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

© Copyright by the CyberSEAS Consortium
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No 101020560

DOCUMENT D3.2
DELIVERABLE STATE FINAL
REVISION V1.0
DELIVERY DATE 16/08/2022
DISSEMINATION LEVEL CO

WORKPACKAGE WP3
PROGRAMME H2020-SU-DS-2020
IDENTIFIER
GRANT AGREEMENT ID 101020560
PROJECT START DATE 01/10/2021
DURATION 3 YEARS
DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain CyberSEAS consortium parties, and may not be reproduced or copied without permission. All CyberSEAS consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CyberSEAS consortium as a whole, nor a certain party of the CyberSEAS consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

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 Nº 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

### TOPIC

### 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 FÖRDERUNG 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 LYSEIΣ PIROFORIKIS AUTOMATISOU & TILIPIKOINIONIION 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 NACIONAL DE TRANSPORT AL ENERGIE 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

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

Document History ........................................................................................................................................... 4
Table of Contents ......................................................................................................................................... 5
List of Figures.............................................................................................................................................. 6
List of Tables.............................................................................................................................................. 7
List of Acronyms and Abbreviations .......................................................................................................... 8
Executive Summary .................................................................................................................................... 10
1 Introduction ............................................................................................................................................... 11
2 (Non-)Functional Requirements and Technical Specifications .......................................................... 13
3 CyberSEAS SELP Requirements ........................................................................................................ 58
4 Conclusions ............................................................................................................................................... 65
5 References ............................................................................................................................................... 66
6 ANNEX I - Pilot Description, Privacy Risk Assessment and Approvals Process ............................. 68
List of Figures

Figure 1: Overview of the methodology used for identifying (non-)functional requirements and the technical specification.................................................................14
Figure 2: Monitoring and evaluation structure ..........................................................63
Figure 3: Piloting assessment and approvals process..................................................64
List of Tables

Table 1: Template for the documentation of the (non-)functional requirements per pilot....15
Table 2: Template for the documentation of the technical specification per pilot. ............16
Table 3: Overview of ID building blocks. .................................................................17
Table 4: Functional and non-functional requirements for the Italian pilot......................18
Table 5: Technical specification for the Italian pilot.................................................19
Table 6: Functional and non-functional requirements for the Slovenian & Croatian pilot ....26
Table 7: Technical specification for the Slovenian & Croatian pilot ................................27
Table 8: Functional and non-functional requirements for the Romanian pilot................35
Table 9: Technical specification for the Romanian pilot .........................................37
Table 10: Functional and non-functional requirements for the Finnish pilot..................40
Table 11: Technical specification for the Finnish pilot .............................................43
Table 12: Functional and non-functional requirements for the Estonian pilot.............46
Table 13: Technical specification for the Estonian pilot............................................49
List of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA</td>
<td>Two Factor Authentication</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APIDS</td>
<td>Application Protocol-Based Intrusion Detection System</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CER</td>
<td>Critical Entities Resilience</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial-off-the-Shelf Solution</td>
</tr>
<tr>
<td>CTI</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>EDR</td>
<td>Endpoint Detection and Response</td>
</tr>
<tr>
<td>EPES</td>
<td>Electrical Power and Energy System</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAN</td>
<td>Field Area Network</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-Based Intrusion Detection System</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IDP</td>
<td>Intrusion Detection and Prevention</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEC</td>
<td>Internal Ethics Committee</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IM</td>
<td>Information Management</td>
</tr>
<tr>
<td>IoC</td>
<td>Indicator of Compromise</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MDR</td>
<td>Managed Detection and Response</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>NAN</td>
<td>Neighbourhood Area Network</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>PAM</td>
<td>Privilege Access Management</td>
</tr>
<tr>
<td>PES</td>
<td>Power and Energy System</td>
</tr>
<tr>
<td>PIDS</td>
<td>Protocol-Based Intrusion Detection System</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PSA</td>
<td>Platform Security Architecture</td>
</tr>
<tr>
<td>RRI</td>
<td>Responsible Research and Innovation</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SE</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>SELP</td>
<td>Societal, Ethical, Legal and Privacy</td>
</tr>
<tr>
<td>SEP</td>
<td>Societal, Ethical and Privacy</td>
</tr>
<tr>
<td>SGAM</td>
<td>Smart Grid Architecture Model</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SOAR</td>
<td>Security Orchestration, Automation, and Response</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Centre</td>
</tr>
<tr>
<td>SOP</td>
<td>Security Operation Playbook</td>
</tr>
<tr>
<td>TSO</td>
<td>Transmission System Operator</td>
</tr>
<tr>
<td>UBA</td>
<td>User Behaviour Analytics</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>XDR</td>
<td>Extended Detection and Response</td>
</tr>
</tbody>
</table>
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 ID | 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>
<thead>
<tr>
<th>High-Level Requirement</th>
<th>Functional Requirement</th>
<th>Derived Technical Specification</th>
<th>Available Commercial-off-the-Shelf Solutions and/or Security Functions</th>
<th>Constraints and Parameters</th>
<th>Related CyberSEAS Tools</th>
</tr>
</thead>
</table>

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

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.

<table>
<thead>
<tr>
<th>ID types (prefix)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>Functional component</td>
</tr>
<tr>
<td>Req</td>
<td>(Non-)functional requirement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pilot (infix)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Italian pilot</td>
</tr>
<tr>
<td>S</td>
<td>Slovenian and Croatian pilot</td>
</tr>
<tr>
<td>R</td>
<td>Romanian pilot</td>
</tr>
<tr>
<td>F</td>
<td>Finnish pilot</td>
</tr>
<tr>
<td>E</td>
<td>Estonian pilot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enumeration (suffix)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For functional components: Running number of functional components in a pilot</td>
<td>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.</td>
</tr>
<tr>
<td>For (non-)functional requirements: Number of the functional component and the running number of the requirement, delimited by a dot</td>
<td>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.</td>
</tr>
</tbody>
</table>
2.2 Italian Pilot

