D3.2 CyberSEAS Technical Requirements, SELP Requirements and System Specification

DOCUMENT	D3.2	**WORKPACKAGE**	WP3
DELIVERABLE STATE	**FINAL**	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V1.0	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	16/08/2022	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	**CO**	**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)
TOPIC	SU-DS04-2018-2020 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	WP3
DELIVERABLE TYPE	**R Document, report**
DISSEMINATION LEVEL	**CO Confidential**
DELIVERABLE STATE	**FINAL**
CONTRACTUAL DATE OF DELIVERY	31/07/2022
DOCUMENT TITLE	D3.2 CyberSEAS Technical Requirements, SELP Requirements and System Specifications
AUTHOR(S)	Lasse Nitz, Mehdi Akbari Gurabi, Avikarsha Mandal
REVIEWER(S)	INF, ZIV
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	FUNCTIONAL REQUIREMENTS, TECHNICAL SPECIFICATIONS, SELP REQUIREMENTS

Document History

Version	Date	Contributor(s)	Description
V0.1	10/04/2022	FRAUNHOFER	ToC
V0.2	30/06/2022	TLX	SELP requirements
V0.3	04/07/2022	FRAUNHOFER, ENG, CINI, ACS, GT, IKE, ICS, SIMAVI, SYN, WIN, ZIV	Aggregation of pilot partners' inputs
V0.4	06/07/2022	FRAUNHOFER	Revision of the document structure
V0.5	11/07/2022	FRAUNHOFER, ENG, CINI, ACS, GT, IKE, ICS, SIMAVI, SYN, WIN, ZIV	Update of partners' inputs based on feedback
V0.6	14/07/2022	FRAUNHOFER	First compelete draft
V0.7	15/07/2022	FRAUNHOFER	Ready to quality check
V0.8	19/07/2022	FRAUNHOFER	Ready to quality check , incorporate updates
V0.9	28/07/2022	FRAUNHOFER	Incorporate review feedback (release candidate)
V1.0	15/08/2022	FRAUNHOFER	Final version

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

(Non-)Functional	Functional and Non-Functional
2FA	Two Factor Authentication
AI	Artificial Intelligence
API	Application Programming Interface
APIDS	Application Protocol-Based Intrusion Detection System
CCTV	Closed-Circuit Television
CER	Critical Entities Resilience
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
COTS	Commercial-off-the-Shelf Solution
CTI	Cyber Threat Intelligence
DBMS	Database Management System
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDR	Endpoint Detection and Response
EPES	Electrical Power and Energy System
EU	European Union
FAN	Field Area Network
GDPR	General Data Protection Regulation
HIDS	Host-Based Intrusion Detection System
HR	Human Resources
IAM	Identity and Access Management
ID	Identifier
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IEC	Internal Ethics Committee
IED	Intelligent Electronic Device
IM	Information Management
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
KPI	Key Performance Indicator
MAC	Media Access Control
MDR	Managed Detection and Response

MFA	Multi-Factor Authentication
NAN	Neighbourhood Area Network
NFC	Near Field Communication
NIDS	Network Intrusion Detection System
NTP	Network Time Protocol
OT	Operational Technology
PAM	Privilege Access Management
PES	Power and Energy System
PIDS	Protocol-Based Intrusion Detection System
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSA	Platform Security Architecture
RRI	Responsible Research and Innovation
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SE	Social Engineering
SELP	Societal, Ethical, Legal and Privacy
SEP	Societal, Ethical and Privacy
SGAM	Smart Grid Architecture Model
SIEM	Security Information and Event Management
SMS	Short Message Service
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
SOP	Security Operation Playbook
TSO	Transmission System Operator
UBA	User Behaviour Analytics
VPN	Virtual Private Network
WAN	Wide Area Network
WP	Work Package
XDR	Extended Detection and Response

Executive Summary

This deliverable deals with the documentation of functional and non-functional requirements for the CyberSEAS pilots as well as the technical specification derived from them. It constitutes the bridge from task T3.1 and its deliverable D3.1, which focuses on the definition of pilot scenarios and high-level requirements, to task T3.3, which uses the content of this deliverable as input for the design of the toolset architecture and integration approach. Additionally, metrics for evaluating compliance of development activities with the identified requirements have been documented.

Further, this deliverable documents the societal, ethical, legal and privacy (SELP) value framework for the CyberSEAS project, specific SELP values and requirements derived from relevant documents (such as the EU framework for Responsible Research and Innovation, and the General Data Protection Regulation). Additionally, a general methodology for applying and monitoring SELP values within the project is proposed.

1 Introduction

The content of this deliverable consists of two major parts: The specification of the high-level requirement defined in deliverable D3.1 from a functional and technical perspective (which is introduced in detail as part of the methodology section below), and the definition of the SELP value framework of the CyberSEAS project. Taking the result of D3.1 as input, a specification process has been documented and applied for each pilot. The process started with the identification of functional components based on high-level requirements and pilot scenarios. From these components, both functional and non-functional requirements have been derived to shape the functional view of the desired system. This deliverable further contains a documentation of metrics that can be used to measure compliance with the identified requirements. In the next step, the (non-)functional requirements have been technically specified, including the identification and mapping of potentially suitable Commercial-off-the-Shelf Solutions (COTS) and/or security mechanisms, relevant constraints and parameters for them, and relevant CyberSEAS tools. The results of this specification process are documented per pilot in this deliverable.

Additionally to the functional and technical view, the societal, ethical, legal and privacy aspects have been considered and documented in this deliverable. The SELP requirements aim to align the CyberSEAS project with European legislation as well as ethical and socio-cultural values. To ensure compliance with the SELP requirements, it has to be addressed how they can be formalised and monitored in practice. In response to these questions, this deliverable documents the identification of relevant sources of SELP norms, specific SELP values, specific SELP requirements based on relevant legislation, and the CyberSEAS SELP framework. This framework follows the theory of Value Sensitive Design by establishing a normative framework for future development activities in CyberSEAS. To ensure compliance of pilot activities with this framework, a matching methodology has been defined. Further, the SELP evaluation template for pilot description, privacy risk assessment and approval process is attached in the annex.

1.1 Connections to other Deliverables

The content of this document has relations to several other CyberSEAS deliverables. The section on the (non-)functional requirements and technical specification takes the results of task T3.1 and its deliverable D3.1 as input to further refine the high-level requirements. The identification of suitable COTS and security functions additionally utilises the survey performed for deliverable D2.4. The functional and technical views derived as part of this deliverable will further serve as input for task T3.3 and its deliverables D3.3 and D3.4, which focus on the CyberSEAS toolset architecture and integration. Moreover, the documentation serves as a reference for implementation work packages (WPs), for example via the documented non-functional requirements.

Further, this deliverable is related to task T2.5 and its deliverables D2.5 and D2.6, which document the privacy risk mitigation plan of the CyberSEAS project. Specifically, societal, ethical and privacy (SEP) requirements have been addressed in detail in D2.5 and an initial data protection impact assessment has been carried out. In contrast to D2.5, this deliverable also considers additional legal aspects and thus extends the content of D2.5. Other related

deliverables are D10.1 and D10.2, focusing on human involvement in CyberSEAS and the processing of personal data, respectively.

1.2 Structure of this Deliverable

Regarding the structure of this deliverable, first, the functional requirements and technical specification are presented. This section starts with a description of the methodology used to derive respective results and also includes a definition of the key terms used. The methodology description is followed by a table-style documentation of (non-)functional requirements and the technical specification per pilot. Suitable metrics to quantify compliance of development activities with the identified requirements are documented in the subsequent section. Next, the SELP requirements are documented, including the SELP value framework for CyberSEAS, the identification of cross-cutting SELP requirements, and the SELP implementation approach for CyberSEAS. Lastly, a conclusion is given. The annex contains the template of the assessment framework from deliverable D2.5 to facilitate cross-checking.

2 (Non-)Functional Requirements and Technical Specifications

This section begins with the derivation of functional and non-functional requirements from the high-level requirements documented in D3.1. The functional view created through this process is then further specified technically as part of the technical specification. In the following, first, the used methodology is briefly presented. Next, the result of this process is documented per pilot, each of which has a separate table for the functional view and the technical view.

2.1 Methodology

This deliverable builds on the high-level requirements documented in deliverable D3.1 and further specifies them regarding functionality and matching technologies. Similar to D3.1, this deliverable distinguishes between the different pilots and hence documents the (non-)functional requirements and technical specification per pilot in respective sub-sections. The knowledge gained through this specification process will later be used as input for the architecture design in task T3.3 and its two deliverables D3.3 and D3.4. The goal of the methodology used in this section is hence the description of a process, which allows to derive and document the intermediate results of this specification process in a structured step-by-step way.

The chosen methodology follows a straight-forward flow, in which each step further specifies the result of the previous one. The flow and its key intermediate results are depicted in Figure 1. Taking the high-level requirements from D3.1 as input, the methodology consists of two main results:

1. The description of the functional (and non-functional) requirements.
2. The identification of suitable technical components and potentially suitable technologies which implement them.

The first one is referred to as the "(non-)functional requirements" part, and the second one as the "technical specification". Conceptually, the derived results become more specific the further down they are in the depicted flow.

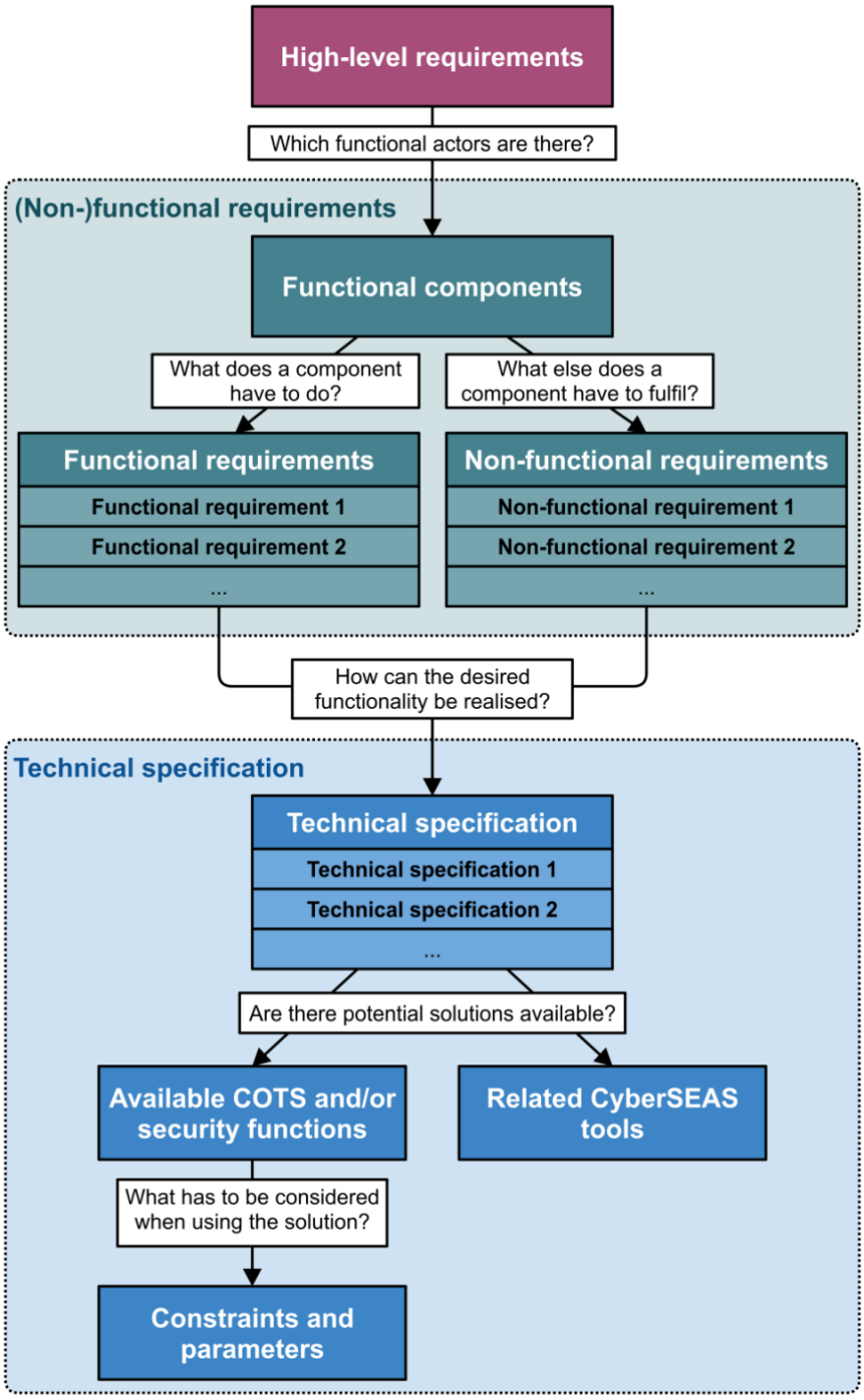

Figure 1: Overview of the methodology used for identifying (non-)functional requirements and the technical specification.

