D8.8

Report on recommendations for certification, standardization and exchange of information at the EU level

DOCUMENT	D8.8	**WORKPACKAGE**	WP8
DELIVERABLE STATE	FINAL	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V1	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	30/06/2024	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PU	**DURATION**	3 YEARS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560

DISCLAIMER

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020)
	SU-DS04-2018-2020
TOPIC	Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)
PRINCIPAL CONTRACTORS	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP8
DELIVERABLE TYPE	Report
DISSEMINATION LEVEL	PU Public
DELIVERABLE STATE	FINAL
CONTRACTUAL DATE OF DELIVERY	30/06/2024
ACTUAL DATE OF DELIVERY	10/07/2024
DOCUMENT TITLE	Report on recommendations for certification, standardization and exchange of information at the EU level
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	STANDARIZATION, CERTIFICATION, CRITICAL INFRASTRUCTURE, SECURITY

Document History

Version	Date	Contributor(s)	Description
V0.1	03/01/2024	IKE	Table of content
V0.2	10/05/2024	IKE	Section 2
V0.3	15/05/2024	IKE	Section 3,4
V0.4	15/05/2024	BEN, TEL, ENERIM, OPR, PET	Provide information for Section 3
V0.5	06/06/2024	FRAUNHOFER	Section 2.2, Section 2.4, Chapter 7
V0.6	06/06/2024	IKE	Section 6
V0.7	07/06/2024	IKE	Section 1,8
V0.8	25/06/2024	IKE, FRAUNHOFER, ENG, CINI, STAM, ZIV, RWTH, ICS, SYNELIXIS, WIN, GT, ACS, INF	Questionary responses (Information for Section 5)
V0.9	26/06/2024	IKE	Section 5
	08/07/2024	IKE	Corrections suggested by ICS and WIN
V1.0	09/07/2024	IKE, ENG	Final version

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

C5	Cloud Computing Compliance Controls Catalogue
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Teams
EDR	Endpoint Detection and Response
EU	European Union
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GDPR	General Data Protection Regulation
HEMS	Home Energy Management Systems
IDPS	Intrusion Detection and Prevention Systems
ISAC	Information Sharing & Analysis Centre
MSSPs	Managed Security Service Providers
NCCS	Network Code on Cybersecurity (NCCS)
NTA	Network Traffic Analysis
SIEM	Security Information and Event Management
TIP	Threat Intelligence Platforms

Executive Summary

This document contains recommendations for a certification process. Several recommendations are provided for the company or organisation to start a certification process with a certification entity. For this purpose, an analysis of the IEC 62443 standard, the NIS2 directive and the Cyber Resilience Act has been carried out in order to detect their contributions and requirements. Then, the CyberSEAS infrastructures and tools are analysed considering the requirements of the IEC 62443 standard. Additionally, a questionnaire has been carried out for tool providers to find out their interests regarding certification.

In conclusion, this deliverable aims to help companies or organisations to know the state they are in before entering the certification phase with a certification entity.

1 Introduction

The energy sector is part of the critical infrastructure, which is really important for the society, so ensuring the security of energy systems is necessary. The increase of digitisation and interconnection of energy grids, smart grid technology, renewable energy and distributed energy resources can be a source of vulnerabilities. Cybersecurity threats to the energy sector can have devastating consequences, such as power outages, infrastructure damage, economic losses and threats to public safety, making it a principal target for cyber-attacks, with incidents ranging from ransomware attacks on energy companies to sophisticated state-sponsored intrusions aimed at disrupting critical operations [2].

International standards such as the IEC 62443 [3] industrial cyber security standard, which provides guidelines for securing industrial automation and control systems, play a key role in establishing a baseline for cyber security in the energy sector. Compliance with these standards helps organisations to identify vulnerabilities, implement effective security controls and achieve certification, ensuring a high level of protection against threats. In addition, regulatory frameworks such as the NIS2 Directive [4] and the Cyber Resilience Act (CRA) [5] emphasise the need for comprehensive risk management, incident reporting and information sharing to improve the resilience of critical infrastructures.

The CRA aims to address concerns about the security of digital products and services. It introduces mandatory cybersecurity requirements for the design, development and lifecycle management, ensuring that security is implemented correctly. This complements existing regulation and aims to create a cohesive and resilient cybersecurity environment in the EU.

The NIS2 Directive updates the original NIS Directive on network and information systems, expands the scope and strengthens cybersecurity requirements for critical and important EU entities. This directive emphasises incident reporting, risk management and cooperation between Member States, pushing higher levels of cybersecurity preparedness and resilience.

By integrating the principles and requirements of IEC 62443, NIS2 and CRA, this report outlines a roadmap for achieving industry certification by providing a high-level analysis of tools and infrastructures and recommendations for how companies can become certified in the future.

2 Cybersecurity Certification, Standardization and Data Exchange in the EPES Sector

In this chapter, is discussed general information on standards affecting EPES and also other regulations or directives that have impact on it.

2.1 Cybersecurity Certification & the Importance of Data Exchange in EPES

In recent years, Europe has been intensifying its efforts to regulate and standardise cybersecurity. The Cyber Resilience Act (CRA) is a key piece of legislation that aims to strengthen cybersecurity by establishing a common certification framework for cybersecurity-related products, services, and processes. The European Union (EU) has been adopting and adapting international standards, such as NIST's, for its own cybersecurity policies and practices. The NIST Framework for Improving Critical Infrastructure Cybersecurity is particularly relevant and provides solid guidelines for improving cyber resilience.

One of Europe's main objectives is to develop cyber resilience capabilities, i.e. it wants its systems to be able to resist and recover from attacks, but also to be able to prevent them. For this reason, proactive security measures are implemented, and cyber security awareness is increased across the whole landscape.

Regarding EPES, this industry is a critical infrastructure, so special attention is paid to it in terms of cyber security. In this sector, efforts are being made to improve the cybersecurity of the systems. Companies are investing in technologies and practices that allow them to remain operational even in the event of cyber-incidents, as it is very important to have the highest possible availability in these systems. Moreover, in the electric sector, there are specific regulations on cyber security. This may include the NIS Directive and other regulations specific to the electricity sector that set out cyber security and incident reporting requirements. Detecting threats early is crucial to protect these systems and advanced monitoring systems, network behavioural analysis and threat detection and response solutions are being implemented to proactively identify and mitigate attacks.

2.2 Relevant Standards and Frameworks

Below, in Table 1, the standards that are related to electrical or critical infrastructures are listed.