2.2.1 Functional Requirements and Non-Functional Requirements

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-I.1</td>
<td>Cabin</td>
<td>Avoid intrusion into the cabin</td>
<td>Req-I.1.1</td>
<td>Functional</td>
<td>Detection of unauthorized access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.1.2</td>
<td>Functional</td>
<td>Promptly alert whether an intrusion takes place</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.1.3</td>
<td>Non-Functional</td>
<td>Real-time communication of intrusion alert</td>
</tr>
<tr>
<td>FC-I.2</td>
<td>Data storage</td>
<td>Tamper resistant storage support</td>
<td>Req-I.2.1</td>
<td>Non-Functional</td>
<td>Support of different levels of access to the data storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.2.2</td>
<td>Functional</td>
<td>Ability to restore a previous system state</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.2.3</td>
<td>Functional</td>
<td>Protection against unauthorized access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.2.4</td>
<td>Non-Functional</td>
<td>Traceability of data modification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.2.5</td>
<td>Functional</td>
<td>Visualize user activity logs and content processing logs</td>
</tr>
<tr>
<td>FC-I.3</td>
<td>Management software</td>
<td>Avoid intrusion into the IT network</td>
<td>Req-I.3.1</td>
<td>Functional</td>
<td>Promptly alert whether an intrusion takes place</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.3.2</td>
<td>Functional</td>
<td>Intrusion detection on software management system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.3.3</td>
<td>Non-Functional</td>
<td>Traceability of data modification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.3.4</td>
<td>Non-Functional</td>
<td>Real-time communication of intrusion alert</td>
</tr>
<tr>
<td>FC-I.4</td>
<td>Decision support system</td>
<td>Guarantee support for the decision-making process of the IT personnel</td>
<td>Req-I.4.1</td>
<td>Functional</td>
<td>Early detection of an intrusion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.4.2</td>
<td>Functional</td>
<td>Ability to differentiate decision support for different kind of cyberattack</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.4.3</td>
<td>Functional</td>
<td>Tracking of actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-I.4.4</td>
<td>Functional</td>
<td>Offline Risk Assessment for enhancing strategic protection of grid</td>
</tr>
</tbody>
</table>
## 2.2.2 Technical Specification