2.1.1 Functional and Non-Functional Requirements

The functional and non-functional requirements focus on the question of what must be done to achieve a high-level requirement. Neither functional nor non-functional requirements propose any specific approach or technology, but are related to a specific kind of functionality. While functional requirements directly describe such functionality or behaviour, the non-functional requirements can be considered as quality goals, which are relevant for the further specification of the desired system. Examples of non-functional requirements include real-time capability, compliance with specific standards, or specific properties such as interpretability, traceability, or interoperability.

For the identification of (non-)functional requirements, the following workflow has been used:

1. Based on the high-level requirements from D3.1, functional components are identified. Such a functional component can be seen as an abstract actor, which fulfils specific functionalities independent of any technology. It may interact with other functional components.
2. For each of the identified functional components, the relevant high-level requirements are documented.
3. The functionality of each functional component is further specified by identifying its functional requirements. This is done based on the high-level requirements, from which the specific functional component has been derived, and shapes the desired behaviour of the component. The key question that the functional requirements of a functional component aim to answer is what this component is supposed to do.
4. For each functional component, the non-functional requirements are derived. This further specifies the description of a functional component by defining relevant properties beyond its functionality, focusing more on the question of how the system should deliver the desired functionality. The non-functional requirements are hence closely related to quality attributes. The non-functional requirements are also of special interest for later implementation work packages in the project, as they can be seen as development requirements for systems, which aim to implement the functional component. For the sake of simplicity, we consider the collection of non-functional requirements to be part of the functional requirements process (cf. Figure 1), as it is applied on a similar abstraction level.

The result of this process has been documented in tables, which follow the format shown in Table 1.

Table 1: Template for the documentation of the (non-)functional requirements per pilot.

Functional Component ID	Functional Component	Related High-Level Requirement	ID of Derived Requirement	Type of Derived Requirement (Functional, Non-Functional)	Derived Requirement

2.1.2 Technical Specification

In contrast to the (non-)functional requirements, the technical specification aims to answer the question of how a (non-)functional requirement can be realised technically. It hence constitutes the step from the functional view ("What has to be done?") to the technical view ("How can it be done?") and by that further specifies the desired system.

The workflow for the technical specification takes the (non-)functional and high-level requirements as input and performs the following steps:

1. For each (non-)functional requirement, the technical specification is derived. A functional requirement might have to be specified via several technical specifications, as a specific functionality may require a collection of different technologies to interact.
2. For the derived technical specifications, relevant COTS and/or security functions are identified based on deliverable D2.4. These COTS and/or security functions are expected to provide suitable implementations of a technical specification and should at least be considered for the pilot architecture design.
3. To further document relevant considerations about the potential usage of identified COTS and/or security functions, the constraints and parameters relevant to the intended usage scenario in CyberSEAS are documented.
4. Additionally to COTS, also suitable CyberSEAS tools are identified for the technical specification based on the mapping of high-level requirements to tools in deliverable D3.1. This mapping is further refined by crosschecking with the tool data sheets, which have been provided by the respective tool owners for the CyberSEAS project.

The result of this process has been documented in tables, which follow the format shown in Table 2.

Table 2: Template for the documentation of the technical specification per pilot.

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-Shelf Solutions and/or Security Functions	Constraints and Parameters	Related CyberSEAS Tools

2.1.3 Output

The output of this process is a description of (non-)functional requirements and their mapping to relevant technologies as well as specific implementations of such technologies as COTS or CyberSEAS tools. This description will further be utilised in task T3.3 to define the CyberSEAS toolset architecture and integration approach.

2.1.4 ID Format

Unique IDs have been assigned to functional components and (non-)functional requirement per pilot. These IDs follow a format consisting of three parts, specifically a prefix, which determines the type of ID, an infix, which determines the associated pilot, and a suffix, which distinguishes different IDs of identical type within the same pilot.

Specifically, the IDs follow the format "prefix-infix.suffix". The potential values for each of these categories can be found in Table 3. As an example, the ID "FC-F.4" refers to the fourth functional component in the Finnish pilot, and the ID "Req-F.4.1" refers to the first (non-)functional requirement for this component. This ID format contains basic contextual information about what an ID refers to and also allows to later assign IDs to newly added components and requirements, if necessary.

Table 3: Overview of ID building blocks.

ID types (prefix)	
FC	Functional component
Req	(Non-)functional requirement
Pilot (infix)	
I	Italian pilot
S	Slovenian and Croatian pilot
R	Romanian pilot
F	Finnish pilot
E	Estonian pilot
Enumeration (suffix)	
For functional components: Running number of functional components in a pilot	Unique number among the entries with identical ID type and pilot. Functional component suffixes are assigned as running numbers within a pilot, starting at 1.
For (non-)functional requirements: Number of the functional component and the running number of the requirement, delimited by a dot	The (non-)functional requirements have been defined per functional component. The suffix for a (non-)functional requirement hence starts with the running number of the respective functional component, followed by the running number of the (non-)functional requirement for this component.

2.2 Italian Pilot

2.2.1 Functional Requirements and Non-Functional Requirements

Table 4: Functional and non-functional requirements for the Italian pilot

Funct. Comp. ID	Functional Component	Related High-Level Requirement	ID of Derived Req.	Type of Derived Req. (Functional, Non-Functional)	Derived Requirement
FC-I.1	Cabin	Avoid intrusion into the cabin	Req-I.1.1	Functional	Detection of unauthorized access
			Req-I.1.2	Functional	Promptly alert whether an intrusion takes place
			Req-I.1.3	Non-Functional	Real-time communication of intrusion alert
FC-I.2	Data storage	Tamper resistant storage support	Req-I.2.1	Non-Functional	Support of different levels of access to the data storage
			Req-I.2.2	Functional	Ability to restore a previous system state
			Req-I.2.3	Functional	Protection against unauthorized access
			Req-I.2.4	Non-Functional	Traceability of data modification
			Req-I.2.5	Functional	Visualize user activity logs and content processing logs
FC-I.3	Management software	Avoid intrusion into the IT network	Req-I.3.1	Functional	Promptly alert whether an intrusion takes place
			Req-I.3.2	Functional	Intrusion detection on software management system
			Req-I.3.3	Non-Functional	Traceability of data modification
			Req-I.3.4	Non-functional	Real-time communication of intrusion alert
FC-I.4	Decision support system	Guarantee support for the decision-making process of the IT personnel	Req-I.4.1	Functional	Early detection of an intrusion
			Req-I.4.2	Functional	Ability to differentiate decision support for different kind of cyberattack
			Req-I.4.3	Functional	Tracking of actions
			Req-I.4.4	Functional	Offline Risk Assessment for enhancing strategic protection of grid

			Req-I.4.5	Functional	Near real-time Risk Assessment for tactical protection of grid
			Req-I.4.6	Functional	Provide IT personnel with an updated Situational Awareness for rapid understanding of the status of the assets
			Req-I.4.7	Functional	Visualize attacker activities and movements inside the network
FC-I.5	SCADA system	To be promptly warned in case of an intrusion into the SCADA system	Req-I.5.1	Functional	Ability to early detect an intrusion
			Req-I.5.2	Non-Functional	Traceability of actions carried out by the attacker
			Req-I.5.3	Non-Functional	Integration with advanced tamper resistant storage to avoid data modification
FC-I.6	Disconnector	Impede the access to the disconnector to unauthorized people	Req-I.6.1	Functional	People detection near the disconnector
			Req-I.6.2	Functional	Promptly alert whether an intrusion takes place
			Req-I.6.3	Functional	Ability to restore a previous system state
			Req-I.6.4	Non-Functional	Real-time communication of damage alert
FC-I.7	Smart Meter	Avoid smart meter sabotage	Req-I.7.1	Functional	Ability to early detect anomalies
			Req-I.7.2	Functional	Promptly alert whether a sabotage takes place
			Req-I.7.3	Non-Functional	Real-time communication of alerts

2.2.2 Technical Specification

Table 5: Technical specification for the Italian pilot

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-Shelf Solutions and/or Security Functions	Constraints and Parameters	Related CyberSEAS Tools
Tamper resistant storage support	Support of different levels of access to the data storage	Two factor authentication	Entrust Duo Multi-Factor Authentication	Must verify the domain where TFA is used Phishing protections	ATRS

			Prove MFA		
			HID Global Identity and Access Management		
			ESET Secure Authentication		
			Ping Identity		
			TypingDNA Verify 2FA		
			Thales SafeNet Trusted Access		
			JumpCloud Protect		
			ManageEngine ADSelfService Plus		
			Twilio Authy		
			OKTA Adaptive Multi-Factor Authentication		
		Role management	Login Radius	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	-
			Award force Role management		
			Orange Scrum role management		
	Ability to restore a previous system state	Automated creation of backups	IBM data protection	Offsite and offline solutions	-
			Segment		
			RuleX		
			Acronis		

	Protection against unauthorized access	Encryption	Atakama file encryption software Zero trust security by NordLayer AxCrypt Premium Folder Lock CryptoForge	Known secure algorithms only	PKI
	Traceability of data modification	Logging	Sydecon	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements.	-
	Visualize user activity logs and content processing logs	Data visualization and data analytics	EventLog Analyzer Google analytics SmartLook	-	-
Avoid intrusion into the cabin	Detection of unauthorized access	Access control	Virtual Business Assistant	-	ARTEMIS
	Promptly alert whether an intrusion takes place	Alert system based on sensors	Oaktree products; Digital alert systems; HSS engineering Ascom alert management system	Ability to detect people and alert operators	BP-IDS ARTEMIS
	Real-time communication of intrusion alert	Polling technique Stream data mining Access control via badge	Splunk enterprise SignalR gRPC Desk Alert	Ability to detect people and alert operators	SIEM
Avoid intrusion into the IT network	Promptly alert whether an intrusion takes place	Alert system based on Threat detection	Oaktree products Digital alert systems HSS engineering	Ability to detect intrusion	BP-IDS ARTEMIS

			Ascom alert management system	alerting operators	
		Anomaly detection	Ascom alert management system	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS ARTEMIS
	Intrusion detection on software management system	DNS filtering	Perimeter 81	On-Prem solutions only	BP-IDS
		Firewall	SIEM system		
		Signature-based method	NIDS		
			HIDS		
		Anomaly-based method	PIDS		
			APIDS		
			SolarWinds Security Event Manage		
			Bro		
			OSSEC		
			Security onion		
			Verve security		
	Traceability of data modification	Logging	Sydecon	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	SIEM
	Real-time communication of intrusion alert	Polling technique	Splunk enterprise	Ability to detect people	SIEM
			SignalR		

		Stream data mining		and alert operators	
			gRPC		
			Desk Alert		
	Visualisation of alert	Creation of a dashboard to visualize alert	-	Warn users about detected intrusion	Situational awareness (ENG)
Guarantee support for the decision-making process of the IT personnel	Early detection of an intrusion	DNS filtering	Perimeter 81	On-Prem solutions only	BP-IDS
		Firewall	SIEM system		
		Signature-based method	NIDS		
			HIDS		
		Anomaly-based method	PIDS		ARTEMIS
			APIDS		
			SolarWinds Security Event Manage		
			Bro		
			OSSEC		
			Security onion		
			Verve security		
	Ability to differentiate decision support for different kind of cyberattack	Data visualization and optimization	-	-	
	Tracking of actions	Logging	Sydecon	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	SIEM
	Offline Risk Assessment for enhancing strategic protection of grid		-	On-Prem solution only	SecurGrid RATING
	Near real-time Risk Assessment for tactical protection of grid		-	Cloud-based	SecurGrid