Table 1: Standards and frameworks for electrical infrastructures

Area	Standard or Framework
General IT security reflecting business requirements	ISO/IEC 27001 Security requirements
	ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment
Energy Systems Operational Environments (Organisational and Procedural Security Controls)	NIST Cybersecurity Framework
	ISO/IEC 27002, 27019 Security Controls
	NISTIR 7628 Smart Grids Security Controls
Energy Systems Operational Technologies (Technical Security Controls and Techniques)	IEC 62443-3-2-3, 2-4 and 4-1 security controls
	IEC/TR 62351-12 Resilence of power systems with DER
	IEC 62443-4-2 security for products
Common level of cybersecurity for cross-border electricity flows	EU network code on cybersecurity for the electricity sector (C/2024/1383)
Guidelines for Smart Grid Cybersecurity	NISTIR 7628

2.3 Alignment with European Initiatives

Two of the most important cyber security initiatives in Europe are the Cyber Resilience Act (CRA) and the NIS2 directive.

The CRA is a legislation designed to improve cybersecurity and resilience in all critical sectors, including the electrical industry, within the European Union (EU). The electrical sector is particularly vulnerable to cyber threats due to its reliance on interconnected digital systems for the generation, transmission, and distribution of electricity.

The CRA imposes specific cybersecurity requirements on operators of critical infrastructure, including electric utilities, covering measures such as risk assessment, incident notification and cybersecurity controls to protect against cyber threats and ensure system resilience. It establishes procedures for incident response and recovery in the event of cyber incidents, requiring timely notification, stakeholder coordination and mitigation measures. In addition, the CRA promotes information sharing and collaboration among electricity sector stakeholders, facilitating the exchange of threat information and best practices to improve cyber resilience. Regulatory oversight by bodies such as energy regulators and cybersecurity authorities enforce CRA requirements, conducting audits and ensuring

compliance to safeguard electricity infrastructure. Provisions can also address supply chain security, requiring risk assessments for external suppliers to mitigate supply chain attacks and maintain component integrity.

The NIS2 Directive is the EU's cybersecurity regulation, which became effective in 2023. It sets out legal measures to boost the overall level of cybersecurity within the EU. This directive updates the EU cybersecurity rules introduced in 2016. It modernises the legal framework to deal with the increase in digitisation and cybersecurity threats. By extending the scope of the cybersecurity rules to new sectors and entities, it improves resilience and incident response capability [6].The main differences between both initiatives are that NIS2 is more targeted at critical infrastructures and it is aimed at service providers and CRA is more targeted at commercial elements and it is aimed at manufacturers. Furthermore, in the case of NIS2 there are no exceptions, but CRA does not apply in the following cases: Free or Open-source software, pure B2B SaaS applications, covered under NIS2, AI Act, etc.or covered under EU Health Data Space Regulation for eHR. On the other hand, NIS2 requires risk management measures, incident reporting, cooperation and monitoring, while CRA requires cybersecurity risk assessments, security updates, CE marking and external audits. Finally, NIS2 is a directive that Member States must transpose into national law, while CRA is a regulation directly applicable throughout the EU [7].

2.4 Alignment with European Initiatives for EPES Cybersecurity

Specifically, within the context of the EPES sector, laws and regulations have also been implemented in conjunction with the regulations mentioned in Section 2.3. The EU Network Code on Cybersecurity (NCCS) [1] for EU electricity sector has been adopted within this context and forms an important aspect of the EU action plan to digitalize the energy system.

One of the aims of the network code is to establish a recurring process of obligatory cybersecurity risk assessments in the electricity sector and specify clear roles and responsibilities for the actors within this context. The network code specifically focuses on cross-border electricity flows and therefore its objectives cannot be achieved at the national levels. While defining the high-impact and critical entities that are involved in facilitating cross-border electricity flows, it establishes a governance model that is aligned with the newly established NIS2 regulation thereby simplifying cross-border cybersecurity related data exchange for the energy system. The rules are intended to promote a common baseline keeping in mind existing practices and investments.

It also requires ENTSO and EU DSO Entity to develop a proposal for minimum and advanced cybersecurity controls, which shall be based upon national and international standards in cybersecurity, although these are yet to be concretely specified. For measures related to exchange of information in the context of coordinated exchange cyber-threat or cyber-incident related information, it considers the legal obligations and legitimate interests of the actors within the electricity domain when to comes to sharing of personal data especially with reference to General Data Protection Regulation (GDPR).

The Smart Grid Task Force of the EC as part of the Clean Energy for all Europeans package also set forth recommendations for the implementation of planning, monitoring, reporting and crisis management [8]. Some of these recommendations have been implemented in NCCS. In the context of CTI information sharing, the ENTSO and EU DSO Entity are required to perform a feasibility study to assess the possibility and financial costs necessary to develop a common tool enabling all entities to share cyber threat information with relevant national authorities. As suggested in the report of the Smart Grids Task force, inspiration could come from E-ISACs set up in the United States, which are meant for voluntary information sharing. A similar solution for the energy sector already exists within the EU, namely, the European Energy-ISAC (European Energy Information Sharing & Analysis Centre) [9]. It is an industry-driven initiative for cybersecurity and cyber resilience related information sharing in which both private utilities and solution providers and semi-public institutions can participate.

For high-impact and critical-impact entities identified within the NCCS, a recommendation to establish Cybersecurity operation centre (CSOC) capabilities within its cybersecurity parameters and share relevant information with its computer security incident response (CSIRT) teams is set forth. Figure 1 shows the conceptual framework for rapid information sharing proposed within the NCCS to minimize cascading effects in the grid.