Table 5: Technical specification for the Italian pilot

<table>
<thead>
<tr>
<th>High-Level Requirement</th>
<th>Functional Requirement</th>
<th>Derived Technical Specification</th>
<th>Available Commercial-off-the-Shelf Solutions and/or Security Functions</th>
<th>Constraints and Parameters</th>
<th>Related CyberSEAS Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper resistant storage support</td>
<td>Support of different levels of access to the data storage</td>
<td>Two factor authentication</td>
<td>Entrust</td>
<td>Must verify the domain where TFA is used</td>
<td>ATRS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Duo Multi-Factor Authentication</td>
<td>Phishing protections</td>
<td></td>
</tr>
</tbody>
</table>
D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Role management</th>
<th>Login Radius</th>
<th>On-Prem solutions only</th>
<th>Award force Role management</th>
<th>Limited access to specific segmented networks</th>
<th>Orange Scrum role management</th>
<th>Data confidentiality requirements</th>
<th>Ability to restore a previous system state</th>
<th>Automated creation of backups</th>
<th>IBM data protection</th>
<th>Segment</th>
<th>RuleX</th>
<th>Acronis</th>
<th>Offsite and offline solutions</th>
<th>-</th>
</tr>
</thead>
</table>
## D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Protection against unauthorized access</th>
<th>Encryption</th>
<th>Known secure algorithms only</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Atakama file encryption software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero trust security by NordLayer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AxCrypt Premium Folder Lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CryptoForge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability of data modification</th>
<th>Logging</th>
<th>On-Prem solutions only</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sydecon</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize user activity logs and content processing logs</th>
<th>Data visualization and data analytics</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EventLog Analyzer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SmartLook</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the cabin</th>
<th>Detection of unauthorized access</th>
<th>Access control</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promptly alert whether an intrusion takes place</td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td>ARTEMIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ascom alert management system</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the IT network</th>
<th>Promptly alert whether an intrusion takes place</th>
<th>Oaktree products</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time communication of intrusion alert</td>
<td>Polling technique</td>
<td>Ability to detect people and alert operators</td>
<td>ARTEMIS</td>
</tr>
<tr>
<td>Stream data mining</td>
<td>Splunk enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SignalR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>gRPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control via badge</td>
<td>Desk Alert</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the IT network</th>
<th>Promptly alert whether an intrusion takes place</th>
<th>Ability to detect intrusion</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect against unauthorized access</td>
<td>Encryption</td>
<td>Known secure algorithms only</td>
<td>PKI</td>
</tr>
<tr>
<td>Detection of unauthorized access</td>
<td>Atakama file encryption software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero trust security by NordLayer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AxCrypt Premium Folder Lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CryptoForge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protection against unauthorized access</th>
<th>Encryption</th>
<th>Known secure algorithms only</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Atakama file encryption software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero trust security by NordLayer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AxCrypt Premium Folder Lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CryptoForge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability of data modification</th>
<th>Logging</th>
<th>On-Prem solutions only</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sydecon</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize user activity logs and content processing logs</th>
<th>Data visualization and data analytics</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EventLog Analyzer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SmartLook</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the cabin</th>
<th>Detection of unauthorized access</th>
<th>Access control</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promptly alert whether an intrusion takes place</td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td>ARTEMIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ascom alert management system</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the IT network</th>
<th>Promptly alert whether an intrusion takes place</th>
<th>Oaktree products</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect against unauthorized access</td>
<td>Encryption</td>
<td>Known secure algorithms only</td>
<td>PKI</td>
</tr>
<tr>
<td>Detection of unauthorized access</td>
<td>Atakama file encryption software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero trust security by NordLayer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AxCrypt Premium Folder Lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CryptoForge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability of data modification</th>
<th>Logging</th>
<th>On-Prem solutions only</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sydecon</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize user activity logs and content processing logs</th>
<th>Data visualization and data analytics</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EventLog Analyzer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SmartLook</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the cabin</th>
<th>Detection of unauthorized access</th>
<th>Access control</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promptly alert whether an intrusion takes place</td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td>ARTEMIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oaktree products; Digital alert systems; HSS engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ascom alert management system</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avoid intrusion into the IT network</th>
<th>Promptly alert whether an intrusion takes place</th>
<th>Oaktree products</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect against unauthorized access</td>
<td>Encryption</td>
<td>Known secure algorithms only</td>
<td>PKI</td>
</tr>
<tr>
<td>Detection of unauthorized access</td>
<td>Atakama file encryption software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero trust security by NordLayer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AxCrypt Premium Folder Lock</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CryptoForge</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability of data modification</th>
<th>Logging</th>
<th>On-Prem solutions only</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sydecon</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize user activity logs and content processing logs</th>
<th>Data visualization and data analytics</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EventLog Analyzer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SmartLook</td>
<td></td>
</tr>
</tbody>
</table>
### Table: CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>Solution</th>
<th>Description</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anomaly detection</strong></td>
<td>Ascom alert management system</td>
<td>alerting operators</td>
<td></td>
</tr>
<tr>
<td><strong>Intrusion detection on software management system</strong></td>
<td>DNS filtering, Perimeter 81, SIEM system</td>
<td>On-Prem solutions only, Limited access to specific segmented networks, Data confidentiality requirements</td>
<td>BP-IDS, ARTEMIS</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Signature-based method</strong></td>
<td>NIDS, HIDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Anomaly-based method</strong></td>
<td>PIDS, APIDS, SolarWinds Security Event Manage, Bro, OSSEC, Security onion, Verve security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Traceability of data modification</strong></td>
<td>Logging, Sydecon</td>
<td>On-Prem solutions only, Limited access to specific segmented networks, Data confidentiality requirements</td>
<td>SIEM</td>
</tr>
<tr>
<td><strong>Real-time communication of intrusion alert</strong></td>
<td>Polling technique, Splunk enterprise, SignalR</td>
<td>Ability to detect people</td>
<td>SIEM</td>
</tr>
<tr>
<td>D3.2 CyberSEAS technical requirements, SELP requirements and system specifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Stream data mining</strong></td>
<td><strong>and alert operators</strong></td>
<td><strong>Visualisation of alert</strong></td>
<td><strong>Creation of a dashboard to visualize alert</strong></td>
</tr>
<tr>
<td>gRPC</td>
<td>Desk Alert</td>
<td>Visualisation of alert</td>
<td>Creation of a dashboard to visualize alert</td>
</tr>
<tr>
<td><strong>Guarantee support for the decision-making process of the IT personnel</strong></td>
<td><strong>Early detection of an intrusion</strong></td>
<td><strong>DNS filtering</strong></td>
<td>Perimeter 81</td>
</tr>
<tr>
<td>Firewall</td>
<td><strong>Signature-based method</strong></td>
<td><strong>NIDS</strong></td>
<td><strong>HIDS</strong></td>
</tr>
<tr>
<td>Anomaly-based method</td>
<td><strong>PIDS</strong></td>
<td><strong>APIDS</strong></td>
<td>SolarWinds Security Event Manage Bro OSSEC Security onion Verve security</td>
</tr>
<tr>
<td><strong>Ability to differentiate decision support for different kind of cyberattack</strong></td>
<td><strong>Data visualization and optimization</strong></td>
<td><strong>-</strong></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td><strong>Tracking of actions</strong></td>
<td><strong>Logging</strong></td>
<td><strong>Sydecon</strong></td>
<td>On-Prem solutions only Limited access to specific segmented networks Data confidentiality requirements</td>
</tr>
<tr>
<td><strong>Offline Risk Assessment for enhancing strategic protection of grid</strong></td>
<td><strong>-</strong></td>
<td><strong>-</strong></td>
<td>On-Prem solution only</td>
</tr>
<tr>
<td><strong>Near real-time Risk Assessment for tactical protection of grid</strong></td>
<td><strong>-</strong></td>
<td><strong>-</strong></td>
<td>Cloud-based</td>
</tr>
<tr>
<td>Requirement</td>
<td>Solution</td>
<td>Cloud-based</td>
<td>SEurGrid RATING</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Provide IT personnel with an updated Situational Awareness for rapid understanding of the status of the assets</td>
<td>-</td>
<td></td>
<td>Situational Awareness (ENG)</td>
</tr>
<tr>
<td>Visualize attacker activities and movements inside the network</td>
<td>DNS filtering</td>
<td>SiEM system</td>
<td>On-Prem solutions only</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td></td>
<td>BP-IDS</td>
</tr>
<tr>
<td></td>
<td>Signature-based method</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomaly-based method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To be promptly warned in case of an intrusion into the SCADA system</td>
<td>Ability to early detect an intrusion</td>
<td>Perimeter 81</td>
<td>On-Prem solutions only</td>
</tr>
<tr>
<td></td>
<td>DNS filtering</td>
<td></td>
<td>BP-IDS</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>SiEM system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signature-based Method</td>
<td>NIDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomaly-based Method</td>
<td>HIDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>APIDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Security Event Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bro</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSSEC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security onion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verve security</td>
<td></td>
</tr>
<tr>
<td>Traceability of actions carried out by the attacker</td>
<td>Logging</td>
<td>SIAM RPM</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td>Integration with advanced tamper resistant storage to avoid data modification</td>
<td>-</td>
<td>Diskshield</td>
<td>Data communicatio n requirements</td>
</tr>
<tr>
<td>Impede the access to the disconnector to unauthorized people</td>
<td>Detection of unauthorized access</td>
<td>-</td>
<td>CyberRange</td>
</tr>
<tr>
<td></td>
<td>Remote control of potential cyberattacks</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Promptly alert whether an intrusion takes place</td>
<td>Alert system based on sensors</td>
<td>Oaktree products</td>
<td>Ability to detect people and alert operators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital alert systems</td>
<td>BP-IDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HSS engineering</td>
<td></td>
</tr>
</tbody>
</table>
### D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>System</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to restore a previous system state</td>
<td>Automated creation of backups</td>
<td>IBM Data protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Segment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RuleX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acronis</td>
</tr>
<tr>
<td>Real-time communication of damage alert</td>
<td>Sensors</td>
<td>Oaktree products</td>
</tr>
<tr>
<td></td>
<td>Anomaly detection</td>
<td>Digital alert systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Limited access to specific segmented networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Limited access to specific segmented networks</td>
</tr>
<tr>
<td></td>
<td>HSS engineering</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td>Avoid Smart Meter sabotage</td>
<td>Ability to early detect anomalies</td>
<td>Constant Monitoring of consumption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advance DMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BP-IDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecurGrid</td>
</tr>
<tr>
<td>Promptly alert whether a sabotage takes place</td>
<td>Alert system</td>
<td>Oaktree products</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital alert systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HSS engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ascom alert management system</td>
</tr>
<tr>
<td>Real-time communication of alerts</td>
<td>Anomaly Detection</td>
<td>Oaktree products</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BP-IDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Situational Awareness (ENG)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecurGrid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIEM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Situational Awareness (ENG)</td>
</tr>
</tbody>
</table>
## 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