	Provide IT personnel with an updated Situational Awareness for rapid understanding of the status of the assets		-	Cloud-based	SecurGrid RATING Situational Awareness (ENG)
	Visualize attacker activities and movements inside the network	DNS filtering	SIEM system	On-Prem solutions only	BP-IDS
		Firewall			
		Signature-based method			
		Anomaly-based method			
To be promptly warned in case of an intrusion into the SCADA system	Ability to early detect an intrusion	DNS filtering	Perimeter 81	On-Prem solutions only	BP-IDS
		Firewall	SIEM system		
		Signature-based Method	NIDS		
		Anomaly-based Method	HIDS		
			PIDS		
			APIDS		
			SolarWinds Security Event Manage		
			Bro		
			OSSEC		
			Security onion		
			Verve security		
	Traceability of actions carried out by the attacker	Logging	SIAM RPM	-	SIEM
	Integration with advanced tamper resistant storage to avoid data modification	-	Diskshield	Data communication requirements	-
Impede the access to the disconnector to unauthorized people	Detection of unauthorized access	Remote control of potential cyberattacks	-	-	CyberRange
	Promptly alert whether an intrusion takes place	Alert system based on sensors	Oaktree products	Ability to detect people and alert operators	BP-IDS
			Digital alert systems		
			HSS engineering		

			Ascom alert management system	Offsite and offline solutions	
	Ability to restore a previous system state	Automated creation of backups	IBM Data protection	Offsite and offline solutions On-Prem solutions only	-
			Segment		
			RuleX		
			Acronis		
	Real-time communication of damage alert	Sensors Anomaly detection	Oaktree products Digital alert systems	Limited access to specific segmented networks Limited access to specific segmented networks	SIEM Situational Awareness (ENG)
			HSS engineering Ascom alert management system	Data confidentiality requirements	
Avoid Smart Meter sabotage	Ability to early detect anomalies	Constant Monitoring of consumption	Advance DMS		BP-IDS SecurGrid
	Promptly alert whether a sabotage takes place	Alert system	Oaktree products		BP-IDS SIEM Situational Awareness (ENG) SecurGrid
			Digital alert systems		
			HSS engineering		
			Ascom alert management system		
	Real-time communication of alerts	Anomaly Detection	Oaktree products		SIEM Situational Awareness (ENG)

2.3 Slovenian & Croatian Pilot

2.3.1 Functional Requirements and Non-Functional Requirements

Table 6: Functional and non-functional requirements for the Slovenian & Croatian pilot

Funct. Comp. ID	Functional Component	Related High-Level Requirement	ID of Derived Req.	Type of Derived Req. (Functional, Non-Functional)	Derived Requirement
FC-S.1	Vulnerability detection system for IEDs	Implementation of vulnerability detection system for weather stations	Req-S.1.1	Functional	Vulnerabilities reporting for IED components (hardware, operating system, libraries, etc.)
			Req-S.1.2	Functional	Poisoned data detection
			Req-S.1.3	Functional	Visualize reporting
FC-S.2	Intrusion detection system	Early notification to IT personnel in case of an intrusion in the SCADA system and SUMO dynamic rating system	Req-S.2.1	Non-Functional	Definition of business/process level KPIs related to intrusions
			Req-S.2.2	Functional	Intrusion notification
			Req-S.2.3	Functional	Poisoned data detection
			Req-S.2.4	Functional	Visualize KPIs and logs
FC-S.3	IT-OT network anomaly and intrusion detection	Implementation of a system to detect anomalous events and traffic in the SCADA/SUMO managed network of power lines, implementation of security event management and alerting	Req-S.3.1	Functional	Information collection from sensors
			Req-S.3.2	Functional	Insights and predictions, through AI algorithms applied to collected data
			Req-S.3.3	Functional	Identification and addressing cascading effects
			Req-S.3.4	Functional	Threats identifications
			Req-S.3.5	Functional	Visualize results and logs
FC-S.4	IT network anomaly and intrusion detection	Implementation of a system to track anomalous events on VPN connections and in the IT environment, and to track	Req-S.4.1	Functional	Information collection from IT devices, servers, workstations, firewalls and VPN connections
			Req-S.4.2	Functional	User behaviour information collection
			Req-S.4.3	Functional	User behaviour analytics

		user behaviour anomalies – uncommon use of user credentials	Req-S.4.4	Functional	Insights and predictions, through AI algorithms applied to collected data
			Req-S.4.5	Functional	Threats identifications
			Req-S.4.6	Functional	Visualize results and logs
FC-S.5	Incident response, CTI, risk assessment and decision support	Support to IT personnel and network operators in case of a cyberattack	Req-S.5.1	Non-Functional	Security patterns and libraries to implement IEC 62443-4-2 requirements in software applications
			Req-S.5.2	Functional	Assessment of risks based on a common approach
			Req-S.5.3	Functional	Decision analysis and visualisations to mitigate incidents and threats
FC-S.6	Social engineering prevention	Implementation of security measures to prevent vulnerabilities exploitation and stealing of credentials – prevention to gain unauthorized access to IT segment, VPN and OT environment	Req-S.6.1	Functional	Social Engineering (SE) ongoing attack detection
			Req-S.6.2	Functional	Alarm and visualize ongoing SE attack
FC-S.7	Simulation training	Support for cyberattack pattern recognition	Req-S.7.1	Functional	Attack-defence-simulation to study potential attack and countermeasures evolution
FC-S.8	Indicators of compromise (IoC), and Cyber Threat Intelligence (CTI) exchange	Support for the exchange of IoC and CTI between different organisations (TSOs, CERTs …)	Req-S.8.1	Functional	Cyber threat analysis
			Req-S.8.2	Functional	CTI exchange and incident response management
			Req-S.8.3	Non-Functional	CTI standards, data formats, ontologies, and exchange mechanisms (protocols, APIs …)
			Req-S.8.4	Non-Functional	Common CTI repositories and libraries
			Req-S.8.5	Non-Functional	CTI exchange platform and protocols

2.3.2 Technical Specification

Table 7: Technical specification for the Slovenian & Croatian pilot

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-	Constraints and Parameters	Related CyberSEAS Tools

			Shelf Solutions and/or Security Functions		
Implementation of vulnerability detection system for weather stations	Vulnerabilities reporting for IED components (hardware, operating system, libraries, etc.)	Events data capturing in IEDs Events time stamping in IEDs IED faults and vulnerabilities diagnosis Data visualization and data reporting	-	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	Heimdall ARTEMIS
	Poisoned data detection	Weather data capturing Data analytics Machine learning anomaly detection Statistical anomaly detection	IBM Watson Studio RStudio V7 Gurobi Optimizer	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	ARTEMIS
	Visualize reporting	Data visualization and data analytics	EventLog Analyzer Google Analytics SmartLook	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	Heimdall ARTEMIS
Early notification to IT personnel in case of an intrusion in the SCADA system and SUMO dynamic rating system	Definition of business/process level KPIs related to intrusions	KPI software Risk assessment software Decision support system	Sisense Fathom Scoreboard Visual KPI Dimensional Insight Callio	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS RATING

			RiskWatch CASIS		
	Intrusion notification	Alert system based on sensors Polling technique	Oaktree products Digital alert systems Ascom alert system SignalIR Desk Alert	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS
	Poisoned data detection	Data capturing Data analytics Machine learning anomaly detection Statistical anomaly detection	IBM Watson Studio RStudio V7 Gurobi Optimizer	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS
	Visualize KPIs and logs	Data visualization and data analytics Dashboard software	Google Data Studio Google Analytics Databox Cluvio	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS
Implementation of a system to detect anomalous events and traffic in the SCADA/SUMO managed network of power lines, implementation of security event managemen	information collection from sensors	Data capturing SIEM	QRadar Spluk LogRythm SIEMonster	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
	Insights and predictions, through AI algorithms applied to collected data	Data analytics Machine learning anomaly detection	IBM Watson Studio RStudio V7	On-Prem solutions only Limited access to specific segmented networks	CI SOC ARTEMIS

t and alerting		Statistical anomaly detection	Gurobi Optimizer	Data confidentiality requirements	
	Identification and addressing cascading effects	Risk assessment software	Callio RiskWatch RATING CASIS	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
	Threats identifications	Risk assessment software CTI software	Callio RiskWatch CASIS Cisco Umbrella DeCYFIR Recorded Future Dataminr	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS RATING
	Visualize results and logs	Data visualization and data analytics Dashboard software	EventLog Analyzer Google Data Studio Google Analytics SmartLook Databox Cluvio	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
Implementation of a system to track anomalous events on VPN connections and in the IT environment, and to track user behaviour	Information collection from IT devices, servers, workstations, firewalls and VPN connections	Data capturing SIEM Authentication	QRadar Spluk LogRythm SIEMonster	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
	User behaviour information collection	Data capturing UBA platform	Spluk Rapid7 LogRythm	Limited access to specific segmented networks	CI SOC ARTEMIS

anomalies – uncommon use of user credentials		Network monitoring Endpoint detection and response	MS Azure ATA Cynet 360 Fortinet	Data confidentiality requirements	
	User behaviour analytics	Data analytics Network analytics UBA platform Vulnerability scanning Forensics	Spluk Rapid7 LogRythm MS Azure ATA Cynet 360 Fortinet	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
	Insights and predictions, through AI algorithms applied to collected data	Data analytics Machine learning prediction	IBM Watson Studio RStudio V7 Gurobi Optimizer	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS
	Threats identifications	Risk assessment software CTI software	Callio RiskWatch CASIS Cisco Umbrella DeCYFIR Recorded Future Dataminr	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS RATING
	Visualize results and logs	Data visualization and data analytics Dashboard software	EventLog Analyzer Google Data Studio Google Analytics SmartLook Databox Cluvio	Limited access to specific segmented networks Data confidentiality requirements	CI SOC ARTEMIS

Support to IT personnel and network operators in case of a cyberattack	Security patterns and libraries to implement IEC 62443-4-2 requirements in software applications	Security programming libraries Security programming platform Platform Security Architecture (PSA) IEC 62443-4-2	Java Eclipse JavaScript Python PHP Microsoft .NET C++/C#	Limited access to specific segmented networks Data confidentiality requirements	DAISY KARMA RATING IEC 62443-4-2
	Assessment of risks based on a common approach	Risk assessment software	Callio RiskWatch CASIS	Limited access to specific segmented networks Data confidentiality requirements	DAISY KARMA RATING SAPPAN IEC 62443-4-2
	Decision analysis and visualisations to mitigate incidents and threats	Decision support system Data analytics and visualization	EIDOS MATLAB M-MACBETH Google Analytics SmartLook	Limited access to specific segmented networks Data confidentiality requirements	DAISY KARMA RATING SAPPAN IEC 62443-4-2
Implementation of security measures to prevent vulnerabilities exploitation and stealing of credentials – prevention to gain unauthorized access to IT segment, VPN and OT environment	SE ongoing attack detection	Multifactor authentication VPN protection OT security – asset discovery OT security – network segmentation OT security – threat prevention Social engineering detection Social engineering penetration testing	Private Internet Access CyberGhost ExpressVPN Duo Tenable.OT Cisco CheckPoint Confense PhishMe Social Engineer Toolkit Kaspersky	Limited access to specific segmented networks Data confidentiality requirements	TO4SEE