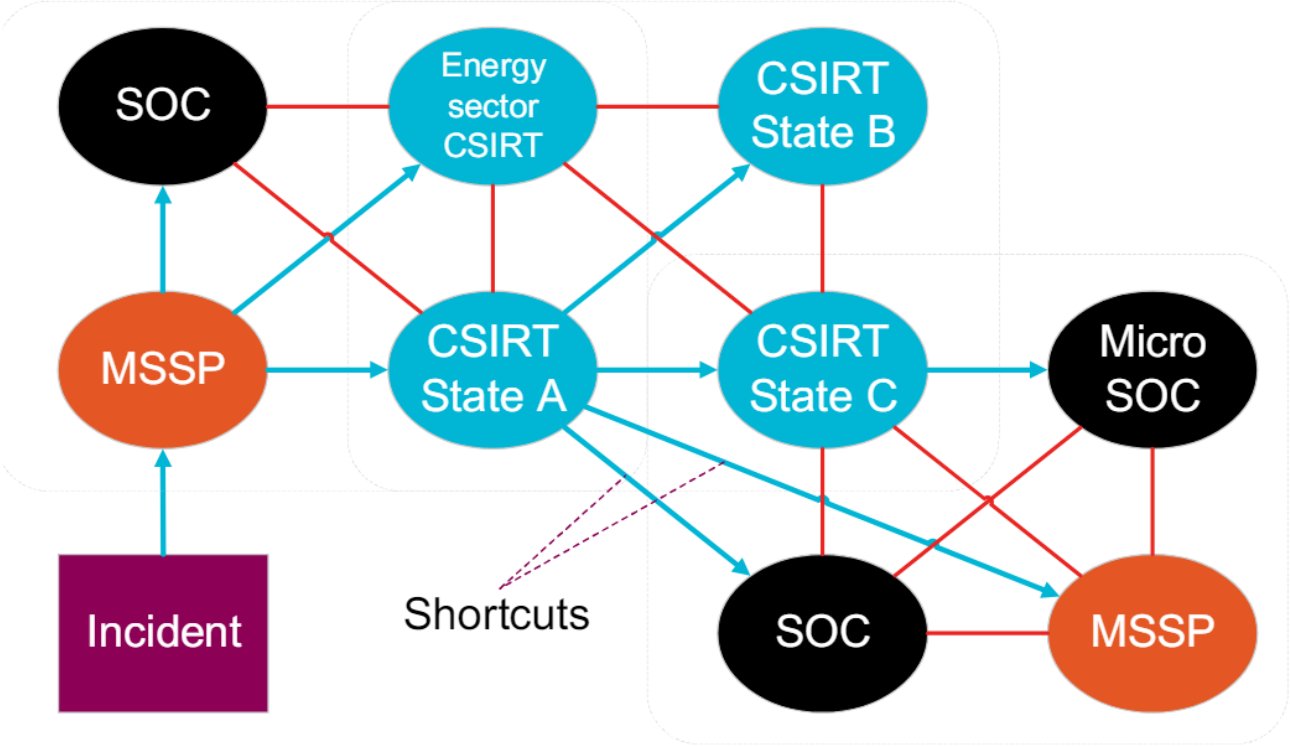

Figure 1: Conceptual framework for information sharing in the energy sector [10]

Regarding the NIS2 Directive has important implications for the energy sector, as previously explained its main objective is focused on strengthening the security and resilience of

systems against cyber-attacks and other threats, including EPES. It is therefore crucial that energy companies have a thorough understanding of its provisions and requirements [11].

In this context, the implications of the NIS2 for the energy sector are significant. On the one hand, it requires companies to implement appropriate technical and organisational measures to prevent, detect and respond to incidents that may compromise the security and continuity of energy supply. These measures cover the protection of critical infrastructure, data security and privacy, as well as ensuring the availability of energy services.

In addition, the directive also lays down specific requirements regarding the protection of personal data. Energy companies must take appropriate measures to safeguard the personal information they handle, as well as to report any incidents that may jeopardise the security of this data.

These provisions reflect the growing importance of cyber security and data protection in the energy sector, underlining the need for companies to take proactive measures to ensure the integrity and reliability of their systems and services.

Moreover, the extension of the scope of the NIS2 Directive to additional sectors and sub-sectors in energy infrastructure, such as hydrogen production, storage and transport, as well as district heating and cooling systems, together with the expansion of the electricity sub-sector to include operators of electric recharging points, reflects technological developments and new market realities. This expansion demonstrates the growing importance of ensuring cyber security in these critical areas, in line with technological advances and changing market demands.

3 Assessment of CyberSEAS Infrastructures

In this chapter, CyberSEAS infrastructures are evaluated according to IEC 62443 standard.

3.1 Comprehensive Study of Current Cybersecurity Practices

In Table 2, the requirements of the use cases and scenarios defined in deliverable 3.1 have been mapped. As can be seen, the defined requirements can be aligned with several FRs of the IEC 62443-4-2 standard. This work is done to guarantee the complete coverage of the requirements, ensuring that all critical aspects of the system are covered in the corresponding use cases and scenarios. In addition, it facilitates traceability of requirements, enabling clear and accurate tracking from initial requirements to implementation. It also optimises system design and development by identifying and grouping related requirements, thus improving efficiency and avoiding redundancies. It also improves system validation and verification, providing a solid basis for ensuring that all requirements are adequately tested and that the system meets the expectations and needs of end users. This mapping facilitates communication between the different project stakeholders, providing a clear and structured view of how requirements align with use cases and scenarios. Finally, it helps to identify dependencies and relationships between different requirements, allowing for a more coherent and orderly planning and execution of the project.

Table 2: Mapping of requirements and FRs

Requirement	Use case	Scenario	IEC 62443
Avoid intrusion into the cabin	Benetutti	1	FR3- System Integrity
Avoid intrusion into the IT network	Benetutti	1,4,5	FR1- Identification and Authentication Control
Guarantee support for the decision-making process of the IT personnel	Benetutti	1,4,5	FR 6 – Timely response to events
To be promptly warned in case of an intrusion into the SCADA system	Benetutti	2	FR3- System Integrity

Tamper Resistant Storage Support	Benetutti	2	FR 4 – Data confidentiality
To be promptly warned in case of an intrusion into the system	Benetutti	3	FR 6 – Timely response to events
Impede the access to the disconnector to unauthorized people	Benetutti	5	FR1- Identification and Authentication Control
Vulnerability detection on weather stations	Slovenian pilot	1	FR 2 – Use control
IT-OT network anomaly and intrusion detection	Slovenian pilot	1,2	FR 6 – Timely response to events
Simulation training	Slovenian pilot	2	FR3- System Integrity
Notification system	Slovenian pilot	1,2,3	FR1- Identification and Authentication Control, FR3- System Integrity
Incident response, CTI, risk assessment and decision support	Slovenian pilot	1,2,3	FR 6 – Timely response to events
Indicators of compromise (IoC) and Cyber Threat Intelligence (CTI) exchange	Slovenian pilot	3,4	FR3- System Integrity
Social engineering prevention	Slovenian pilot	1,2,4	FR1- Identification and Authentication Control
IT intrusion detection system	Transelectrica	1,2,3	FR 6 – Timely response to events

Decision Support System	Transelectrica	1,2,3	FR 6 – Timely response to events
Real time cyber security monitoring	Transelectrica	1,2,3	FR 6 – Timely response to events
Notification System	Transelectrica	1	FR1- Identification and Authentication Control, FR3- System Integrity
Intrusion detection	Transelectrica	3	FR 6 – Timely response to events
Use Antivirus/Antimalware	Enerim	1	FR 7 – Resource availability
Network Intrusion Prevention	Enerim	1	FR 6 – Timely response to events
Restrict Web Based Content	Enerim	1	FR3- System Integrity
Software Configuration	Enerim	1	FR3- System Integrity
User training	Enerim	1	FR1- Identification and Authentication Control
Audit	Enerim	1	FR 6 – Timely response to events
Limit Access to Resource Over Network	Enerim	2	FR 7 – Resource availability
Limit Hardware Installation	Enerim	2	FR3- System Integrity
Use network segmentation	Enerim	3,4	FR 5 – Restricted data flow
User account control	Enerim	3,4	FR1- Identification and Authentication Control
User Account Management	Enerim	8	FR1- Identification and Authentication Control
Minimize available info	Enerim	4	FR 4 – Data confidentiality