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

Table 7: Technical specification for the Slovenian & Croatian pilot

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-S.5 Incident response, CTI, risk assessment and decision support</td>
<td>Support to IT personnel and network operators in case of a cyberattack</td>
<td>Req-S.5.1 Non-Functional</td>
<td>Security patterns and libraries to implement IEC 62443-4-2 requirements in software applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.5.2 Functional</td>
<td>Assessment of risks based on a common approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.5.3 Functional</td>
<td>Decision analysis and visualisations to mitigate incidents and threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC-S.6 Social engineering prevention</td>
<td>Implementation of security measures to prevent vulnerabilities exploitation and stealing of credentials – prevention to gain unauthorised access to IT segment, VPN and OT environment</td>
<td>Req-S.6.1 Functional</td>
<td>Social Engineering (SE) ongoing attack detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.6.2 Functional</td>
<td>Alarm and visualize ongoing SE attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC-S.7 Simulation training</td>
<td>Support for cyberattack pattern recognition</td>
<td>Req-S.7.1 Functional</td>
<td>Attack-defence-simulation to study potential attack and countermeasures evolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC-S.8 Indicators of compromise (IoC), and Cyber Threat Intelligence (CTI) exchange</td>
<td>Support for the exchange of IoC and CTI between different organisations (TSOs, CERTs …)</td>
<td>Req-S.8.1 Functional</td>
<td>Cyber threat analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.8.2 Functional</td>
<td>CTI exchange and incident response management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.8.3 Non-Functional</td>
<td>CTI standards, data formats, ontologies, and exchange mechanisms (protocols, APIs …)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.8.4 Non-Functional</td>
<td>Common CTI repositories and libraries</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req-S.8.5 Non-Functional</td>
<td>CTI exchange platform and protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation of vulnerability detection system for weather stations</td>
<td>Vulnerabilities reporting for IED components (hardware, operating system, libraries, etc.)</td>
<td>Events data capturing in IEDs</td>
<td>Events time stamping in IEDs</td>
<td>IED faults and vulnerabilities diagnosis</td>
<td>Data visualization and data reporting</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Poisoned data detection</td>
<td>Weather data capturing</td>
<td>IBM Watson Studio</td>
<td>RStudio</td>
<td>V7</td>
<td>Gurobi Optimizer</td>
</tr>
<tr>
<td>Visualize reporting</td>
<td>Data visualization and data analytics</td>
<td>EventLog Analyzer</td>
<td>Google Analytics</td>
<td>SmartLook</td>
<td>Heimdall</td>
</tr>
<tr>
<td>Early notification to IT personnel in case of an intrusion in the SCADA system and SUMO dynamic rating system</td>
<td>Definition of business/process level KPIs related to intrusions</td>
<td>KPI software</td>
<td>Risk assessment software</td>
<td>Decision support system</td>
<td>Sisense</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BP-IDS</td>
</tr>
<tr>
<td>Intrusion notification</td>
<td>Alert system based on sensors</td>
<td>Oaktree products</td>
<td>On-Prem solutions only</td>
<td>BP-IDS</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Polling technique</td>
<td>Digital alert systems</td>
<td>Limited access to specific segmented networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ascom alert system</td>
<td>Data confidentiality requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SignalIR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Desk Alert</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Poisoned data detection</th>
<th>Data capturing</th>
<th>IBM Watson Studio</th>
<th>On-Prem solutions only</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data analytics</td>
<td>RStudio</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Machine learning anomaly detection</td>
<td>V7</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statistical anomaly detection</td>
<td>Gurobi Optimizer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize KPIs and logs</th>
<th>Data visualization and data analytics</th>
<th>Google Data Studio</th>
<th>On-Prem solutions only</th>
<th>BP-IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dashboard software</td>
<td>Google Analytics</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Databox</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluvio</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implementation of a system to detect anomalous events and traffic in the SCADA/SUM O managed network of power lines, implementation of security event management</th>
<th>Data capturing from sensors</th>
<th>QRadar</th>
<th>On-Prem solutions only</th>
<th>CI SOC ARTEMIS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SIEM</td>
<td>Spluk</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LogRythm</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIEMONster</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Insights and predictions, through AI algorithms applied to collected data</th>
<th>Data analytics</th>
<th>IBM Watson Studio</th>
<th>On-Prem solutions only</th>
<th>CI SOC ARTEMIS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Machine learning anomaly detection</td>
<td>RStudio</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>V7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Technique</td>
<td>Software</td>
<td>Data confidentiality requirements</td>
<td>CI/ARTEMIS</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>3.2 CyberSEAS technical requirements, SELP requirements and system</td>
<td>Statistical anomaly detection</td>
<td>Gurobi Optimizer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specifications</td>
<td>Risk assessment software</td>
<td>Callio</td>
<td>Limited access to specific segmented networks</td>
<td>CI SOC ARTEMIS</td>
</tr>
<tr>
<td>Identification and addressing cascading effects</td>
<td>Risk assessment software</td>
<td>RiskWatch</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk assessment software</td>
<td>RATING</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk assessment software</td>
<td>CASIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>Callio</td>
<td>Limited access to specific segmented networks</td>
<td>CI SOC ARTEMIS</td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>RiskWatch</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>CASIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>Cisco Umbrella</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>DeCYFIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>Recorded Future</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CTI software</td>
<td>Dataminr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visualize results and logs</td>
<td>Data visualization and data analytics</td>
<td>EventLog Analyzer</td>
<td>Limited access to specific segmented networks</td>
<td>CI SOC ARTEMIS</td>
</tr>
<tr>
<td></td>
<td>Data visualization and data analytics</td>
<td>Google Data Studio</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data visualization and data analytics</td>
<td>Google Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data visualization and data analytics</td>
<td>SmartLook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data visualization and data analytics</td>
<td>Databox</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data visualization and data analytics</td>
<td>Cluvio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementati on of a system to track anomalous events on VPN connections</td>
<td>Information collection from IT devices, servers, workstations, firewalls</td>
<td>QRadar</td>
<td>Limited access to specific segmented networks</td>
<td>CI SOC ARTEMIS</td>
</tr>
<tr>
<td>and in the IT environment, and to track user behaviour</td>
<td>and VPN connections</td>
<td>Spluk</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information collection from IT devices, servers, workstations, firewalls</td>
<td>LogRhythm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User behaviour information collection</td>
<td>Authentication</td>
<td>SIEMMonster</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>SIEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>SIEMObject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>Spluk</td>
<td>Limited access to specific segmented networks</td>
<td>CI SOC ARTEMIS</td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>Rapid7</td>
<td>Data confidentiality requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>LogRhythm</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>Spluk</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>Rapid7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data capturing</td>
<td>LogRhythm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Anomalies – uncommon use of user credentials</th>
<th>Network monitoring</th>
<th>MS Azure ATA</th>
<th>Data confidentiality requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint detection and response</td>
<td>Cynet 360</td>
<td>Fortinet</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User behaviour analytics</th>
<th>Data analytics</th>
<th>Splūk</th>
<th>Limited access to specific segmented networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network analytics</td>
<td>Rapid7</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td>UBA platform</td>
<td>LogRythm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vulnerability</td>
<td>MS Azure ATA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanning</td>
<td>Cynet 360</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forensics</td>
<td>Fortinet</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Insights and predictions, through AI algorithms applied to collected data</th>
<th>Data analytics</th>
<th>IBM Watson Studio</th>
<th>Limited access to specific segmented networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Machine learning prediction</td>
<td>RStudio</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td>V7</td>
<td>V7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gurobi Optimizer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threats identifications</th>
<th>Risk assessment software</th>
<th>Callio</th>
<th>Limited access to specific segmented networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CTI software</td>
<td>RiskWatch</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CASIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Umbrella</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeCYFIR</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recorded Future</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dataminr</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visualize results and logs</th>
<th>Data visualization and data analytics</th>
<th>EventLog Analyzer</th>
<th>Limited access to specific segmented networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dashboard software</td>
<td>Google Data Studio</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SmartLook</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Databox</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluvio</td>
<td></td>
</tr>
</tbody>
</table>