		Credential stealing detection Antivirus and antimalware software	Cordex XDR ScanGuard Norton McAfee Kaspersky Bitdefender		
	Alarm and visualize ongoing SE attack	Data analytics and visualization SE attack alarming Antivirus and antimalware software SOAR	Google Analytics SmartLook ScanGuard Norton McAfee Kaspersky Bitdefender Apache Airflow Node-Red Splunk SOAR IBM QRadar DarkTrace	Limited access to specific segmented networks Data confidentiality requirements	TO4SEE
Support for cyberattack pattern recognition	Attack-defence-simulation to study potential attack and countermeasures evolution	Attack-defence modelling and simulation AI based attack pattern recognition	Winf River Simics Simul8 MATLAB Simulink Simio AVEVA	Limited access to specific segmented networks Data confidentiality requirements	Attack-Defence Simulator
Support for the exchange of IoC and CTI between different organisations	Cyber threat analysis	Risk assessment software CTI software	Callio RiskWatch CASIS Cisco Umbrella	Limited access to specific segmented networks Data confidentiality requirements	MISP

(TSOs, CERTs …)			DeCYFIR Recorded Future Dataminr		
	CTI exchange and incident response management	Risk assessment software CTI software Incident response tools	Callio RiskWatch CASIS Cisco Umbrella DeCYFIR Recorded Future Dataminr SolarWinds CrowdStrike Falcon Splunk Phantom Manage Engine Log360 LogRhythm SIEM	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	MISP
	CTI standards, data formats, ontologies, and exchange mechanisms (protocols, APIs …)	CTI standard CTI data/object format CTI ontology CTI exchange protocol CTI APIs	STIX TAXII NIST SP 800-150 MITRE ATT&CK CTI IODEF/IDMEF OpenIOC OpenTPX	Limited access to specific segmented networks Data confidentiality requirements	MISP
	Common CTI repositories and libraries	Shared and common CTI data	STIX NIST SP 800-150	Limited access to specific segmented networks	MISP

		Shared and common CTI rules IoCs	MITRE ATT&CK CTI	Data confidentiality requirements	
	CTI exchange platform and protocols	CTI exchange protocols CTI exchange procedures CTI exchange platform CTI exchange actors and community (CERTs, SecOPS, security staff, decision-makers, EPES stakeholders)	Cisco Umbrella DeCYFIR Recorded Future CrowdStrike Falcon Dataminr FortiGate	Limited access to specific segmented networks Data confidentiality requirements	MISP

2.4 Romanian Pilot

2.4.1 Functional Requirements and Non-Functional Requirements

Table 8: Functional and non-functional requirements for the Romanian pilot

Funct. Comp. ID	Functional Component	Related High-Level Requirement	ID of Derived Req.	Typeof Derived Req. (Functional, Non-Functional)	Derived Requirement
FC-R.1	IT intrusion detection system	Implementation of a system to detect anomalous traffic on the network	Req-R.1.1	Non-Functional	Log management
			Req-R.1.2	Functional	Traffic analysis
			Req-R.1.3	Functional	Automatic generation of alerts and reporting
			Req-R.1.4	Non-Functional	Traceability of actions and data modification
			Req-R.1.5	Functional	Notifications from sensors

			Req-R.1.6	Non-Functional	Backup and restore functions
			Req-R.1.7	Non-Functional	Store all sensor input data into the database
FC-R.2	Decision support system	Support to IT personnel in case of a cyberattack	Req-R.2.1	Functional	Intrusion detection system
			Req-R.2.2	Functional	Tracking of actions
			Req-R.2.3	Functional	Decision support system
			Req-R.2.4	Non-Functional	Cyber awareness training with ambassador programs to increase the cybersecurity culture level (phishing tool)
			Req-R.2.5	Non-Functional	Integration with Database Management System (DBMS) that stores data input
			Req-R.2.6	Non-Functional	Integration with model management system to store and access models that are used to make decisions
FC-R.3	Real time cyber security monitoring	Real time cyber security monitoring of events from multiple diverse sources	Req-R.3.1	Non-Functional	Real-Time Log & Data Collection
			Req-R.3.2	Functional	Data collection
			Req-R.3.3	Non-Functional	Data management and correlation
			Req-R.3.4	Functional	Automatic generation of alerts and reporting
			Req-R.3.5	Non-Functional	Assure secure transmission of collected information
FC-R.4	Notification system	Early notification to IT personnel in case of an intrusion in the SCADA system	Req-R.4.1	Functional	Automatic user notification
			Req-R.4.2	Functional	Ability to early detect an intrusion
			Req-R.4.3	Non-Functional	Traceability of actions carried out by the attacker
			Req-R.4.4	Non-Functional	Run in the background without an active user interface

2.4.2 Technical Specification

Table 9: Technical specification for the Romanian pilot

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-Shelf Solutions and/or Security Functions	Constraints and Parameters	Related CyberSEAS Tools
Implementation of a system to detect anomalous traffic on the network	Log management	Collecting logs in a central location using agents	Various SIEM tools Splunk	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	SIEM
		Central log management			
		Backup and restore function for logs			
		Collect and store all sensor input data into the database			
	Traffic analysis	Processing traffic and alerts	Various IDS tools	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS SIEM
		Analysing traffic and alerts			
		Reporting on unexpected traffic and abnormalities			
	Automatic generation of alerts and reporting	Warning on high level alerts	Dashboard tools SIEM tools with alerting	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	SIEM
		Displaying high level alerts in a compact way			
		Storing high level alerts			
		Define event rules that will generate alerts			
		Define user-specified notifications			
		Define alerts for various active database rules			
		Ability to define and schedule ad-hoc reports defined by the user			
	Traceability of actions and data modification	Traceability of actions carried out by the attacker	-	-	BP-IDS SIEM
		Traceability of data modification			
	Notifications from sensors	Automatic deployment of various IDS configurations to IDS			

		Receive automatic notifications from IDS sensors (IT and OT)			
Support to IT personnel in case of a cyberattack	Intrusion detection system	Early detection of an intrusion			BP-IDS SIEM
		Ability to differentiate good traffic from anomaly traffic			
	Tracking of actions	Visualize attacker activities and movements inside the network			
	Decision support system	Allow the decision-maker to interact in a natural manner due to the careful design of the user interface			BP-IDS SIEM (SAPPAN)
		Support decisions that are formulated as semi structured, complex problem			
		Decision support for different kind of cyberattack			
	Cyber awareness training with ambassador programs to increase the cybersecurity culture level (Phishing tool)	Craft email messages using known vendor templates	Some open-source platforms. The best well-known providers are cloud based like: knowbe4, proofpoint	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	Antiphishing tool or training
		Ability to add attachments to email			
		Campaign creating with reporting and user tracking and statistics creation			
		Ability to track if the user has clicked on the phishing link and if the user has provided log-in credentials			
		Ability to test for 2FA credential grabbing			
		Automatic shown of results to the user including teaching moment page			
Real time cyber security monitoring of events from multiple diverse sources	Data collection	Real-time log collection from various sources including OT	-	-	ALIDA (?) BP-IDS TO4SEE SIEM
	Data management and correlation	Log correlation			
		Threat intelligence based on known threats and alerts coming from logs			
	Automatic generation of alerts	Real-time notification & alerting			
		Prioritization, analytics & AI for alerts			

	and reporting	Definition of security workflows and alerting			
		Warning on high level alerts			
		Displaying high level alerts in a compact way			
		Storing high level alerts			
		Define event rules that will generate alerts			
		Define user-specified notifications			
		Define alerts for various active database rules			
		Ability to define and schedule ad-hoc reports defined by the user			
Early notification to IT personnel in case of an intrusion in the SCADA system	Automatic user notification	Transmits alarm information anywhere via text-to-voice phone calls, SMS text messages, emails			BP-IDS
		User can login into account to check and acknowledge alarms or send commands to equipment			
	Ability to early detect an intrusion	DNS filtering	Perimeter 81	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS
		Firewall	SIEM system		
		Signature-based method	NIDS		
		Anomaly-based method	HIDS		
			PIDS		
			APIDS		
			SolarWinds Security Event Manage		
			Bro		
			OSSEC		
			Security onion		
			Verve security		
	Traceability of actions carried out by the attacker	Logging	SIAM RPM	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	SIEM

2.5 Finnish Pilot

2.5.1 Functional Requirements and Non-Functional Requirements

Table 10: Functional and non-functional requirements for the Finnish pilot

Funct. Comp. ID	Functional Component	Related High-Level Requirement	ID of Derived Req.	Type of Derived Req. (Functional, Non-Functional)	Derived Requirement
FC-F.1	End point detection and response	Use antivirus/anti malware Network intrusion prevention Restrict web-based content Software configuration Monitor network traffic content Monitor network traffic flow	Req-F.1.1	Functional	Automatic quarantine of suspicious files
			Req-F.1.2	Functional	Intrusion prevention systems
			Req-F.1.3	Functional	Scanning and removal of malicious email attachments
			Req-F.1.4	Functional	Blocking unknown or unused attachments that should not be transmitted over email
			Req-F.1.5	Functional	Scanning and analysing compressed and encrypted formats
			Req-F.1.6	Functional	Authenticating mechanisms to filter messages based on validity checks of the sender domain and integrity of messages
			Req-F.1.7	Functional	Malware analysis engine
			Req-F.1.8	Functional	Monitoring and analysing traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows
			Req-F.1.9	Functional	Monitoring network data for uncommon data flows
FC-F.2	Software version control	Update software	Req-F.2.1	Functional	Upgrading management services to the latest supported and compatible version
			Req-F.2.2	Functional	Continuous vulnerability scanning
			Req-F.2.3	Functional	Monitoring updated list of software and their status

			Req-F.2.4	Functional	Following active vulnerabilities related to the list of software
FC-F.3	User account management	User account control User account management Privileged account management Monitor application log content	Req-F.3.1	Functional	Managing accounts and permissions used by parties in trusted relationships
			Req-F.3.2	Functional	Restricting users and accounts to the least privileges they require
			Req-F.3.3	Functional	Limiting administrator accounts from activities that may expose them to potential adversaries
			Req-F.3.4	Functional	Limiting permissions so that users and user groups cannot create tokens
			Req-F.3.5	Functional	Monitoring authentication logs for succeeded and failed attempts to system and application login
			Req-F.3.6	Non-Functional	Formal process for providing permissions and accesses
			Req-F.3.7	Non-Functional	Annual check of validation of permissions and accesses
FC-F.4	User training	User training	Req-F.4.1	Functional	Continuous training for users to identify social engineering activities and spearphishing emails
			Req-F.4.2	Non-functional	Process for reporting suspicious activities
FC-F.5	Access control	Audit Limit access to resource over network Limit hardware installation Use network segmentation Minimize available info Properly set user account policies Use multi factor authentication	Req-F.5.1	Functional	Limiting access to data and resources based upon necessity and principle of least privilege
			Req-F.5.2	Non-Functional	Implementing network access control policies
			Req-F.5.3	Functional	Blocking unknown devices and accessories
			Req-F.5.4	Functional	Isolating infrastructure components that do not require broad network access
			Req-F.5.5	Non-Functional	Minimizing the amount and sensitivity of data available to external parties
			Req-F.5.6	Functional	Setting account lockout policies after a certain number of failed login attempts
			Req-F.5.7	Functional	Enabling multi-factor authentication
			Req-F.5.8	Non-Functional	Guidelines for creating password policies

		Password policies			
FC-F.6	Monitoring Policy	Monitor driver load Monitor windows registry key modification Monitor command execution Monitor OS API execution Monitor process creation Monitor network traffic content Monitor network traffic flow Monitor application log content	Req-F.6.1	Functional	Monitor for unusual kernel driver installation activity
			Req-F.6.2	Functional	Monitor for changes made to windows registry keys or values
			Req-F.6.3	Functional	Monitor executed commands and arguments that may enumerate files and directories
			Req-F.6.4	Functional	Monitor for API calls that may enumerate files and directories
			Req-F.6.5	Functional	Monitor newly executed processes that may enumerate files and directories
			Req-F.6.6	Functional	Monitoring and analysing traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows
			Req-F.6.7	Functional	Monitoring network data for uncommon data flows
			Req-F.6.8	Non-Functional	Centralized log management
			Req-F.6.9	Functional	SIEM (security information and event management)
			Req-F.6.10	Functional	Active monitoring the last SOC (security operation centre) function
			Req-F.6.11	Non-functional	Monthly reporting about the current status
			Req-F.6.12	Non-functional	Logging policy to define the logs that need to be collected
			Req-F.6.13	Non-functional	Define process about how to react in case of information security incidents
FC-F.7	Data backup and encryption	Manage process metadata	Req-F.7.1	Functional	Data backup and encryption
			Req-F.7.2	Functional	Backup and restore testing
			Req-F.7.3	Non-functional	Information classification guidance
			Req-F.7.4	Non-functional	Encryption policy
			Req-F.7.5	Non-functional	Backup policy that defines all the requirements of backup (how often to take backup and how long it takes to restore)