Monitor driver load	Enerim	5	FR3- System Integrity
Monitor windows registry key modification	Enerim	5	FR1- Identification and Authentication Control
Privileged Account Management	Enerim	5,8	FR1- Identification and Authentication Control
Manage process metadata	Enerim	5	FR3- System Integrity
Monitor command execution	Enerim	6	FR3- System Integrity
Monitor OS API execution	Enerim	6	FR3- System Integrity
Monitor process creation	Enerim	6	FR3- System Integrity
Properly set user account policies	Enerim	7	FR1- Identification and Authentication Control
Use multi factor authentication	Enerim	7	FR1- Identification and Authentication Control
Password policies	Enerim	7	FR1- Identification and Authentication Control
Update software	Enerim	7	FR3- System Integrity
Monitor application log content	Enerim	7	FR 6 – Timely response to events
Monitor network traffic content	Enerim	9	FR 5 – Restricted data flow
Monitor network traffic flow	Enerim	9	FR 5 – Restricted data flow
Sabotage Detection System	Estonian pilot	1	FR3- System Integrity

Critical configuration detection	Estonian pilot	1	FR3- System Integrity
Physical intrusion detection	Estonian pilot	2	FR3- System Integrity
Decision Support System	Estonian pilot	2	FR3- System Integrity
Version control system	Estonian pilot	3	FR3- System Integrity
Administrative rights management, identity access management and user behaviour analyzation	Estonian pilot	3	FR 2 – Use control
Network segmentation	Estonian pilot	4	FR 5 – Restricted data flow
Isolated IoT implementation	Estonian pilot	4	FR 5 – Restricted data flow
Data confidentiality and integrity	Estonian pilot	5	FR 4 – Data confidentiality
Isolated networks	Estonian pilot	5	FR 5 – Restricted data flow
Implementation of maintenance process	Estonian pilot	6	FR3- System Integrity
Enhance data integrity	Estonian pilot	7	FR3- System Integrity
Overhaul of system by functions	Estonian pilot	8	FR3- System Integrity
Controlled procedures with legacy systems	Estonian pilot	8	FR1- Identification and Authentication Control

Global sync of time of all substations in grid	Estonian pilot	9	FR 2 – Use control
Precautions for protecting local area networks	Estonian pilot	10	FR 5 – Restricted data flow
Detection of suspicious hardware	Estonian pilot	11	FR3- System Integrity
Multiple ways to compare configurations to reality	Estonian pilot	12	FR3- System Integrity
Automated detection of social engineering	Estonian pilot	12	FR 1 – Identification and authentication control
Secure updating process	Estonian pilot	13	FR3- System Integrity
Enhanced security for 3rd party	Estonian pilot	14	FR 1 – Identification and authentication control
Modern physical security	Estonian pilot	15	FR 5 – Restricted data flow
Digital monitoring of all visits in substations	Estonian pilot	15	FR 1 – Identification and authentication control
Enhanced security processes	Estonian pilot	16	FR3- System Integrity
Automated detection of suspicious configurations	Estonian pilot	16	FR3- System Integrity

4 Analysis of CyberSEAS Tools and Their Role

In this chapter, the CyberSEAS tools are analysed according MITRE

MITRE play a critical role in identifying, assessing, and mitigating threats, specifically, MITRE ATT&CK® matrix, is instrumental in understanding and deploying these tools effectively. However, there are different methods to analyse the tools.

Threat Intelligence Platforms (TIPs): These platforms aggregate, analyse, and disseminate threat intelligence data. With these tools organizations are able to anticipate and respond to threats.

Security Information and Event Management (SIEM) Systems: Those systems collect and analyse security event data in real-time to detect any unusual event.

Endpoint Detection and Response (EDR) Tools: They monitor and respond to threats at the endpoint level.

Network Traffic Analysis (NTA) Tools: These are the tools to analyse network traffic to identify anomalous patterns that may indicate malicious activities. They are very useful tools to detect lateral movement.

Vulnerability Management Tools: These tools scan for and identify vulnerabilities in systems and applications.

Intrusion Detection and Prevention Systems (IDPS): IDPS tools monitor network and system activities for malicious actions and policy violations. Additionally, they are able to block or mitigate identified threats.

4.1 Evaluation of CyberSEAS Tools' Capabilities

This section discusses the MITRE requirements with which the tools that have been developed in the CyberSEAS project comply. Task 5.1 analysed the different CyberSEAS tools and which MITRE mitigations they had. Therefore, the following is a summary of the main functionality of the tool and which MITRE mitigation applies to it. In this way, the following subsection will analyse the relationship with the IEC 62443 standard in both the component (4-2) and system (3-3) parts.

Below are the corresponding mitigations for each tool, following the analysis performed in task 5.1. These results must be analysed in order to know which requirements of the standard they must comply with.

- ALIDA

This tool performs the deployment, execution, and monitoring of AI-based big data analytics applications. In addition, it detects spear phishing.

This tool can detect and block activities that may indicate that an exploit is taking place (M0938). It also has intrusion detection (M0931) but has limited mitigations (M0816).

- ## SED

Performs SE detection and has malware detection mitigations (M0949), is capable of detecting and blocking activities that may indicate that an exploit is occurring (M0938), has several restricted websites (M0921), has a threat intelligence program (M0919) and trains users before using the tool (M0917).

- ## MIDA

This tool allows to verify the integrity of security control policies and the actual status of assets, infrastructure, and services. This tool has several mitigations such as access management (M0801), access policies (M0936), antivirus (M0949), restrictions on code execution (M0948), audits (M0947), signature to verify the integrity of executed code (M0945), access limitations (M0935), and supply chain management (M817).

- ## ARTEMIS

A tool for detecting anomalies in SCADA signals. This tool shall consider access restriction (M0922), process and device authentication (M0813), user account management (M0918), user training (M0918), and validation of program inputs (M018).

- ## BP-IDS

This tool detects anomalies in business process flows. It must have anti-virus (M0949), exploit protection (M0950), and watchdog timers (M0815).

- ## CVIAT

It is a tool to assess vulnerabilities. It must audit (M0947) and have a threat intelligence program (M0919).