**Technologies and tools used:**

- Splūk
- Rapid7
- LogRythm
- IBM Watson Studio
- RStudio
- V7
- Gurobi Optimizer
- Callio
- RiskWatch
- CASIS
- Cisco Umbrella
- DeCYFIR
- Recorded Future
- Dataminr
- EventLog Analyzer
- Google Data Studio
- Google Analytics
- SmartLook
- Databox
- Cluvio

**CI SOC ARTEMIS**

**CI SOC ARTEMIS**

**CI SOC ARTEMIS**

**CI SOC ARTEMIS**

**CI SOC ARTEMIS**

**CI SOC ARTEMIS**
<p>| 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 | Java Eclipse | Java JavaScript | Python | PHP | 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 | 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 |</p>
<table>
<thead>
<tr>
<th>Support for cyberattack pattern recognition</th>
<th>Attack-defence-simulation to study potential attack and countermeasure s evolution</th>
<th>Attack-defence modelling and simulation</th>
<th>AI based attack pattern recognition</th>
<th>Winf River Simics</th>
<th>Simul8</th>
<th>MATLAB</th>
<th>Simulink</th>
<th>Simio</th>
<th>AVEVA</th>
<th>Limited access to specific segmented networks</th>
<th>Attack-Defence Simulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for the exchange of IoC and CTI between different organisations</td>
<td>Cyber threat analysis software</td>
<td>Risk assessment software</td>
<td>CTI software</td>
<td>Callio</td>
<td>RiskWatch</td>
<td>CASIS</td>
<td>Cisco Umbrella</td>
<td>Limited access to specific segmented networks</td>
<td>Data confidentiality requirements</td>
<td>MISP</td>
<td></td>
</tr>
</tbody>
</table>
### D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

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

Page 34 of 79
## 2.4 Romanian Pilot

### 2.4.1 Functional Requirements and Non-Functional Requirements

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

<table>
<thead>
<tr>
<th>Functional Component ID</th>
<th>Functional Component</th>
<th>Related High-Level Requirement</th>
<th>ID of Derived Req.</th>
<th>Type of Derived Req. (Functional, Non-Functional)</th>
<th>Derived Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-R.1</td>
<td>IT intrusion detection system</td>
<td>Implementation of a system to detect anomalous traffic on the network</td>
<td>Req-R.1.1 Non-Functional</td>
<td>Log management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-R.1.2 Functional</td>
<td>Traffic analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-R.1.3 Functional</td>
<td>Automatic generation of alerts and reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-R.1.4 Non-Functional</td>
<td>Traceability of actions and data modification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-R.1.5 Functional</td>
<td>Notifications from sensors</td>
<td></td>
</tr>
<tr>
<td>FC-R.2</td>
<td>Decision support system</td>
<td>Support to IT personnel in case of a cyberattack</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------</td>
<td>------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.1</td>
<td>Functional</td>
<td>Intrusion detection system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.2</td>
<td>Functional</td>
<td>Tracking of actions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.3</td>
<td>Functional</td>
<td>Decision support system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.4</td>
<td>Non-Functional</td>
<td>Cyber awareness training with ambassador programs to increase the cybersecurity culture level (phishing tool)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.5</td>
<td>Non-Functional</td>
<td>Integration with Database Management System (DBMS) that stores data input</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Req-R.2.6</td>
<td>Non-Functional</td>
<td>Integration with model management system to store and access models that are used to make decisions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FC-R.3</th>
<th>Real time cyber security monitoring</th>
<th>Real time cyber security monitoring of events from multiple diverse sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-R.3.1</td>
<td>Non-Functional</td>
<td>Real-Time Log &amp; Data Collection</td>
</tr>
<tr>
<td>Req-R.3.2</td>
<td>Functional</td>
<td>Data collection</td>
</tr>
<tr>
<td>Req-R.3.3</td>
<td>Non-Functional</td>
<td>Data management and correlation</td>
</tr>
<tr>
<td>Req-R.3.4</td>
<td>Functional</td>
<td>Automatic generation of alerts and reporting</td>
</tr>
<tr>
<td>Req-R.3.5</td>
<td>Non-Functional</td>
<td>Assure secure transmission of collected information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FC-R.4</th>
<th>Notification system</th>
<th>Early notification to IT personnel in case of an intrusion in the SCADA system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-R.4.1</td>
<td>Functional</td>
<td>Automatic user notification</td>
</tr>
<tr>
<td>Req-R.4.2</td>
<td>Functional</td>
<td>Ability to early detect an intrusion</td>
</tr>
<tr>
<td>Req-R.4.3</td>
<td>Non-Functional</td>
<td>Traceability of actions carried out by the attacker</td>
</tr>
<tr>
<td>Req-R.4.4</td>
<td>Non-Functional</td>
<td>Run in the background without an active user interface</td>
</tr>
</tbody>
</table>
## 2.4.2 Technical Specification