2.5.2 Technical Specification

Table 11: Technical specification for the Finnish pilot

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-Shelf Solutions and/or Security Functions	Constraints and Parameters	Related CyberSEAS Tools
Use antivirus/anti malware Network intrusion prevention Restrict web-based content software configuration Monitor network traffic content Monitor network traffic flow	Automatic quarantine of suspicious files	Anomaly detection Active monitoring Signatory based detection Rapid response File isolation capability Threat analysis	EDR (endpoint detection and response) XDR (extended detection and response) MDR (managed detection and response)	_	Antivirus Antimalware software Antiphishing, training/knowledge awareness TO4SEE (ENG) IDS Firewall BP-IDS (CINI) Network antivirus
	Scanning and removal of malicious email attachments			_	
	Authenticating mechanisms to filter messages based on validity checks of the sender domain and integrity of messages	Firewall PKI (public key infrastructure) Encryption Trusted domain list screening Email filtering	Intrusion detection and prevention (IDP)	_	
Update software	Upgrading management services to the latest supported and compatible version	Configuration manager Software batch repository	_	_	Patch management tools MIDA (GT)
	Continuous vulnerability scanning	Real-time continuous assessment SOC Configuration control	_	_	
	Monitoring updated list of software and their status	CMDB (configuration management database)	Multiple products like ServiceNow	_	

	Following active vulnerabilities related to the list of software	Threat intelligence News feed	_	_	
User account control User account management Privileged account management Monitor application log content	Managing accounts and permissions used by parties in trusted relationships	IAM (Identify and access management) PAM (privilege access management) Logging	Multiple products like Microsoft Active Directory and Beyond Trust	_	IAM solutions SIEM (CINI) Federated learning framework (SYN)
	Restricting users and accounts to the least privileges they require			_	
	Limiting administrator accounts from activities that may expose them to potential adversaries			_	
	Monitoring authentication logs for succeeded and failed attempts to system and application login	Logging SOC	Splunk and Qradar	_	
User training	Continuous training for users to identify social engineering activities and spearphishing emails	E-learning platform Social engineering testing	_	_	OPENESS.edu (ENG) TO4SEE (ENG) Antiphishing Training/knowledge awareness
Audit Limit access to resource over network Limit hardware installation Use network segmentation Minimize available info	Limiting access to data and resources based upon necessity and principle of least privilege	IAM (identify and access management) PAM (privilege access management) Firewall Monitoring Alerting	IDP Secure data exchange protocols Firewall SIEM (security information and event management) SOC	_	SIEM (CINI) MIDA (GT) Testing lab (FRAUNHOFER) SQS Test Lab (SQS) Firewall VPN solutions DRM management tool IAM
	Implementing network access control policies			_	
	Minimizing the amount and sensitivity of data available to external parties			_	
	Setting account lockout policies after a certain number of failed login attempts			_	

Properly set user account policies Use multi factor authenticati on Password policies	Enabling multi-factor authentication	Multi-factor authentication	Multi-factor authentication	_	
Monitor driver load Monitor windows registry key modification Monitor command execution Monitor OS API execution Monitor process creation Monitor network traffic content Monitor network traffic flow Monitor application log content	Monitor for API calls that may enumerate files and directories	Firewall Web-application firewall IDS (intrusion detection system)	Multiple products by different vendors	_	MIDA (GT) SIEM (CINI) BP-IDS (CINI) Firewall Federated learning framework (SYN)
	Centralized log management	Centralized log management	Multiple products like Splunk and Qradar	_	
	SIEM (security information and event management)	SIEM	Splunk and Qradar	_	
	Active monitoring the last SOC (security operation centre) function	SOC	_	_	
	Define process about how to react in case of information security incidents	SOAR	Multiple SOAR products like Checkpoint SOAR and PaloAlto SOAR	_	
Manage process metadata	Data backup and encryption	Backup system Encryption	Multiple backup systems like VEEAM	_	FIM – file integrity monitoring tools

2.6 Estonian Pilot

2.6.1 Functional Requirements and Non-Functional Requirements

Table 12: Functional and non-functional requirements for the Estonian pilot

Funct. Comp. ID	Functional Component	Related High-Level Requirement	ID of Derived Req.	Type of Derived Req. (Functional, Non-Functional)	Derived Requirement
FC-E.1	Sabotage detection system	Implementation of a system to detect abnormalities in remote access traffic caused by sabotage (Sc. 1)	Req-E.1.1	Functional	Log management
			Req-E.1.2	Non-Functional	Backup and restore functions
		Functionality to define pre-set configurations which must be avoided (Sc. 1)	Req-E.1.3	Functional	Configuration management
FC-E.2	Physical intrusion detection	Implementation of a constant surveillance to substations for detecting physical intrusion to the premises (Sc. 2)	Req-E.2.1	Functional	Perimeter security
FC-E.3	Decision support system	Support the Control Centre Operator in managing and prioritizing alarms. (Sc. 2)	Req-E.3.1	Non-Functional	Well defined operational support material for control centre operator
FC-E.4	Version control system	Save, sign, and manage system configurations layer by layer (Sc. 3)	Req-E.4.1	Functional	Configuration management
FC-E.5	Administrative rights management, identity access	Management of identities and their access rights.	Req-E.5.1	Functional	User management and analyses

	management and user behaviour analyzation	Implementation of HR processes (Sc. 3)			
FC-E.6	Network segmentation	Access permissions by IP address, 2fA etc (Sc. 4)	Req-E.6.1	Functional	Access control security
FC-E.7	Isolated IoT implementation	Substation configurations and management in IoT by secured Starlink connection. (Sc. 4)	Req-E.7.1	Functional	Secured private network
FC-E.8	Data confidentiality and integrity	Data transfer must be prohibited, and data leaks must be monitored (Sc. 5)	Req-E.8.1	Functional	Data security in transit
			Req-E.8.2	Functional	Backup management
			Req-E.8.3	Functional	Recovery management
FC-E.9	Isolated networks	Unauthorized access must be avoided, internal data must be separated from external networks (Sc. 5)	Req-E.9.1	Functional	Network security
FC-E.10	Implementation of maintenance process	Maintenance of electric grid should be run by program, not incidents (Sc. 6)	Req-E.10.1	Functional	Electrical grid maintenance
			Req-E.10.2	Non-Functional	Periodical maintenance
			Req-E.10.3	Non-Functional	Synchronization with accountancy
FC-E.11	Enhanced data integrity	Commands must be automatically validated, including time and user (Sc. 7)	Req-E.11.1	Functional	Automatic data integrity protection and verification to verify integrity, time and signer
FC-E.12	Overhaul of system by functions	Modular architecture of functions, multiple security layers (Sc. 8)	Req-E.12.1	Non-Functional	Hardening tools and implementation
FC-E.13	Controlled procedures for legacy systems	Educate and remain awareness handling legacy equipment (Sc. 8)	Req-E.13.1	Functional	Vulnerability management activities
			Req-E.13.2	Functional	Vulnerability scanning activities
FC-E.14	Global sync of time of all substation in grid	For precise timing of instructions time resolution must be as good as latency (1 ms) (Sc. 9)	Req-E.14.1	Functional	System time synchronization for precise timing of instructions
			Req-E.14.2	Non-functional	Latency <1s

FC-E.15	Precautions for protecting local area networks	Extra security layers between local area networks and substations (Sc. 10)	Req-E.15.1	Functional	Advanced network security features
FC-E.16	Detection of suspicious hardware	Automated detection solutions to find unidentified devices (Sc. 11)	Req-E.16.1	Functional	Network management and monitoring
FC-E.17	Multiple ways to compare configuration s to reality	Layers of indicators to detect difference between configuration and actual status of substation/RTU (Sc. 12)	Req-E.17.1	Functional	Configuration immutability monitoring
FC-E.18	Automated detection of social engineering	Automated detection of social engineering in substation configuration (Sc. 13)	Req-E.18.1	Non-functional	Processes and playbooks to keep order
FC-E.19	Secure updating process	Automated solution for patch management and version management (Sc. 13)	Req-E.19.1	Functional	Patch management and verification
FC-E.20	Enhanced security for 3rd party	Extra layers for monitoring activities of 3rd party users (Sc. 14)	Req-E.20.1	Functional	User behaviour monitoring and analysis
FC-E.21	Modern physical security	Important substations must have better physical security (Sc. 15)	Req-E.21.1	Functional	Key and access card management
FC-E.22	Digital monitoring of all visits in substations	All activities in substations must be recorded (Sc. 15)	Req-E.22.1	Functional	User/visitor monitoring
FC-E.23	Enhanced security processes and training quality	Better processes, education, and discipline (Sc. 16)	Req-E.23.1	Functional	Cyber awareness training with ambassador programs to increase the cybersecurity culture level
FC-E.24	Automated detection of	Suspicious configurations of	Req-E.24.1	Functional	Deployed configuration checks

	suspicious configurations	substations and RTU`s must be detected (Sc. 16)	Req-E.24.2	Non-Functional	Periodically repeating checks of deployed configurations

2.6.2 Technical Specification

Table 13: Technical specification for the Estonian pilot

High-Level Requirement	Functional Requirement	Derived Technical Specification	Available Commercial-off-the-Shelf Solutions and/or Security Functions	Constraints and Parameters	Related CyberSEAS Tools
Implementation of a system to detect abnormalities in remote access traffic caused by sabotage	Log management	Log collection & analysis	Syslog (rsyslog), Splunk, Graylog, or SIEM	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	CINI's SIEM
Functionality to define pre-set configurations which must be avoided	Configuration management	Configuration immutability verifications	SolarWinds Server Configuration Monitor, Guardtime 's MIDA	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	Guardtime's MIDA
Implementation of a constant surveillance to substations for detecting physical intrusion to the premises	Perimeter security	Cameras for video recording	HIKvision EasyIP 3.0, Bosch BVMS, Cisco Meraki	Data communication requirements	_
		Motion sensor	Ajax, Paradox, ICT	Ability to detect people and alert operators	_

			Protégé, iConnect		
		Door alarms	Ajax, Paradox, ICT Protégé, iConnect	Ability to report alerts to operators	_
Support the control centre operator in managing and prioritizing alarms	Well defined operational support material for control centre operator.	Operations playbooks / SOP	Splunk, ManageEngine, SolarWinds, Check Point Incident Response	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements.	SIEM (CINI) CI SOC ENG's EPES solution RATING DAISY (SAPPAN)
Save, sign, and manage system configurations layer by layer	Configuration management	Version control for configurations	Gitlab, Github, SVN	On-Prem solutions	_
		Configuration deployment	Chef, Puppet, Ansible	On-Prem solutions	_
Management of identities and their access rights Implementation of HR processes	User management and analyses	Identity and Access Management	Auth0, Okta, Ping Identity	On-Prem solutions	_
		User behaviour analysis	UBA	On-Prem solutions	PKI (CINI
Access permissions by IP address, 2fA, etc.	Access control security	MFA	Twilio offers a great set of 2FA one time pin options: SMS, Email, Software, Push, notifications, Google authenticator tokens.	Must verify the domain where MFA is used Phishing protections	_
		Firewalls	Sophos, Palo Alto networks, Cisco PIX, pfSense	On-Prem solutions only	_