- ## SIEM_CISOC

Collects security alerts and correlates them in real time. Must have antivirus (M0949), exploit protection (M0950), and threat intelligence program (M0919).

- ## RATING-OT

This tool performs risk analysis in OT environments. As mitigations it must perform an audit (M0947) and perform vulnerability scanning (M0916).

- ## SecurGrid

This is a tool that performs impact assessment. This tool does not have mitigations.

- ## FMLonIDS

Performs federated learning on IDS. It must have anti-virus (M0949), have filter for traffic (M0937), and prevent network intrusion (M0931).

- ## HEIMDALL

This is a tool that allows vulnerability assessments to be carried out. This tool must have a threat intelligence program (M0919) and perform vulnerability scans (M0916).

- ## APEN

This is a tool for advanced penetration testing. It must be audited (M0947), have network traffic filters (M0937), have a threat intelligence program (M0919) and perform vulnerability scans (M0916).

- ## ATRS

This is a tool for advance resistant tampering storage. Mitigation is to perform data backup (M0953) and prevent data loss (M0803).

- ## MDPI

It is a tool that has a situational awareness dashboard. It should be audited (M0947), prevent data loss (M0803), have exploit protection (M0950), have limited mitigations (M0816), prevented network intrusion (M0931), and had a threat intelligence program (M0919).

- ## SAPPAN

It is a repository of incident notification procedures. It has to have a threat intelligence program (M0919).

4.2 Alignment with Selected Standards and Frameworks

Next, in this section, the relationship between the previously identified mitigations and the IEC 62443 standard is analysed. In this way, it can be seen which FRs have the most mitigations. These results are collected in Table 3.

Table 3: Relation between MITRE and IEC 62443

MITRE ID	IEC 62443 part
M0801	3-3 SR2.1, 4-2 CR2.1
M0936	3-3 SR1.11, 4-2 CR2.11
M0915	---
M0949	3-3 SR3.2, 4-2 CR3.2
M0913	---
M0948	3-3 SR5.4, 4-2 CR5.4
M0947	3-3 SR3.4, 4-2 CR3.4
M0800	3-3 SR2.1, 4-2 CR2.1
M0946	4-2 CR3.14
M0945	3-3 SR3.4, 4-2 CR3.4
M0802	3-3 SR3.1, 4-2 CR3.1
M0953	3-3 SR7.3, 4-2 CR7.3
M0803	3-3 SR4.1, 4-2 CR4.1
M0942	3-3 SR7.7, 4-2 CR7.7
M0808	3-3 SR4.1, 4-2 CR4.1
M0941	3-3 SR4.1, 4-2 CR4.1
M0938	3-3 SR3.2, 4-2 CR3.2
M0950	3-3 SR3.2, 4-2 CR3.2
M0937	3-3 SR5.1, 4-2 CR5.1
M0804	3-3 SR1.1, 4-2 CR1.1
M0935	3-3 SR5.1, 4-2 CR5.1
M0934	3-3 SR3.2, 4-2 CR3.2
M0805	---
M0806	3-3 SR1.6, 4-2 CR1.6
M0816	---
M0932	3-3 SR1.7, 4-2 CR1.7
M0807	---
M0931	3-3 SR6.2, 4-2 CR6.2
M0930	3-3 SR5.1, 4-2 CR5.1
M0928	3-3 SR7.7, 4-2 CR7.7
M0809	3-3 SR4.1, 4-2 CR4.1
M0810	---
M0927	3-3 SR1.5, 4-2 CR1.5
M0926	3-3 SR1.3, 4-2 CR1.3
M0811	---

M0922	3-3 SR2.1, 4-2 CR2.1
M0944	3-3 SR7.7, 4-2 CR7.7
M0924	3-3 SR2.1, 4-2 CR2.1
M0921	3-3 SR2.4, 4-2 CR2.4
M0812	---
M0954	3-3 SR7.7, 4-2 CR7.7
M0813	3-3 SR1.2, 4-2 CR1.2
M0920	---
M0814	3-3 SR7.7, 4-2 CR7.7
M0817	---
M0919	---
M0951	4-2 CR3.10
M0918	3-3 SR1.3, 4-2 CR1.3
M0917	---
M0818	3-3 SR3.5, 4-2 CR3.5, 3-3 SR3.6, 4-2 CR3.6
M0916	---
M0815	4-2 CR7.2
M0801	3-3 SR2.1, 4-2 CR2.1
M0936	3-3 SR1.11, 4-2 CR2.11
M0915	---
M0949	3-3 SR3.2, 4-2 CR3.2
M0913	---
M0948	3-3 SR5.4, 4-2 CR5.4
M0947	3-3 SR3.4, 4-2 CR3.4
M0800	3-3 SR2.1, 4-2 CR2.1
M0946	4-2 CR3.14
M0945	3-3 SR3.4, 4-2 CR3.4
M0802	3-3 SR3.1, 4-2 CR3.1
M0953	3-3 SR7.3, 4-2 CR7.3
M0803	3-3 SR4.1, 4-2 CR4.1
M0942	3-3 SR7.7, 4-2 CR7.7
M0808	3-3 SR4.1, 4-2 CR4.1
M0941	3-3 SR4.1, 4-2 CR4.1
M0938	3-3 SR3.2, 4-2 CR3.2
M0950	3-3 SR3.2, 4-2 CR3.2
M0937	3-3 SR5.1, 4-2 CR5.1
M0804	3-3 SR1.1, 4-2 CR1.1
M0935	3-3 SR5.1, 4-2 CR5.1
M0934	3-3 SR3.2, 4-2 CR3.2
M0805	---
M0806	3-3 SR1.6, 4-2 CR1.6
M0816	---
M0932	3-3 SR1.7, 4-2 CR1.7
M0807	---
M0931	3-3 SR6.2, 4-2 CR6.2
M0930	3-3 SR5.1, 4-2 CR5.1

M0928	3-3 SR7.7, 4-2 CR7.7
M0809	3-3 SR4.1, 4-2 CR4.1
M0810	---
M0927	3-3 SR1.5, 4-2 CR1.5
M0926	3-3 SR1.3, 4-2 CR1.3
M0811	---
M0922	3-3 SR2.1, 4-2 CR2.1
M0944	3-3 SR7.7, 4-2 CR7.7
M0924	3-3 SR2.1, 4-2 CR2.1
M0921	3-3 SR2.4, 4-2 CR2.4
M0812	---
M0954	3-3 SR7.7, 4-2 CR7.7
M0813	3-3 SR1.2, 4-2 CR1.2
M0920	---
M0814	3-3 SR7.7, 4-2 CR7.7
M0817	---
M0919	---
M0951	4-2 CR3.10
M0918	3-3 SR1.3, 4-2 CR1.3
M0917	---
M0818	3-3 SR3.5, 4-2 CR3.5, 3-3 SR3.6, 4-2 CR3.6
M0916	---
M0815	4-2 CR7.2

After reviewing this analysis, the majority of mitigations (9) are related to FR1 (Identification and Authentication Control), followed by FR3 (System Integrity) with 8 mitigations. FR7 (Resource Availability) has 7 associated mitigations, FR2 (Use Control) with 5 and FR4 (Data Confidentiality) and FR5 (Restricted Data Flow) with 4. Finally, FR6 (Time Response to Events) has 1 associated mitigation. With this information, improvements could be made to the tools if they are to be certified in the future, as when certifying a system or product, it must be ensured that all necessary mitigations are correctly implemented.