### Table 9: Technical specification for the Romanian pilot

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

Page 37 of 79
<p>| Support to IT personnel in case of a cyberattack | Intrusion detection system | Early detection of an intrusion | Ability to differentiate good traffic from anomaly traffic | BP-IDS | SIEM |
| 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 | Support decisions that are formulated as semi-structured, complex problem | Decision support for different kind of cyberattack | BP-IDS | SIEM (SAPPAN) |
| Cyber awareness training with ambassador programs to increase the cybersecurity culture level (Phishing tool) | Craft email messages using known vendor templates | 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 &amp; alerting | Prioritization, analytics &amp; AI for alerts | | |</p>
<table>
<thead>
<tr>
<th>and Reporting</th>
<th>Definition of security workflows and alerting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Warning on high level alerts</td>
</tr>
<tr>
<td></td>
<td>Displaying high level alerts in a compact way</td>
</tr>
<tr>
<td></td>
<td>Storing high level alerts</td>
</tr>
<tr>
<td></td>
<td>Define event rules that will generate alerts</td>
</tr>
<tr>
<td></td>
<td>Define user-specified notifications</td>
</tr>
<tr>
<td></td>
<td>Define alerts for various active database rules</td>
</tr>
<tr>
<td></td>
<td>Ability to define and schedule ad-hoc reports defined by the user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Early notification to IT personnel in case of an intrusion in the SCADA system</th>
<th>Automatic user notification</th>
<th>Transmits alarm information anywhere via text-to-voice phone calls, SMS text messages, emails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to early detect an intrusion</td>
<td>DNS filtering</td>
<td>Perimeter 81</td>
</tr>
<tr>
<td>Firewall</td>
<td>Signature-based method</td>
<td>NIDS</td>
</tr>
<tr>
<td>Anomaly-based method</td>
<td>BP-IDS</td>
<td>On-Prem solutions only</td>
</tr>
<tr>
<td></td>
<td>SIEM system</td>
<td>Limited access to specific segmented networks</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td>SIEM system</td>
<td></td>
</tr>
<tr>
<td>Traceability of actions carried out by the attacker</td>
<td>Logging</td>
<td>SIAM RPM</td>
</tr>
<tr>
<td></td>
<td>SolarWinds</td>
<td>On-Prem solutions only</td>
</tr>
<tr>
<td></td>
<td>Security Event Manage</td>
<td>Limited access to specific segmented networks</td>
</tr>
<tr>
<td></td>
<td>Bro</td>
<td>Data confidentiality requirements</td>
</tr>
<tr>
<td></td>
<td>OSSEC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security onion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verve security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
<td></td>
</tr>
</tbody>
</table>
## 2.5 Finnish Pilot

### 2.5.1 Functional Requirements and Non-Functional Requirements

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

<table>
<thead>
<tr>
<th>Funct. Compl. ID</th>
<th>Functional Component</th>
<th>Related High-Level Requirement</th>
<th>ID of Derived Req.</th>
<th>Type of Derived Req. (Functional, Non-Functional)</th>
<th>Derived Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-F.1</td>
<td>End point detection and response</td>
<td>Use antivirus/anti-malware Network intrusion prevention Restrict web-based content Software configuration Monitor network traffic content Monitor network traffic flow</td>
<td>Req-F.1.1 Functional</td>
<td>Automatic quarantine of suspicious files</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.2 Functional</td>
<td>Intrusion prevention systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.3 Functional</td>
<td>Scanning and removal of malicious email attachments</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.4 Functional</td>
<td>Blocking unknown or unused attachments that should not be transmitted over email</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.5 Functional</td>
<td>Scanning and analysing compressed and encrypted formats</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.6 Functional</td>
<td>Authenticating mechanisms to filter messages based on validity checks of the sender domain and integrity of messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.7 Functional</td>
<td>Malware analysis engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.8 Functional</td>
<td>Monitoring and analysing traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.1.9 Functional</td>
<td>Monitoring network data for uncommon data flows</td>
<td></td>
</tr>
<tr>
<td>FC-F.2</td>
<td>Software version control Update software</td>
<td>Req-F.2.1 Functional</td>
<td>Upgrading management services to the latest supported and compatible version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.2.2 Functional</td>
<td>Continuous vulnerability scanning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-F.2.3 Functional</td>
<td>Monitoring updated list of software and their status</td>
<td></td>
</tr>
<tr>
<td>FC-F.3</td>
<td>User account management</td>
<td>Req- F.2.4</td>
<td>Functional</td>
<td>Following active vulnerabilities related to the list of software</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User account control</td>
<td>Req- F.3.1</td>
<td>Functional</td>
<td>Managing accounts and permissions used by parties in trusted relationships</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User account management</td>
<td>Req- F.3.2</td>
<td>Functional</td>
<td>Restricting users and accounts to the least privileges they require</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privileged account management</td>
<td>Req- F.3.3</td>
<td>Functional</td>
<td>Limiting administrator accounts from activities that may expose them to potential adversaries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitor application log content</td>
<td>Req- F.3.4</td>
<td>Functional</td>
<td>Limiting permissions so that users and user groups cannot create tokens</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.3.5</td>
<td>Functional</td>
<td>Monitoring authentication logs for succeeded and failed attempts to system and application login</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.3.6</td>
<td>Non-Functional</td>
<td>Formal process for providing permissions and accesses</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.3.7</td>
<td>Non-Functional</td>
<td>Annual check of validation of permissions and accesses</td>
<td></td>
</tr>
<tr>
<td>FC-F.4</td>
<td>User training</td>
<td>Req- F.4.1</td>
<td>Functional</td>
<td>Continuous training for users to identify social engineering activities and spear phishing emails</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User training</td>
<td>Req- F.4.2</td>
<td>Non-functional</td>
<td>Process for reporting suspicious activities</td>
<td></td>
</tr>
<tr>
<td>FC-F.5</td>
<td>Access control</td>
<td>Audit</td>
<td>Req- F.5.1</td>
<td>Functional</td>
<td>Limiting access to data and resources based upon necessity and principle of least privilege</td>
</tr>
<tr>
<td></td>
<td>Limit access to resource over network</td>
<td>Req- F.5.2</td>
<td>Non-Functional</td>
<td>Implementing network access control policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limit hardware installation</td>
<td>Req- F.5.3</td>
<td>Functional</td>
<td>Blocking unknown devices and accessories</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use network segmentation</td>
<td>Req- F.5.4</td>
<td>Functional</td>
<td>Isolating infrastructure components that do not require broad network access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimize available info</td>
<td>Req- F.5.5</td>
<td>Non-Functional</td>
<td>Minimizing the amount and sensitivity of data available to external parties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Properly set user account policies</td>
<td>Req- F.5.6</td>
<td>Functional</td>
<td>Setting account lockout policies after a certain number of failed login attempts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use multi factor authentication</td>
<td>Req- F.5.7</td>
<td>Functional</td>
<td>Enabling multi-factor authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.5.8</td>
<td>Non-Functional</td>
<td>Guidelines for creating password policies</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>-----------</td>
<td>------------</td>
<td>--------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.2</td>
<td>Functional</td>
<td>Monitor for changes made to windows registry keys or values</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.3</td>
<td>Functional</td>
<td>Monitor executed commands and arguments that may enumerate files and directories</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.4</td>
<td>Functional</td>
<td>Monitor for API calls that may enumerate files and directories</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.5</td>
<td>Functional</td>
<td>Monitor newly executed processes that may enumerate files and directories</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.6</td>
<td>Functional</td>
<td>Monitoring and analysing traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.7</td>
<td>Functional</td>
<td>Monitoring network data for uncommon data flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.8</td>
<td>Non-Functional</td>
<td>Centralized log management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.9</td>
<td>Functional</td>
<td>SIEM (security information and event management)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.10</td>
<td>Functional</td>
<td>Active monitoring the last SOC (security operation centre) function</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.11</td>
<td>Non-Functional</td>
<td>Monthly reporting about the current status</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.12</td>
<td>Non-Functional</td>
<td>Logging policy to define the logs that need to be collected</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.6.13</td>
<td>Non-Functional</td>
<td>Define process about how to react in case of information security incidents</td>
<td></td>
</tr>
<tr>
<td>FC-F.7</td>
<td>Data backup and encryption</td>
<td>Req- F.7.1</td>
<td>Functional</td>
<td>Data backup and encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage process metadata</td>
<td>Req- F.7.2</td>
<td>Functional</td>
<td>Backup and restore testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.7.3</td>
<td>Non-Functional</td>
<td>Information classification guidance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.7.4</td>
<td>Non-Functional</td>
<td>Encryption policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Req- F.7.5</td>
<td>Non-Functional</td>
<td>Backup policy that defines all the requirements of backup (how often to take backup and how long it takes to restore)</td>
<td></td>
</tr>
</tbody>
</table>
### 2.5.2 Technical Specification

