-Utilities-v1.01.012019.pdf

[25] "Guidelines for Smart Grid Cybersecurity Volume 1-Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee", Doi: 10.6028/NIST.IR.7628r1.

[26] "STANDARDISATION Mandate.", [Online]. Available:

https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction =search.detail&id= 475 (accessed Jun. 14, 2021).

[27] "CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security," 2012.

[28] "EUCS – Cloud Services Scheme — ENISA.", [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/ (accessed Jun. 14, 2021).

[29] "Cybersecurity Certification Group | Shaping Europe's digital future.", [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group (accessed Jun. 14, 2021).

[30] "ISO/IEC 27001:2005 Information Security Management standard.", [Online]. Available: https://www.iso.org/standard/42103.html (accessed Jun. 25, 2021)

[31] "OWASP Application Security Verification Standard.", [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/ (accessed Jun. 25, 2021)

[32] "ENISA Smart Grid Threat Landscape and Good Practice Guide.", [Online]. Available: . https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide (accessed Jun. 25, 2021)

[33] "Unified eXchange Platform.", [Online]. Available: . https://cyber.ee/products/secure-data-exchange/ (accessed Jun. 25, 2021)

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

[34] Workshop DPIA Test phase. Directorate General for Energy European Commission. Brussels, 22/05/2015, [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA_22May_Workshop_final.pdf (accessed Jul. 26, 2021)

[35] [FIWARE] Developers Catalogue - FIWARE., [Online]. Available: https://www.fiware.org/developers/catalogue/ (accessed Jul. 25, 2021)

[36] [ESTFEED] Estfeed - Technology., [Online]. Available: https://www.estfeed.eu/en/technology (accessed Jul. 25, 2021)

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

10. Appendix

This section includes the online questionnaire distributed to the partners. The answers are presented in Chapter 6.

Cybersecurity Survey

Dear Participant,

We kindly seek your response to this survey conducted by UBITECH Energy. This research is part of T5.8 “Cybersecurity, privacy and other business regulatory requirements” of the OneNet project. The purpose of this survey is to contact various industries to address what is the current status of the organisations regarding the business, legal standards and regulations in the aspect of cybersecurity.

Please note that while analysing your response, your identity or that of your organisation will not be revealed and no publication will include any personal data of the respondents.

For more information on this survey, please contact: Name of researcher: Magda Zafeiropoulou Organization: UBITECH Energy

E-mail: m

** Required*

zafeiropoulou@ubitech.eu

1. Have you suffered a security breach in the last 12 months (multiple answers possible)? *

Check all that apply.

a) Weaknesses highlighted during testing

b) Lost assets (lost/stolen laptops or memory cards)

c) Malware or viruses

d) Hacker attacks

e) Ransomware

f) Denial-of-service attacks

g) Spam emails

h) Redirection to fraudulent websites

i) Impersonating organisation in emails

j) Unauthorised use of computers networks or servers by outsiders

k) Unauthorised use of computers, networks by staff

l) Any other breaches or attacks

m) We were not exposed to hacking

2. Which industry is your organisation in? *

Mark only one oval.

a) ESCO

b) System Operator

c) Market operator

d) Technology Provider Other:

3. How many people does your IT-department employ? *

Mark only one oval.

a) 1-2

b) 3-5

c) 6-10

d) 11-15

e) >15

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

4. What are the assets (software and/or hardware) you consider more critical in your demo regarding cybersecurity?

5. Does your organization utilize a security management and risk assessment process? If yes, please identify which ones (multiple answers possible). *

Check all that apply.

a) No

b) Yes – ISO/IEC 27019

c) Yes – IEC 62351

d) Yes – ISO 31000

e) Yes – NISTIR 7628

f) Yes, regulatory standards

g) Yes, COBIT

h) Yes, ITIL Other:

6. What do you perceive your organisation's biggest vulnerabilities are? *

Mark only one oval.

a) OT

b) ICT

c) Policies

d) Supply chain

Other:

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

7. How secure do you think your organisation's network is? *

Mark only one oval.

a) Sufficiently secure

b) Secure to a certain extent

c) Information not available

d) Not secure

e) Highly secure

8. Have you already implemented any cybersecurity awareness training process in your organisation? *

Mark only one oval.

a) No

b) Yes

9. If you have answered yes in the previous question, please specify if you use any methodology to define the training contents - e.g., SANS

10. How do you keep informed of new forms of information security attacks and threats (multiple answers possible)? *

Check all that apply.

a) Consulting firms/ external consulting

b) Scientific publications

c) Providers (vendors)

d) Social network

e) News on websites / blogs / from professional associations

f) Security conferences

g) Mailing lists

h) No, I do not get regular updates regarding security attacks and threats Other:

11. Does your organisation have/will engage a DPO to follow up your activities within the project? *

Mark only one oval.

a) Yes, we already have

b) No, we don’t have

c) We will engage a DPO

12. Who is your national data protection supervisory authority, and are you aware if they have issued a list of further data processing activities requiring a DPIA (under Art 35(4) GDPR) (Please here include the website address of the authority, and link to any relevant guidance that they have issued in relation to DPIA (Data Protection Impact Assessment)) *

13. On a scale of 1 (“lowest”) to 5 (“highest”), how prepared is your organization to respond to a cyber-security incident? *

Mark only one oval.

1 2 3 4 5

14. Which industrial protocols used by your organization/environment are considered as vulnerable (multiple answers possible)? *

Check all that apply.

a) IEC 62351

b) IEC 61850

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

c) IEC 61850-7-410

d) IEC 61850-7-420

e) IEC 60850-5-102

f) IEC 60870-5-101/104

g) Modbus

h) DNP3 Other:

15. Which security measures has your organisation implemented (multiple answers possible)? *

Check all that apply.

a) Safety endpoints

b) Managing event logs (solutions SIEM (Security Information and Event Management))

c) Data Loss Prevention / file encryption (memory)

d) Vulnerability Management

e) Intrusion Detection Systems / Intrusion Prevention Systems

f) Anti-spam / spyware / phishing solutions

g) Firewalls

h) Antivirus

i) Information not available Other:

16. Which of the following threats/attacks are the most critical for your industry? *

Mark only one oval.

a) Insider attack

b) Spear phishing

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

c) Denial of service

d) Ransomware Other:

17. What areas do you believe are most vulnerable to cyber-attack (multiple answers possible)? *

Check all that apply.

a) Generation

b) Transmission

c) Dispatching, control, and supervision (SCADA, RTU, PLS)

d) Distribution

e) Energy Market

f) End-customer premises

g) Data management platform Other:

18. What kind of anomalies do you consider as the most crucial in the electrical grid? *

Mark only one oval.

a) Anomalies related to current (ampere)

b) Anomalies related to voltage (voltage)

c) Anomalies related electric power (watt)

d) Anomalies related to resistance (Ohm) Other:

19. What is the maximum time scale interval in which an intrusion must be detected in your organisation? *

Mark only one oval.

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

a) Seconds

b) Minutes

c) Hours Other:

20. What measures do you usually take to mitigate network attacks targeted at your organisation's infrastructure / customers (multiple answers possible)? *

Check all that apply.

a) Access Control Lists / packet filters

b) Firewalls

c) Intrusion Prevention Systems

d) Source-based remote-triggered blackholes

e) Destination-based remote-triggered blackholes Other:

21. What tools does your organization use to detect attacks (multiple answers possible)? *

Check all that apply.

a) Open-source software

b) Self-developed tools

c) Commercial products

d) Information not available

This content is neither created nor endorsed by Google.

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