5 Questionary

In order to find out about the development of the tools and the knowledge and use of the IEC 62443 standard by the companies that have developed the product, a questionnaire was sent to them. For that, we have asked 8 questions to the partners:

- Do you know the certificate scheme of IEC 62443?
- Is your company's lifecycle certificate?
- Even if it is not certified, in order to certify a tool, it is necessary that its entire lifecycle has been carried out in accordance with the standard. Has this been done? If no explain why? If yes explain how?
- Do you follow and collect information on the whole process of the tool's development (requirements definition, design, development, implementation...)? This is necessary according to the standard IEC 62443.
- Have you tested the tool against each test that the IEC 62443 standard sets in testing section? Why?
- Are you going to check the recommendations given to each tool in deliverable 8.8? If they are not fulfilled, are you going to correct them? Why?
- Are you interested in certifying the tool?
- Has this taken into account or are you aware of that (certifying the tool)?

We received the response of 12 partners, regarding 18 tools (HEIMDALL, CyberRange, APEN, CVIAT, FML on IDS, RATING-OT, SED, ALIDA, MDPI, SAPPAN, ARTEMIS, BP-IDS, SIEM_CISOC, ATRS, Attack-defense Simulator, MIDA tool, SecurGrid, DSS and ZIV Event Detector).

Most partners know the standard IEC 62443 and %35.7 have the lifecycle certificate, but not with the standard IEC 62442. They are certificated by another standard such as ISO 27001, UNE EN ISO 9001 CVSS 4.0…

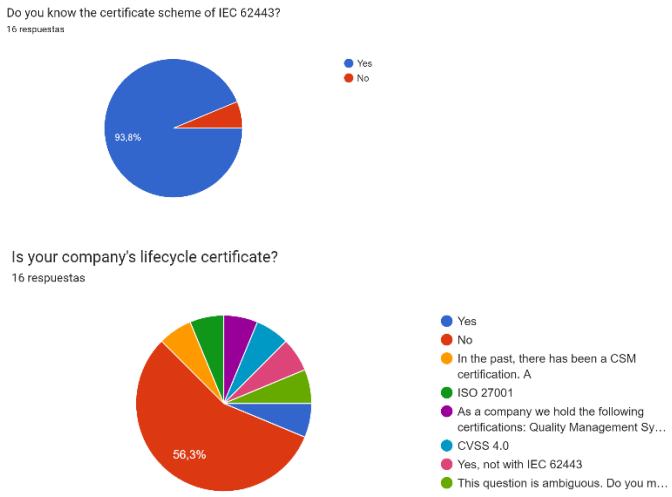

Figure 1: Graphics of questionary answers about knowledge of IEC 62443 and company´s lifecycle

With the certified lifecycle, even if it is not IEC 62443 certification, several improvements in the safety of the products being developed are achieved. On the one hand, it helps to identify risks more effectively so that they can be mitigated more easily. In addition, it allows the implementation of best practices to ensure that all systems/products are designed, developed, operated, and maintained in a way that always guarantees safety. In addition, having a certificate in place gives confidence to customers, as it is an indication that the company is following best practice and enhances its reputation in the marketplace. On the other hand, it standardises the product/system process and all the documentation that is generated, increasing efficiency and consistency in operations. As controls are increased and preventative measures are taken, security incidents are reduced, reducing downtime and costs associated with security breaches.

Although they did not have a certified lifecycle, it has been consulted whether the tool has been developed following the IEC 62443 standard. Only the Attack-defense Simulator tool has been developed following the secure by design implementation in their development. We conducted verification and validation testing to verify that our code functions as intended under various scenarios and conditions. In the other cases there are several reasons why the design and development has not been carried out according to IEC 62443. The other tools have not been developed following the standard but the rationale for this has been reviewed. On the one hand, HEIMDAL is a tool that has been worked on for several years, so it has been developed taking into account best practices, but the standard has not been specifically followed. Moreover, the cost of maintaining a certification over time is very high. In other cases, such as in the ZIV Event Detector and APEN tools, part of the development has been done following the instructions of the standard, but part has not, even so, in this case the company is ISO 27001 certified, but the standard has not been strictly followed. In other cases, as in the case of the CVIAT and FML tools, they believe they are aligned with the basic requirements of the standard, as they are certified to ISO 9001:2015, ISO 14001:2015 and ISO/IEC 27001:2017. On the other hand, in the case of the SecurGrid, BP-IDS, SIEM CISOC and ATRS tools, there is no interest in certifying them, so the process has not been followed taking into account IEC 62443. In other cases, such as SAPPAN, they consider that following the standard can be very complex and is not aligned with the needs of the organisation, and in the case of MIDA, they have followed the company's internal control guidelines, but there is no business interest in certification. In the case of DSS tool, its TRL does not reach 7 so as it is not going to be certificated, they do not develop it according the exact requirements of IEC 62443. Finally, in the case of RATING-OT, SED, ALIDA, and MDPI, they have not been developed with any certification in mind, as the development carried out in CyberSEAS is a prototype, which will be developed in the future for market launch.

Furthermore, if certification is to be obtained in the future, it is necessary to have sufficient evidence of the development of the product/system. Although the IEC 62443 standard has not been followed in the development of all the tools, all the necessary documentation has been collected in order to have evidence of how the tool has been designed and developed. Furthermore, in order to certify a product/system it is necessary to carry out the necessary security tests. Therefore, although not all the tests required by the IEC 62443 standard have been followed, several tests have been carried out, some of which are in accordance with the standard and others required by the client.

Finally, companies were asked about their interest in certifying the tool and the result was that 50% of the companies that responded to the questionnaire are interested in certifying the product, although they are not going to do so in the short term. Therefore, all the improvements that are made to the tools in terms of complying with the standard will make it easier for companies to certify the product in the future.

6 Recommendations for Cyber-Resilience and Certification

Some recommendations that have been obtained from the analysis are listed below. Although there is currently no interest in certifying the tools, these recommendations will help to make the process easier if they are to be certified in the future.