Table 11: Technical specification for the Finnish pilot

<table>
<thead>
<tr>
<th>High-Level Requirement</th>
<th>Functional Requirement</th>
<th>Derived Technical Specification</th>
<th>Available Commercial-off-the-Shelf Solutions and/or Security Functions</th>
<th>Constrain ts and Parameters</th>
<th>Related CyberSEAS Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use antivirus/anti malware</td>
<td>Automatic quarantine of suspicious files</td>
<td>Anomaly detection</td>
<td>EDR (endpoint detection and response)</td>
<td>–</td>
<td>Antivirus</td>
</tr>
<tr>
<td>Network intrusion prevention</td>
<td>Scanning and removal of malicious email attachments</td>
<td>Active monitoring</td>
<td>XDR (extended detection and response)</td>
<td>–</td>
<td>Antimalware software</td>
</tr>
<tr>
<td>Restrict web-based content software configuration</td>
<td>Signatory based detection</td>
<td>Rapid response</td>
<td>MDR (managed detection and response)</td>
<td>–</td>
<td>Antiphishing, training/knowledge awareness</td>
</tr>
<tr>
<td>Monitor network traffic content</td>
<td>File isolation capability</td>
<td>Threat analysis</td>
<td>–</td>
<td>–</td>
<td>TO4SEE (ENG)</td>
</tr>
<tr>
<td>Monitor network traffic flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IDS</td>
</tr>
</tbody>
</table>

| | | | | | Firewall |

| | | | | | Network antivirus |

| | | | | | BP-IDS (CINI) |

| | | | | | Multiple products like ServiceNow |

| Update software | Upgrading management services to the latest supported and compatible version | Configuration manager | –               | –               | Patch management tools |
| | | Software batch repository | | | MIDA (GT) |

| | | Real-time continuous assessment | – | – | |
| | | SOC | | | |
| | | Configuration control | | | |

| | | Monitoring updated list of software and their status | CMDB (configuration management database) | Multiple products like ServiceNow | – |
## D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>User account control</th>
<th>Threat intelligence News feed</th>
<th>Following active vulnerabilities related to the list of software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing accounts and permissions used by parties in trusted relationships</td>
<td>IAM (Identify and access management) PAM (privilege access management)</td>
<td>--</td>
</tr>
<tr>
<td>Restricting users and accounts to the least privileges they require</td>
<td>Logging</td>
<td>Multiple products like Microsoft Active Directory and Beyond Trust</td>
</tr>
<tr>
<td>Limiting administrator accounts from activities that may expose them to potential adversaries</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Monitoring authentication logs for succeeded and failed attempts to system and application login</td>
<td>Logging SOC</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User training</th>
<th>Continuous training for users to identify social engineering activities and spearphishing emails</th>
<th>E-learning platform Social engineering testing</th>
<th>--</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>--</td>
<td>OPENESS.edu (ENG) TO4SEE (ENG) Antiphishing Training/knowledge awareness</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit</th>
<th>Limiting access to data and resources based upon necessity and principle of least privilege</th>
<th>IAM (Identify and access management) PAM (privilege access management)</th>
<th>--</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit hardwa</td>
<td>Implementing network access control policies</td>
<td>Firewall Monitoring Alerting</td>
<td>SIEM (CINI)</td>
</tr>
<tr>
<td>re segmentatio</td>
<td>Minimizing the amount and sensitivity of data available to external parties</td>
<td>Secure data exchange protocols</td>
<td>MIDA (GT)</td>
</tr>
<tr>
<td>Minimize available info</td>
<td>Setting account lockout policies after a certain number of failed login attempts</td>
<td>SIEM (security information and event management) SOC</td>
<td>Testing lab (FRAUNHOFER)</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
<td>SQS Test Lab (SQS)</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Firewall</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
<td>VPN solutions</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
<td>DRM management tool</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
<td>IAM</td>
</tr>
<tr>
<td>Property set user account policies</td>
<td>Enabling multi-factor authentication</td>
<td>Multi-factor authentication</td>
<td>Multi-factor authentication</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Monitor driver load</td>
<td>Monitor for API calls that may enumerate files and directories</td>
<td>Firewall</td>
<td>Multiple products by different vendors</td>
</tr>
<tr>
<td>Monitor windows registry key modification</td>
<td>Monitor OS API execution</td>
<td>Centralized log management</td>
<td>Centralized log management</td>
</tr>
<tr>
<td>Monitor command execution</td>
<td>Monitor process creation</td>
<td>SIEM (security information and event management)</td>
<td>Splunk and Qradar</td>
</tr>
<tr>
<td>Monitor network traffic content</td>
<td>Active monitoring the last SOC (security operation centre) function</td>
<td>SOC</td>
<td>--</td>
</tr>
<tr>
<td>Monitor network traffic flow</td>
<td>Define process about how to react in case of information security incidents</td>
<td>SOAR</td>
<td>Multiple SOAR products like Checkpoint SOAR and PaloAlto SOAR</td>
</tr>
<tr>
<td>Monitor application log content</td>
<td>Manage process metadata</td>
<td>Data backup and encryption</td>
<td>Backup system Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multiple backup systems like VEEAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FIM – file integrity monitoring tools</td>
</tr>
</tbody>
</table>
### 2.6 Estonian Pilot