		VPN	OpenVPN, Pulse, …	On-Prem solutions only.	_
Substation configurations and management in IoT by secured Starlink connection	Secured private network	Resilient and secure network for substations and IoT devices	Use case provider (infra) specific	Micro segmentation	_
Data transfer must be prohibited, and data leaks must be monitored	Data security in transit	Data encryption and signing in transit	Let's encrypt	Known secure algorithms only	_
Unauthorized access must be avoided, internal data must be separated from external networks	Network security	Firewall	Sophos, Palo Alto networks, Cisco PIX, pfSense	Micro segmentation	_
		VPN	OpenVPN, Pulse, …	On-Prem solutions	_
Maintenance of electric grid should be run by program, not incidents	Electrical grid maintenance	Maintenance plan	-	Not specified	_
Commands must be automatically validated, including time and user	Automatic data integrity protection and verification to verify integrity, time and signer	Command integrity verification	Guardtime's MIDA	On-Prem solutions only Limited access to specific segmented networks	Guardtime's MIDA
For precise timing of instructions time resolution must be as good as latency (1 ms)	System time synchronization for precise timing of instructions	Time synchronization with NTP	NetTime, Time-Sync, NTP syncing tools integrated in OS, GPS sync time	Limited access to specific segmented networks	_
Extra security layers between local area networks and substations,	Advanced network security features.	Network segmentation	VLANs, firewall rules to restrict communication between VLANs.	Limited access to specific segmented networks	_
		Firewalls	Sophos, Palo Alto networks,	Limited access to specific	_

			Cisco PIX, pfSense	segmented networks Micro Segmentation	
		Port Security	Switches and routers with switchport security feature	Limited access to specific segmented networks	_
		VPN	OpenVPN, Pulse, …	On-Prem solutions only Limited access to specific segmented networks	_
Automated detection solutions to find unidentified devices	Network management and monitoring	Connected device white listing	Switches and routers with Port MAC filter, disabled unused ports	Limited access to specific segmented networks	_
		Monitoring of connected devices	ManageEngine OPManager, SolarWinds network performance monitor, Datadog network device monitoring	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	BP-IDS(?)
		Log management	Splunk	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	CINI's SIEM

		Port security	Switches and routers with switchport security feature, USB Block, USBGuard utility	Logging and centrally alerting on port activities	_
Layers of indicators to detect difference between configuration and actual status of substation/RTU	Configuration immutability monitoring	Version control system	Gitlab, Github, SVN	On-Prem solutions	_
		Tamper resistant data integrity protection and verification	Guardtime's MIDA	On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements	Guardtime's MIDA
Automated solution for patch management and version management	Patch management and verification	Secure software and configuration supply chain	Atera, …	On-Prem solutions only Limited access to specific segmented networks	_
		Tamper resistant data integrity protection and verification	Guardtime's MIDA	On-Prem solutions only Limited access to specific segmented networks	Guardtime's MIDA
Extra layers for monitoring activities of 3rd party users	User behaviour monitoring and analysis	IPS solutions	-	On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.	BP-IDS
		UBA solutions	-	On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.	_

		EDR and XDR solutions	-	On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.	_
		Log management	Splunk	On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.	CINI's SIEM
		Security orchestration	-	On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.	KARMA
Important substations must have better physical security	Key and access card management	NFC keys	-	Latest version, updatable	_
		Central NFC management	-	On-Prem solutions only Limited access to specific segmented networks	ATRS, CINI's PKI
All activities in substations must be recorded.	User/visitor monitoring.	Visitor interaction (logging) registration using tamper resistant proofs	Rsyslog using Guardtime 's KSI blockchai n log signing module	On-Prem solutions only	_
		Surveillance	HIKvision EasyIP 3.0, Bosch BVMS, Cisco Meraki	People activity detection	_
		Door alarms	Ajax, Paradox, ICT Protégé, iConnect	Alerting operators centrally	_
Suspicious configurations of substations and	Deployed configuration periodic checks	Configuration management	Chef, Puppet, Ansible	On-Prem	_

RTU`s must be detected		Monitoring of configuration using tamper resistant proofs	Guardtime's MIDA	On-Prem	Guardtime's MIDA
		Backup management	SCADA backup	Offsite and offline solutions	_

3 Metrics

In the following, we propose a selection of metrics, which can be used to guide and evaluate future development activities on a requirements-level. For better reference, we further define some initial performance levels, where lower levels are associated with lower scores, meaning that "Level 1" indicates the worst performance interval for a metric. The following metrics are based on ones that have been proposed in relevant literature such as [17] and [18].

Requirement coverage: The percentage of functional requirements that have been fulfilled. This metric is intended to measure implementation progress in regard to system functionality. A high score on this metric is desirable. As a point of orientation, we propose the following intervals:

- Level 1: $x < 25\%$
- Level 2: $25\% \leq x < 50\%$
- Level 3: $50\% \leq x < 75\%$
- Level 4: $75\% \leq x < 85\%$
- Level 5: $85\% \leq x$

Requirement stability: The percentage of requirements to which changes have been applied. This metric is intended to measure how stable the view of a planned system is. Generally, a low score on this metric is desirable. The following intervals can serve as a point of orientation:

- Level 1: $80\% \leq x$
- Level 2: $60\% \leq x < 80\%$
- Level 3: $40\% \leq x < 60\%$
- Level 4: $20\% \leq x < 40\ \%$
- Level 5: $x < 20\%$

As new and more detailed requirements might be added later to specify the previously defined requirements based on a more accurate understanding of the planned system, we suggest to only consider actions for this metric, which actively change requirements. The metric further only does not account for the removal of requirements, as this is covered separately by the fault density metric.

Requirement fault density: The percentage of requirements which have been discarded. A poor performance on this metric implies a significant deviation from the initially planned system. Generally, a low score on this metric is desirable. For reference, the following intervals can be used:

- Level 1: $80\% \leq x$
- Level 2: $60\% \leq x < 80\%$
- Level 3: $40\% \leq x < 60\%$
- Level 4: $20\% \leq x < 40\ \%$

- Level 5: x < 20%

4 CyberSEAS SELP Requirements

4.1 Introduction to SELP Requirements and Responsible Innovation

A central requirement for any EU funded project is that it is organized and implemented in accordance with European socio-cultural values, Europe's fundamental rights framework, and European ethical standards. In order to ensure that this requirement is satisfied in CyberSEAS as well, CyberSEAS will design and implement a SELP Governance Framework.
As specified in the Grant Agreement of CyberSEAS, SELP refers to **Societal, Ethical, Legal and Privacy** requirements. The goal is not merely to list relevant requirements on the basis of existing laws and policies, but also to identify how these requirements can be formalized and monitored in practice. In that way, compliance can be continuously evaluated, and CyberSEAS can ensure that there is transparency at all times on which checks have been applied precisely, and where any potential risks may lie.
With that in mind, this section of the deliverable defines:

- Specific SELP values, derived through the application of the principle of Responsible Innovation;
- Specific SELP requirements, derived principally from applicable legislation (including but not limited to the General Data Protection Regulation (GDPR) [1], as the EU's principal legal framework safeguarding informational privacy rights) and the project's overarching SELP value framework.
- A general methodology for applying and monitoring compliance with the SELP values.

4.2 SELP Value Framework in CyberSEAS

The starting point of the CyberSEAS SELP Framework is the **protection of freedoms and fundamental rights of the participants, and compliance with the principle of responsible innovation**, as required for all EU funded research projects.

With respect to ethics, this report applies the EU's framework for Responsible Research and Innovation (RRI)[2]. As described by the Commission, RRI implies that societal actors (researchers, citizens, policy makers, business, third sector organisations, etc.) work together during the whole research and innovation process in order to better align both the process and its outcomes with the values, needs and expectations of society.

The objective of the SELP Framework in CyberSEAS is to ensure that the innovation brought about by the project is in line with European legal, ethics and moral values. With respect to ethics and societal values, this is done by applying the theory of Value Sensitive Design, an approach which aims to integrate a wide range of human and moral values into the design of (information) technology.

In other words, Value Sensitive Design implies that **a normative framework is defined**, and that the designers of a system – in this case the CyberSEAS consortium – integrate this framework into their work, thus recognising that systems are rarely ethically neutral, and that

human well-being, human dignity, justice, welfare, and human rights can be served by integrating them into technological design.

As a first step, it is important to determine the relevant sources of SELP norms. Within the EU, the European Charter of Fundamental Rights [3] provides the legal underpinning of SELP protections for European citizens. The Charter applies a structure of six value domains:

Dignity, notably individuals' right to be secure in their physical and mental integrity.

Freedoms, comprising the rights to data protection and privacy, but also intellectual freedoms (education, expression, thought, religion and information) and social freedoms (assembly, marriage, asylum and property);

Equality, including non-discrimination and rights of minorities and of societally more vulnerable parties;

Solidarity, covering workers' rights and labour rights, social security, collective bargaining, health care and environmental protection;

Citizens' rights, such as the right to vote, to proper administration, access to documents and freedom of movement;

Justice, including access to a fair trial and effective remedy, and the right to defence.

These are of course fundamental but relatively abstract rights. For that reason, to derive more specific SELP requirements, account must be taken of more detailed normative frameworks with respect to fundamental rights protections. These include notably:

- The **General Data Protection Regulation** (GDPR), as the EU's central framework in relation to informational privacy protection.
- Opinions of the European Group on Ethics in Science and New Technologies, including but not limited to EGE **Opinion n°28** - 20/05/2014 - Ethics of Security and Surveillance Technologies [4] and the EGE **Opinion n°26** - 22/02/2012 - Ethics of information and communication technologies [5].
- The European Code of Conduct for Research Integrity [6], including but not limited to **section 1, Articles 2.1, 2.3, 2.4, 2.5**.
- EU Commission's 'Ethics and Data Protection' in research settings (2018) [7], including but not limited to **sections II, VI, X and XIII**
- EU Commission's 'Ethics in Social Science and Humanities' (2018) [8], including but not limited to **sections 3, 4, 6 - 10**

Moreover, the SELP requirements do not relate only to societal, ethical and privacy norms, but also to legal requirements in general. Beyond privacy, data protection and ethics, this means that account must also be taken of:

- The legal framework relating to the **electricity grid and market,** notably the EU's Third energy package and the Clean Energy Package, comprising the **Directive on common rules for the internal market for electricity** (EU) 2019/944 [9](replacing the Electricity Directive (2009/72/EC)), and the new **Regulation on the internal market for electricity** (EU) 2019/943 [10] (replacing the Electricity Regulation (EC/714/2009) on

January 1, 2020). These structurally emphasise the shift to end user control and end user protection, including better protection and control over their electricity data.

- The legal framework relating to **information security and critical infrastructure protection.** This includes the **2016 NIS Directive** [11], which contains the principal current legal framework relating to cybersecurity for network and information systems; and the **2008 Critical Infrastructures Directive** [12], which is the central legal framework for the protection of critical infrastructures in the Member States (including the energy grid). The Directive fundamentally applies an all-hazards approach - a concept built on the conviction that hazards may vary in source, but affect critical infrastructures across industries in similar ways, so that a generalised approach is viable. These are likely to evolve in relatively short order: a Proposal for a **NIS 2 Directive** [13] was published that would strengthen supervision and risk management practices; and a recently proposed **Critical Entities Resilience (CER) Directive** [14] would expand both the scope and depth of the 2008 Directive, requiring critical entities to perform risk assessments, take resilience measures, conduct background checks of their personnel and notify incidents to competent authorities.
- Finally, there is also the emerging European **data legislation,** including the recently approved **Data Governance Act** [15], and the proposal for a **Data Act** [16]. At the highest level, these again stress the importance of user control over their data, and of the security of data storage infrastructures; but also encourage data sharing between duly mandated actors in order to enable further innovation. This includes a regime under the Data Act that incentives (and sometimes requires) data holders to make their data available to third parties when instructed to do so by their customers – an approach that is not entirely new to the electricity market, since the aforementioned Electricity Directive (EU) 2019/944 of 5 June 2019 already provides for a framework for electricity data sharing and data management (including the definition of information to be made available, high level confidentiality and security obligations, the identification of eligible parties for data sharing, and rules on fee setting.

Moreover, the CyberSEAS project is also keenly aware that not all procedures and requirements are defined at the EU level. National and regional legislation may have an impact as well, since procedures and safeguards (e.g. in terms of security, supervision, certification, or prior authorization) can be defined nationally or regionally, in a way that directly impacts the legal feasibility of some use cases to be piloted in CyberSEAS. These must be identifiable to the CyberSEAS project as well.