6.1Strategies for Addressing Cybersecurity Gaps

When analysing whether the system complies with the requirements of the cybersecurity standards, it is first necessary to detect the gaps it has. To do this, it is advisable to analyse the main requirements of the standard and the FRs that must be met, as this will provide information on what needs to be changed in the system in order to comply with them. First of all, the SL that each tool has to fulfil must be analysed, as the requirements are different for each SL. The SL has four levels:

- SL1: unauthorised disclosure of information that can occur through uncontrolled eavesdropping and casual exposure must be prevented.
- SL2: unauthorised disclosure of information is prevented, but in this case to an entity that is actively seeking such information using low resources, low motivation, and unspecified skills.
- SL3: unauthorised disclosure of the information must be prevented to an entity that is actively seeking it, with sophisticated means, medium resources, IACS-specific skills, and moderate motivation.
- SL4: unauthorised disclosure of information to an entity that is actively seeking, with sophisticated means, high resources, IACS-specific skills, and high motivation should be prevented.

6.2Integration of CyberSEAS Tools and Solutions

In the previous section, the mitigations associated with the FRs of the standard for each tool have been listed. Therefore, the recommendations are based on this result. As all mitigations are not associated with a FR of the standard, only those that are aligned with the standard are described. In addition, some mitigations are aligned with the same requirement.

- ALIDA: SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code) and SR6.2/CR6.2 (Continuous monitoring). To meet these requirements, malware detection software must be installed, regularly updated, and all applications must be monitored for each alert.
- SED: SR2.4/CR2.4 (Mobile code) and SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code). To meet these requirements, usage policies must be defined, malware detection software must be installed and regularly updated.

- MIDA: SR1.11/CR1.11 (Unsuccessful login attempts), SR2.1/CR2.1 (Authorisation enforcement), SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code), SR3.4/CR3.4 (Software and information integrity), SR5.1/CR5.1 (Network segmentation), and SR5.4/CR5.4 (Application partitioning). To meet the requirements it will be necessary to have account control, authorise each user to the space they can access, define usage policies, install malware detection software, use digital signatures, zone the network to control access and have a modular architecture.
- ARTEMIS: SR1.2/CR1.2 (Software process and device identification and authentication), SR1.3/CR1.3 (Account management), SR2.1/CR2.1 (Authorisation enforcement); SR3.5/CR3.5 (Input validation) and SR3.6/CR3.6 (Deterministic output). To accomplish this, digital certificates will be needed for identification and authentication, proper account management, authorisation of what each user can access, input validation and output prevention to detect errors.
- BP-IDS: SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code), and CR7.2 (Resource management). In order to meet these requirements, malware detection software must be installed, regularly updated and, in the case of components, the resources available to them must be properly managed.
- CVIAT: SR3.4/CR3.4 (Software and information integrity). The use of digital signatures is recommended to ensure the integrity of data and applications.
- SIEM_CISOC: SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code). To meet these requirements, malware detection software must be installed and regularly updated.
- RATING-OT: SR3.4/CR3.4 (Software and information integrity). The use of digital signatures will be recommended to guarantee the integrity of data and applications.
- FMLonIDS: SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code), SR5.1/CR5.1 (Network segmentation) and SR6.2/CR6.2 (Continuous monitoring). To meet these requirements, malware detection software must be installed, regularly updated, the network must be zoned, and the status must be continuously monitored.
- APEN: SR3.4/CR3.4 (Software and information integrity) and SR5.1/CR5.1 (Network segmentation). The use of digital signatures will be recommended to guarantee the integrity of data and applications and to zone the network.
- ATRS: SR4.1/CR4.1 (Information confidentiality) and SR7.3/CR7.3 (Control system backup). To maintain data confidentiality, it is recommended to encrypt communications and it will also be necessary to store data on a regular basis, so that in the event that something is lost it can be recovered.
- MDPI: SR3.2 (Malicious code protection)/CR3.2 (Protection from malicious code), SR3.4/CR3.4 (Software and information integrity), SR4.1/CR4.1 (Information confidentiality), and SR6.2/CR6.2 (Continuous monitoring). To meet these requirements, malware detection software must be installed, regularly updated, digital signatures must be used to ensure the integrity of data and applications, and the status must be continuously monitored.

6.3Roadmap for Certification

Obtaining IEC 62443 certification involves understanding the standards, defining the scope of the assessment, and conducting a gap analysis to evaluate current cyber security activities. Organisations must then enhance their cybersecurity program, implement the necessary security controls, and conduct internal audits to ensure compliance. To this end, it is important to clarify that in order to certify a product it is necessary to comply with all the requirements of the standard. Therefore, during this section, the tools have been analysed and the first points to be met have been identified. In the case of certification, it will be necessary to carry out a more exhaustive analysis of the entire development of the tools, but this analysis would be a starting point.

- ## Steps for Implementing Recommendations

To implement the recommendations, the IEC 62443 standard must first be fully reviewed to understand the specific requirements and guidelines applicable to the organization's products and processes. Moreover, it is necessary to define the limits of the certification and identify areas for improvement. Improving the cybersecurity program includes developing a plan to address identified deficiencies and prioritizing actions based on risk analysis and impact analysis. Additionally, it is necessary to implement security controls and conduct regular internal audits to ensure compliance or implement corrective actions. In addition, before starting the certification process with the certification entity, the documentation and all processes must be exhaustively analysed. Finally, the application for certification phase involves the preparation and submission of all necessary documentation and commitment to a certification entity for formal assessment.

- ## Timelines and Responsibilities

The time that a company needs to perform the certification phase will depend on the state of its procedures; if it has implemented them according to the standard, it will have the previous work done and will be able to start with the certification. For this, an internal audit will take a few months (2-4 months) and then the certification phase will start (2-6 months) which involves preparing the application for certification and undergoing a formal assessment.

- ## Monitoring and Reporting

Continuous monitoring implies the implementation of automated tools to detect and respond to security incidents in real-time. In addition, it is necessary to analyse the status of security measures on an ongoing basis. It is important to continue to make improvements and review all procedures through audits to maintain certification. Audit reports are kept in detail, tracking the implementation of corrective measures and their effectiveness.

7 Roadmap towards cyber-resilient Digitalised EPES

This section describes how the digitization of EPES has evolved and the importance of sharing all the information securely.

7.1 Evolving Digitalisation of EPES

IT-OT convergence is one of the topics that need to be addressed as the EPES evolves to a decarbonized, sector-coupled, and digitalized energy system. The availability of large amounts of data at the edge of the grid, use of cloud and edge computing as well AI technologies while enabling efficient and secure operation makes EPES landscape more vulnerable to cyber-threats.