4.3 Cross-cutting SELP Requirements

In order to create a SELP Framework, it is important to specify non-functional but operational SELP requirements. In the present deliverable, this is done by firstly identifying the Societal, Ethics and Privacy requirements in general; and then outlining other Legal requirements. The distinction is useful in CyberSEAS, since Societal, Ethics and Privacy requirements are addressed in more detail in other deliverables, notably D2.5 – Privacy Risk Mitigation Plan (v1); but other Legal requirements are not.

In the present deliverable, the emphasis is on identifying cross-cutting (non-country specific and non-use case specific) SELP requirements. A methodology is provided below to identify and assess any national and regional SELP requirements prior to initiating any piloting activities.

4.3.1 Non-functional Societal, Ethics and Privacy Requirements

The Societal, Ethics and Privacy (SEP) requirements are addressed in detail across three deliverables:

- **D10.1 H - Requirement No. 1**. This deliverable contained notably an introduction to the human involvement in CyberSEAS, an incidental findings policy, and a template Informed Consent and Information Sheet
- **D10.2 POPD - Requirement No.2.** This deliverable contained notably the confirmation of the appointment of a qualified data protection officer (DPO) in CyberSEAS, as well as a description of anonymisation and pseudonymisation techniques, and a policy relating to the further processing of previously collected personal data.
- **D2.5 Privacy Risk Mitigation Plan (v1).** This deliverable contained notably an initial data protection impact assessment in order to assess compliance with the General Data Protection Regulation. Moreover, it defines a monitoring methodology for the use cases, requiring each use case to self-assess its compliance with the project's requirements, and to obtain a prior approval from the Internal Ethics Committee (IEC) prior to starting the use case.

The prior assessment and approval framework contains a broad range of SEP requirements, including:

- An assessment of whether data protection law applies
- If so: completion of a data protection impact assessment (DPIA)
- Supervision of use cases by a data protection officer (DPO)
- Prior approval by the CyberSEAS Internal Ethics Committee (IEC)

For the avoidance of doubt: the DPIA also checks compliance with more granular non-functional SEP requirements than the four requirements mentioned above, including but not limited to verification of the legal basis, transparency notices towards affected users, risk and impact assessment of privacy incidents, documenting security measures, risk stratification and incident notification, incidental findings policies, and data minimisation policies (including anonymisation and pseudonymisation requirements). These are however not reprised here to avoid needless repetition; reference can be made to D2.5, where these are outlined in detail.

A comprehensive template of the assessment framework was included in Annex I of Deliverable 2.5. It is reprised in the present deliverable to facilitate cross-checking.

4.3.2 Non-functional Legal Requirements Other than Societal, Ethics and Privacy

Beyond the SEP requirements, other legal requirements will need to be taken into account as well, driven notably by the aforementioned legal frameworks in relation to the energy/electricity markets, data policies (data sharing), and information security.

Based on an initial analysis of these frameworks, the following high level non-functional legal requirements can be identified:

- A legal assessment must be done on a per-use case basis of whether there are national / regional prior approval requirements before initiating any use cases
- A legal assessment must be done on a per-use case basis of whether infrastructure in any use case is designated as critical infrastructure subject to specific security obligations; and if so, defining a tailored plan to satisfy these requirements
- A legal assessment must be done on a per-use case basis of whether data sharing is subject to prior authorisation by end users, and if so, drafting the required consent / agreement documents
- A legal assessment must be done on a per-use case basis of data sharing activities between partners (even within the CyberSEAS consortium), in order to determine whether there are legal constraints (beyond data protection law; e.g. based on security, confidentiality, intellectual property rights or trade secrets), and how these constraints can be satisfied.

These requirements will be evaluated and monitored in the same way as the SEP requirements specified above, using the same governance process, which will be briefly explained below.

4.4 SELP Implementation Approach in CyberSEAS

Especially in a project with the scale and complexity of CyberSEAS, it is critical that compliance with SELP requirements is continuously monitored and evaluated. This is needed to ensure that the SELP approach is known and understood by all relevant CyberSEAS partners, and that they adhere to the non-functional requirements in practice.

The non-functional requirements set out in this deliverable are by necessity still at a relatively high level. A continuous validation, support and verification process is required, that allows all use cases to be monitored continuously.

In order to achieve this goal, CyberSEAS will apply a mechanism that combines:

(1) Self-evaluation and self-assessment by the pilot participants themselves, in which they will conduct their own risk assessment and report on exact SELP measures taken on the basis of a common template;
(2) An independent verification and approvals process by the CyberSEAS Internal Ethics Committee (IEC).

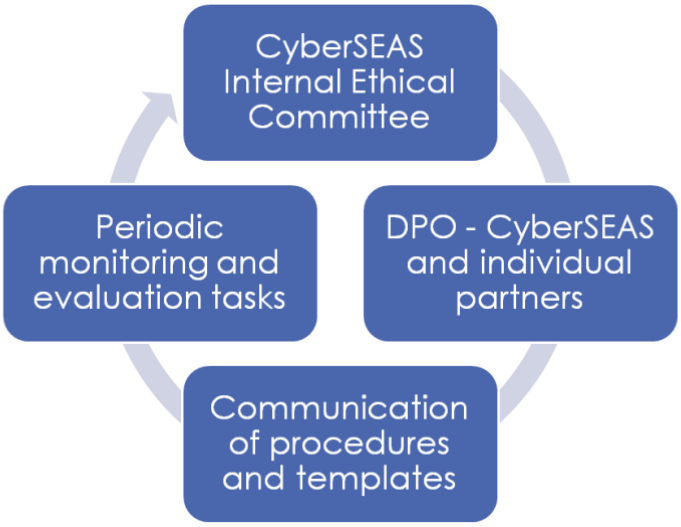

Figure 2: Monitoring and evaluation structure

To support this approach, CyberSEAS applies a standard four tiered governance model, which is depicted in Figure 2. More specifically, the four tiers consist of the following steps:

- **Establishment of a CyberSEAS Internal Ethical Committee** (IEC), which has the assignment of ensuring clarity and consistency in communicating with CyberSEAS project partners on ethics issues, assessing compliance with SELP policies, and supporting interactions with the users. It has the responsibility for monitoring, ethical, privacy and data protection/SELP issues.
- **Appointment of Data Protection Officers** (DPOs) in accordance with the GDPR. The CyberSEAS project has nominated a project DPO (see the next section of this deliverable) to oversee data protection compliance. Moreover, a list of DPOs at the partner level is maintained, to facilitate interaction with local end users, and to ensure that there is hands-on involvement at the partner level.
- **Communication of procedures and templates:** the ethics guidance from the WP10 deliverables are actively disseminated and explained towards all CyberSEAS partners, to ensure that they are known and used in practice. Deviations are of course possible and permissible (including localization, translation and customization of templates), provided that the legal and functional goals set out in this deliverable are achieved.
- **Periodic monitoring and evaluation tasks:** CyberSEAS will evaluate to what extent the SELP principles are respected during the project's execution. Beyond the ethics reporting in the periodic activity reports, CyberSEAS has defined specific tasks to conduct data protection impact assessments (T2.5) and to create and monitor SELP (Security, Ethical, Legal and Privacy) requirements (T3.2), which will be used to further detail, monitor and report on ethics compliance, and to take any corrective actions needed.

In this way, CyberSEAS can ensure compliance throughout the project's duration, by combining a deep and tailored understanding of the pilot circumstances, with neutral and consistent assessment by the IEC.
In practical terms, this means that the process as shown in Figure 3 is followed by each pilot.

Figure 3: Piloting assessment and approvals process

Thus, each pilot is first required to conduct a self-assessment based on a standardized SELP template, included in Annex I to this deliverable. The template will identify specific personal data which is collected, identify risks and potential impacts, and document how the measures prescribed in this deliverable and in the ethics deliverables have been satisfied.

Once completed by the pilot partners, the template is reviewed by the IEC and the CyberSEAS DPO (independently from the individual partners' DPOs, where available), for completeness, accuracy, coherence, and adequacy. Feedback may be provided by the IEC requiring amendment of the pilots.

Only after the formal and documented approval of the report by the IEC, may piloting begin. Thus, no piloting activities will initiate without prior tailored SELP screening by the Internal Ethics Committee, and without the prior documented approval by this Committee.

5 Conclusions

This deliverable focused on bridging the results of task T3.1 to inputs for task T3.3 by deriving (non-)functional requirements and the technical specification from the high-level requirements and pilot scenarios documented in D3.1. For this, a straightforward specification methodology has been used to first specify the functional view on each pilot, which was then further specified from a technical point of view. The result, including a mapping to COTS and CyberSEAS tools, has been documented in this deliverable. Additionally, suitable metrics for monitoring compliance of development activities with the identified requirements have been documented. Further, the SELP value framework, legal requirements beyond the SEP requirements, and the SELP implementation process for CyberSEAS have been documented in this deliverable.

6 References

[1] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). ELI: http://data.europa.eu/eli/reg/2016/679/2016-05-04

[2] European Commission, Directorate-General for Research and Innovation, Towards responsible research and innovation in the information and communication technologies and security technologies fields, Schomberg, R.(editor), Publications Office, 2011, https://data.europa.eu/doi/10.2777/58723

[3] Charter of Fundamental Rights of the European Union. ELI: http://data.europa.eu/eli/treaty/char_2012/oj

[4] European Commission, European Group on Ethics in Science and New Technologies, Ethics of security and surveillance technologies : Brussels, 20 May 2014, Dratwa, J.(editor), Publications Office, 2015, https://data.europa.eu/doi/10.2796/22379

[5] European Commission, European Group on Ethics in Science and New Technologies, Ethics of information and communication technologies, Publications Office, 2012, https://data.europa.eu/doi/10.2796/13541

[6] The European Code of Conduct for Research Integrity (Revised Edition). Available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf

[7] European Commission, Ethics and Data Protection, 2018. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

[8] European Commission, Ethics in Social Science and Humanities, 2018. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

[9] Consolidated text: Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) (Text with EEA relevance). ELI: http://data.europa.eu/eli/dir/2019/944/2022-06-23

[10] Consolidated text: Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) (Text with EEA relevance). ELI: http://data.europa.eu/eli/reg/2019/943/2022-06-23

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. ELI: http://data.europa.eu/eli/dir/2016/1148/oj

[12] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). ELI: http://data.europa.eu/eli/dir/2008/114/oj

[13] Draft directive on measures for a high common level of cybersecurity across the Union – provisional agreement text. Available at: https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf

[14] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A829%3AFIN

[15] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[16] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act). Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2022:68:FIN

[17] S. Sedigh-Ali, A. Ghafoor and R. A. Paul, "Software engineering metrics for COTS-based systems" in *Computer*, vol. 34, no. 5, pp. 44-50, May 2001, doi: 10.1109/2.920611.

[18] H.B. Yadav and D.K. Yadav, "Early software reliability analysis using reliability relevant software metrics" in *Int J Syst Assur Eng Manag*, vol. 8, no. 4, pp. 2097–2108, December 2017, doi: 10.1007/s13198-014-0325-3.

7 ANNEX I - Pilot Description, Privacy Risk Assessment and Approvals Process

7.1 Scope and Objectives of the Present Document

7.1.1 Scope and Objectives

The privacy risk mitigation plan annex contains the template and process to be used in the CyberSEAS project to:

- Capture and summarise the key characteristics of any pilot use case in the CyberSEAS project, including its risks and mitigating measures;
- Obtain formal approval from the CyberSEAS Internal Ethics Committee prior to initiating the pilot.

The objective of this Annex is to ensure that each project is conducted in a legally and ethically compliant manner, in particular from the perspective of data protection law in the European Union as enshrined in the General Data Protection Regulation 2016/679 ("**GDPR**").

7.1.2 Summary of the Procedure for Approval

Prior to initiating a pilot, the pilot participants should jointly complete subsections 2 to 8 of this Annex.

Once a draft Annex is internally approved by all the participants in the particular pilot, the draft Annex can be presented to the Internal Ethics Committee for approval.

Only when the draft Annex has been approved by the Internal Ethics Committee, the pilot can be initiated.

Any challenges, doubts or points of non-compliance, even those raised after the approval of the Annex, should be signalled to the Internal Ethics Committee as soon as reasonably feasible until the end of the CyberSEAS project, including any extensions to the project.

7.2 Description of the Use Case

7.2.1 Intended Goals and Outcomes of the Use Case

Describe briefly and concisely what the use case is intended to achieve. In particular, why is data being collected? What is the general goal of the use case?
[free text description]

7.2.2 Date and Location of the Use Case Data Collection

Planned running dates	[start date – end date]
Location / site 1	[address]
Location / site 2	[address]
Etc.	[address]

Note: this information relates only to the place where data is **collected,** not where it will be **analysed or used** (which may be a different site) for the purposes of the pilot.

7.2.3 Contact Point(s)

For the pilot in general:

Lead contact person	[name]	[company]	[e-mail address]

If the pilot is operated across multiple geographical sites, provide a contact person per site:

Location / site 1	[name]	[company]	[e-mail address]
Location / site 2	[name]	[company]	[e-mail address]

7.3 Description of the Data to be Collected

7.3.1 Description of the Profile of Persons Concerned

Describe briefly and concisely which data will be collected. If it relates to individual persons (including individual households, or their devices/equipment), describe the types of persons.
[free text description]

To which CyberSEAS asset classes does the pilot relate? Tick all that apply.
☐ Power and Energy System (PES) Components: These assets are mostly tangible and physical in nature. Assets, which are associated to the process zone and component layer of the SGAM architecture, are considered under PES Component asset class. Examples include generator, transmission line, transformers and loads.
☐ Information Management (IM) Components: These assets are mostly tangible and physical in nature. Assets, which are associated to the zones field, station, operation, market or enterprise and to the component layer of the SGAM architecture, are considered under IM Component asset class. Examples include relays, PLC, IEDs, physical communication links, routers, gateways, computers and servers.
☐ Communication: This asset class is derived by mapping logical communication networks across the SGAM grid plane to the communication layer of SGAM reference architecture. Therefore, such assets are considered under Communication asset class. These assets are mostly intangible and cyber or logical in nature. Examples may include wide area network (WAN), neighbourhood area network (NAN) and field area network (FAN).
☐ Information: This asset class is derived by mapping various data created and exchanged across the SGAM grid plane to the information layer of SGAM reference architecture. Therefore, such assets are considered under Information asset class. These assets are intangible and cyber in nature. Examples include measurement data, grid data, market data, customer information data, contractual agreements and various databases.
☐ Functional: This asset class is derived by mapping various software executing different functionalities across the SGAM grid plane to the functional layer of SGAM reference architecture. Therefore, such assets are considered under

functional asset class. These assets can be intangible and cyber in nature. Examples include state estimation programs, SCADA functions, optimal power dispatch programs and aggregation software.

☐ Business: This asset class is derived by mapping various policies, processes, procedures and objectives across the SGAM grid plane to the business layer of SGAM reference architecture. Therefore, such assets are considered under business asset class. These assets are mostly organizational in nature. Examples include patching processes, asset management processes.

☐ Human: This asset class consists of various personnel involved in different roles across the SGAM grid plane. Therefore, such assets are considered under human asset class. Examples include state network operators, maintenance personnel, customer service personnel and database administrators.

In your opinion, is any part of the data linkable to individual persons (including individual households, or their devices/equipment)
☐ Yes
☐ No

IF THE ANSWER TO THE QUESTION ABOVE IS 'NO', THE QUESTIONS BELOW ARE INAPPLICABLE, SINCE THEY RELATE TO PERSONAL DATA ONLY. IN THAT CASE, YOU MAY PROCEED DIRECTLY TO SECTION 6.9 OF THIS ANNEX, AND SUBMIT YOUR RESPONSE/ASSESSMENT TO THE INTERNAL ETHICS COMMITTEE. YOU MAY LEAVE THE OTHER QUESTIONS BLANK.

Are some of the persons identifiable as vulnerable? Possibilities include:
☐ Minors (under 18)
☐ Physically impaired persons
☐ Mentally impaired persons
☐ Financially vulnerable persons (e.g. persons who are known to have a lower income)
☐ Other: [free text description]
☐ N.A.: none of the persons can be considered vulnerable, or they are not identifiable as such.

7.3.2 Description of the Data Concerned

Describe briefly and concisely what kind of data will be collected. The categories below can be used as a starting point, but specify the data enough to make the description meaningful.

General description:

[free text description]

Relevant categories of data:

☐ Basic identity information (name)
☐ Contact information
☐ Family situation (married, children, …)
☐ Financial situation (income)

☐ Energy consumption data
☐ Energy equipment data
☐ Energy usage patterns or profile
☐ Prior incident data

☐ Physical characteristics
☐ Health information prior to the pilot
☐ Health information during the pilot

☐ Video imagery during the pilot
☐ Audio recordings during the pilot
☐ Geolocation during the pilot (specific to the individual, not just by inferring where the pilot takes place)

☐ Other: [free text description]

7.3.3 Estimated Number of Persons Concerned

Provide a best estimate of how many persons are expected to be impacted – i.e. how many persons' data will be collected? If applicable: break down into categories
[free text description]

7.3.4 External Recruitment of Research Participants

Will the pilot only involve internal persons of CyberSEAS partners?
☐ Yes, only employees, fixed contractors, directors, etc. ☐ No, also persons who have no permanent link to CyberSEAS partners.

7.3.5 Selection Criteria

On what basis are the persons selected?
☐ Everyone who is relevant will participate, e.g. all employees working with a particular device or on a particular site ☐ We will preselect persons who are relevant on the basis of the following criteria: [specify] ☐ Only persons who volunteer ☐ Only persons who don't opt out ☐ Other – please specify

7.3.6 Data Collection Methods

How is data collected?
☐ Self reporting by the participants ☐ Self reporting will, however, be limited in the present case to a preparatory interview. ☐ Fully automatic measuring / observation / recording without human intervention during data collection or clean-up ☐ Automatic measuring / observation with human intervention (e.g. to add comments, observations, or clean data) ☐ Via video footage and eye-tracking technologies.

☐ Other – please specify

7.4 Description of the Intended Use of the Data, Including Data Sharing

7.4.1 Intended Use

Describe briefly and concisely what the pilot participants plan to do with the data. If possible, indicate which organisation will do what – e.g. X will collect, Y will analyse, Z will provide recommendations, etc.
[free text description]

7.4.2 Intended Recipients (Data Sharing)

Who will obtain access to the raw data (i.e. unprocessed original data, without undergoing any kind of redaction or editing, including any pseudonymization or anonymization)
☐ The site owner ☐ The following CyberSEAS pilot participants: [names or acronyms of the partners] ☐ The following CyberSEAS partners who are not directly involved in the pilot : [names or acronyms of the partners] ☐ The following service providers who are not CyberSEAS partners [specify name and role – e.g. data collection services, data analysis, researchers] ☐ The persons whose data is being collected (if they request it) ☐ Other – please specify Will the data be sent to a destination (a company or infrastructure) located outside the European Economic Area (i.e., the EU Member States, Iceland, Liechtenstein or Norway)? ☐ No ☐ Yes : [specify the countries and reason for transfer]

7.4.3 Anonymisation or Pseudonymisation (if any)

Will the data be anonymised or pseudonymised at any stage? **Anonymisation means that it is impossible to link data back to a person, irrespective of who is trying to re-link the data. Fully statistical data is typically anonymous.** **Pseudonymisation means that the data cannot be directly linked to a person by the recipient, but it could still be linked back to the person with assistance from another party than the recipient. E.g. blurred video images or gait analysis data without direct identifiers referring to the person would qualify.** **If either box is ticked, specific when and why the process is used (e.g. prior to sharing it with other pilot participants, to allow analysis without easy identification of the participants).**
☐ The data is anonymised using the following approach: [specify] ☐ The data is pseudonymised using the following approach:

7.4.4 Intended Retention

For how long will the data be kept?
☐ For the duration of the CyberSEAS project; then it will be deleted or anonymised (as defined in the preceding question). ☐ For a fixed duration beyond the CyberSEAS project: [specify the term, e.g. x years after the end of the CyberSEAS project] ☐ For a different duration: [specify expected date or criterion]

Who will keep the data?
☐ The site owner ☐ The following CyberSEAS pilot participants: [names or acronyms of the partners] ☐ The following CyberSEAS partners who are not directly involved in the pilot [names or acronyms of the partners] ☐ Others: [free text description]

7.5 Potential Risks for the Persons Concerned

Describe briefly and concisely what the potential risks are for the persons concerned, taking into account the measures that you will implement – i.e. it is not necessary to report theoretical risks that you've eliminated because of the measures you've taken. The categories below can be used as a starting point, if desired.

☐ Energy outages
☐ Reputational risks
☐ Financial risks
☐ Physical health risk
☐ Mental health risk (increased risk of stress, anxiety, discomfort)
☐ Other – please specify

Are there risks to third parties (persons other than the person whose data is collected)? If so, please elaborate.

☐ Other household members of the person
☐ Visitors of the person
☐ Site visitors
☐ Other – please specify

7.6 Lawfulness of the Processing (Including Consent)

The pilot will proceed on the basis of:

☐ **Consent**. This implies that persons have the free choice not to participate, volunteer to do so, and can withdraw their consent at any time. This option is **not available when collecting data of employees**, since they are legally presumed to be subject to pressure to consent.

☐ The **necessity to process the data for the performance of a contract** between the person concerned and the organisation collecting the data.

☐ The **necessity to process the data for compliance with a legal obligation** of the organisation collecting the data.

☐ The **necessity to process the data to protect the vital interests of individual natural persons.**

☐ The **legitimate interest** of the organisation collecting the data. **This box should be ticked when employees are involved**, or when the options above are not available.

7.7 Transparency Towards the Persons Concerned

The following measures are taken to ensure transparency to the persons concerned:

☐ They are provided with an information sheet based on the templates in CyberSEAS D10.1 in a language that they understand, using terminology that the person concerned will understand.

☐ They are given an additional spoken explanation by the organisation(s) collecting the data, and invited to ask any questions for clarification.

☐ They can opt out at any time, and may ask that their data is deleted.

☐ They are allowed to ask for a copy of their data until it is deleted or fully anonymised.

7.8 Mitigation and Protection Measures Taken

The following measures are taken prior to initiating the pilot (in addition to obtaining approval of the CyberSEAS Ethics Committee):

☐ There is a prior consultation with representatives of the persons concerned

☐ There is a separate approval procedure (in addition to obtaining approval of the CyberSEAS Ethics Committee): [specify]

☐ The pilot will use certified or audited technologies: [specify]

☐ The pilot will be executed under the supervision of a DPO: [provide contact details]

☐ The pilot will be executed under the supervision of another qualified and independent ☐ professional, such as a CIO or ombudsman

☐ Data will be anonymised prior to sharing it with third parties

☐ Data will be pseudonymised prior to sharing it with third parties

☐ Access control measures are in place to ensure data can only be accessed by specifically mandated persons

☐ Logging measures are in place to ensure data access or use (including modification or deletion) can be detected

☐ All research data will be encrypted and stored on a password protected system or in a secure location

☐ All researchers are competent to carry out the research and have received appropriate training.

☐ All researchers are aware of their confidentiality obligations

☐ Appropriate insurance and indemnity is in place for this research, at all participating sites and for each investigator.

☐ Other – please specify

7.9 Approval Process and Log

7.9.1 Application Submission

Applicant's Name	Version number of the application, and date of submission for approval	Applicant's signature

7.9.2 Application Process and Log

Phase	Date	Action or decision
Feedback from the Internal Ethics Committee (if any)		
Resubmission (if any)		
Approval by the Internal Ethics Committee		

7.9.3 Application Approval by the Ethics Committee

Committee Member's Name	Version number of the application, and date of approval	Committee Member's signature

If any part of the pilot changes in a manner that raises doubts on the completeness or accuracy of this description, or that causes ethics or compliance doubts, the opinion of the Internal Ethics Committee should be sought.