The scalability of cloud solutions has facilitated the adoption of cloud-based platforms, such as energy management solutions, at both the consumer and grid operator levels. This widespread adoption necessitates that cybersecurity standards and frameworks in the energy sector explicitly address the cybersecurity of cloud systems within the EPES supply chain. Some of the existing standards and frameworks as discussed in Section 2.2, already incorporate cloud security.

For instance, in Germany, the Cloud Computing Compliance Controls Catalogue (C5) [12] from the Federal Office for Information Security (BSI) outlines minimum requirements for secure cloud computing. This catalog serves as a valuable resource for small and medium-sized companies in the energy sector when selecting a cloud service provider. Similarly, the Network and Information Systems Directive (NIS2) in the EU mandates that cloud customers use only cloud services certified under the European Cybersecurity Certification Scheme for Cloud Services (EUCS). Moving forward, it is crucial to enhance awareness of cloud certification schemes and other cybersecurity and data privacy measures among end-users, such as those utilizing Home Energy Management Systems (HEMS). Strengthening this awareness will contribute to ensuring the cyber-resilience of EPES. It is recommended that targeted educational initiatives and resources be developed to inform end-users about the importance of cloud security and data privacy, thereby promoting a more secure and resilient energy sector.

Similar issues exist when it comes to IoT devices such as smart transformers, which are a key technology towards enabling the transition towards a digitalized energy system. In this area, the emphasis is placed on the need for standardized security protocols, robust data privacy regulations, and certification schemes for IoT technologies used in the energy system.

7.2 Energy Data Spaces and Information Sharing

Cybersecurity in the context of data exchange is to be considered from two different perspectives; firstly, the sharing of energy data itself and secondly the sharing of cyberthreat intelligence (CTI) information between various stakeholders. Deliverable 6.8 of this project presents information sharing mechanisms, cooperation and communication strategies and tools for the exchange for reports focusing on EPES operators and CERTS.

The transition towards a decarbonized energy system creates the need for additional flexibility options to enable coordination between stochastic generation and demand. Energy data sharing will play a key role in enabling these flexibility solutions and is thus one of the key points in the EU action plan on digitalizing the energy system. Standardization, Interoperability as well as data security and privacy are the challenges that need to be addressed to facilitate energy data sharing. Data Space technology offers a technical solution to address these challenges while enabling Data protection by design. The common European Energy Data Space can provide a technological solution for EPES stakeholders to share energy as well as CTI related data amongst each other as well as with other participants in data spaces such as a Managed Security Service Providers (MSSPs) or Energy ISACs. Nonetheless, as highlighted in the ENISA Report on 'Engineering personal data protection in EU data spaces', robust cybersecurity, and data privacy engineering when it comes to the practical deployment of EU data spaces. The report can provide guidelines and recommended building blocks for data protection engineering for energy data spaces going beyond GDPR compliance. The report also highlights the need for cybersecurity engineering in the deployment of EU data spaces.

8 Conclusions

In an era where the digital and physical worlds are increasingly intertwined, security in the energy sector has never been more critical. This report highlights the vital importance of taking a comprehensive approach to cybersecurity, integrating established standards such as IEC 62443 and complying with regulatory frameworks such as the NIS2 Directive and the forthcoming Cyber Resilience Act.

The importance of the energy sector to national security and economic stability requires an effort to mitigate cybersecurity risks. The recommendations in this report are aligned with the IEC 62443 standard, organisations can achieve certification in the future.

To this end, this document contains the analysis of CyberSEAS tools and infrastructures where the requirements are mapped to MITRE and related to the requirements of the IEC 62443 standard. This work has been done with the aim that all partners of the consortium can have an overview of what they need to consider if they want to go through a certification process in the future. This would be the starting point for certification, as organisational changes and various specific tests required by the IEC 62443 standard are also necessary.

Moreover, a questionnaire has been carried out to the tool providers to check their knowledge and interest in obtaining the IEC 62443 certificate. This analysis has identified that no tool will be certified at the moment, but that it may be the case that in the future they will want to be certified. For that reason, when developing a tool, it is necessary to keep several aspects in mind from the initial identification of requirements. Moreover, it will be necessary to implement secure development practices and version control. On the other hand, it will be necessary to make a correct segmentation of the network and define the security profiles managing who can access each zone. Furthermore, it will be necessary to assess the confidentiality of the system to detect if it is necessary to encrypt it. Also, it will be necessary to plan the necessary tests to demonstrate that the system/product is secure. Finally, it will be crucial to document the whole process thoroughly to demonstrate that the whole process has been done according to the standard. The decision to not certify it for the moment has been taken by the tool providers, as certification involves an effort that they do not consider necessary for present. For this reason, this document provides guidelines for future certification.

In conclusion, the intersection of these standards provides a comprehensive roadmap for achieving robust cyber security in the energy sector. By following the detailed steps for implementation and maintaining rigorous monitoring practices, companies or organisations can significantly improve their cybersecurity capabilities. By prioritizing cybersecurity, the energy sector can secure its critical infrastructures, protect against malicious activity, and maintain a continuous and reliable supply of energy.

9 References

[1] *Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows,* 2024.

[2] S. Staff, «Energy sector faces 39% of critical infrastructure attacks,» 19 09 2023. [Online]. Available: https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks.

[3] ISA, «The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards,» [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[4] E. Commision, «Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive),» 14 09 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. [Atzitze-data: 14 05 2024].

[5] E. Commision, «Cyber Resilence Act Process,» 03 2024. [Online]. Available: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html.

[6] E. Commission, «Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive),» [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[7] I. Goel, «Compare and Contrast: NIS2 Directive & Cyber Resilience Act,» 22 02 2024. [Online]. Available: https://www.gira.group/post/compare-and-contrast-nis2-directive-cyber-resilience-act. [Atzitze-data: 14 05 2024].

[8] S. G. T. F. -. E. G. 2. -. CYBERSECURITY, «Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report,» 2019.

[9] «EE-ISAC - European Energy - Information Sharing & Analysis Centre Home,» [Online]. Available: https://www.ee-isac.eu/. [Atzitze-data: 06 06 2024].

[10] T. Wallis eta R. Leszczyna, «EE-ISAC—Practical Cybersecurity Solution for the Energy Sector,» *Energies,* %1. bol.15, %1 zk.6, 16 03 2022.

[11] Incibe, «FAQ NIS2,» [Online]. Available: https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2.

[12] «Cloud Computing Compliance Criteria Catalogue – C5:2020,» [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=3.

[13] IoT-NGIN, «D9.1 - Project Handbook,» H2020-957246 IoT-NGIN Deliverable Report, 2020.