#### 2.6.1 Functional Requirements and Non-Functional Requirements

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

<table>
<thead>
<tr>
<th>Funct. Comp. ID</th>
<th>Functional Component</th>
<th>Related High-Level Requirement</th>
<th>ID of Derived Req.</th>
<th>Type of Derived Req. (Functional, Non-Functional)</th>
<th>Derived Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-E.1</td>
<td>Sabotage detection system</td>
<td>Implementation of a system to detect abnormalities in remote access traffic caused by sabotage (Sc. 1)</td>
<td>Req-E.1.1</td>
<td>Functional</td>
<td>Log management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Req-E.1.2</td>
<td>Non-Functional</td>
<td>Backup and restore functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functionality to define pre-set configurations which must be avoided (Sc. 1)</td>
<td>Req-E.1.3</td>
<td>Functional</td>
<td>Configuration management</td>
</tr>
<tr>
<td>FC-E.2</td>
<td>Physical intrusion detection</td>
<td>Implementation of a constant surveillance to substations for detecting physical intrusion to the premises (Sc. 2)</td>
<td>Req-E.2.1</td>
<td>Functional</td>
<td>Perimeter security</td>
</tr>
<tr>
<td>FC-E.3</td>
<td>Decision support system</td>
<td>Support the Control Centre Operator in managing and prioritizing alarms. (Sc. 2)</td>
<td>Req-E.3.1</td>
<td>Non-Functional</td>
<td>Well defined operational support material for control centre operator</td>
</tr>
<tr>
<td>FC-E.4</td>
<td>Version control system</td>
<td>Save, sign, and manage system configurations layer by layer (Sc. 3)</td>
<td>Req-E.4.1</td>
<td>Functional</td>
<td>Configuration management</td>
</tr>
<tr>
<td>FC-E.5</td>
<td>Administrative rights management, identity access</td>
<td>Management of identities and their access rights.</td>
<td>Req-E.5.1</td>
<td>Functional</td>
<td>User management and analyses</td>
</tr>
<tr>
<td>Task ID</td>
<td>Task Description</td>
<td>Implementation of HR processes (Sc. 3)</td>
<td>FC-E.6 Network segmentation</td>
<td>Access permissions by IP address, 2IA etc (Sc. 4)</td>
<td>Req-E.6.1 Functional</td>
</tr>
</tbody>
</table>
## FC-E.15 Precautions for protecting local area networks

Extra security layers between local area networks and substations (Sc. 10)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.15.1</td>
<td>Functional</td>
<td>Advanced network security features</td>
</tr>
</tbody>
</table>

## FC-E.16 Detection of suspicious hardware

Automated detection solutions to find unidentified devices (Sc. 11)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.16.1</td>
<td>Functional</td>
<td>Network management and monitoring</td>
</tr>
</tbody>
</table>

## FC-E.17 Multiple ways to compare configurations to reality

Layers of indicators to detect difference between configuration and actual status of substation/RTU (Sc. 12)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.17.1</td>
<td>Functional</td>
<td>Configuration immutability monitoring</td>
</tr>
</tbody>
</table>

## FC-E.18 Automated detection of social engineering

Automated detection of social engineering in substation configuration (Sc. 13)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.18.1</td>
<td>Non-functional</td>
<td>Processes and playbooks to keep order</td>
</tr>
</tbody>
</table>

## FC-E.19 Secure updating process

Automated solution for patch management and version management (Sc. 13)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.19.1</td>
<td>Functional</td>
<td>Patch management and verification</td>
</tr>
</tbody>
</table>

## FC-E.20 Enhanced security for 3rd party

Extra layers for monitoring activities of 3rd party users (Sc. 14)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.20.1</td>
<td>Functional</td>
<td>User behaviour monitoring and analysis</td>
</tr>
</tbody>
</table>

## FC-E.21 Modern physical security

Important substations must have better physical security (Sc. 15)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.21.1</td>
<td>Functional</td>
<td>Key and access card management</td>
</tr>
</tbody>
</table>

## FC-E.22 Digital monitoring of all visits in substations

All activities in substations must be recorded (Sc. 15)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.22.1</td>
<td>Functional</td>
<td>User/visitor monitoring</td>
</tr>
</tbody>
</table>

## FC-E.23 Enhanced security processes and training quality

Better processes, education, and discipline (Sc. 16)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.23.1</td>
<td>Functional</td>
<td>Cyber awareness training with ambassador programs to increase the cybersecurity culture level</td>
</tr>
</tbody>
</table>

## FC-E.24 Automated detection of suspicious configurations

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-E.24.1</td>
<td>Functional</td>
<td>Deployed configuration checks</td>
</tr>
</tbody>
</table>
2.6.2 Technical Specification

Table 13: Technical specification for the Estonian pilot

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

Page 49 of 79
<table>
<thead>
<tr>
<th>Support the control centre operator in managing and prioritizing alarms</th>
<th>Well defined operational support material for control centre operator.</th>
<th>Operations playbooks / SOP</th>
<th>Splunk, ManageEngine, SolarWinds, Check Point Incident Response</th>
<th>On-Prem solutions only</th>
<th>SIEM (CINI) CI SOC ENG's EPES solution RATING DAISY (SAPPAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save, sign, and manage system configurations layer by layer</td>
<td>Configuration management</td>
<td>Version control for configurations</td>
<td>Gitlab, Github, SVN</td>
<td>On-Prem solutions</td>
<td></td>
</tr>
<tr>
<td>Management of identities and their access rights</td>
<td>User management and analyses</td>
<td>Identity and Access Management</td>
<td>Auth0, Okta, Ping Identity</td>
<td>On-Prem solutions</td>
<td></td>
</tr>
<tr>
<td>Implementation of HR processes</td>
<td>User behaviour analysis</td>
<td>UBA</td>
<td>On-Prem solutions</td>
<td>PKI (CINI)</td>
<td></td>
</tr>
<tr>
<td>Access permissions by IP address, 2fA, etc.</td>
<td>Access control security</td>
<td>MFA</td>
<td>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</td>
<td>On-Prem solutions only</td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>Sophos, Palo Alto networks, Cisco PIX, pfSense</td>
<td></td>
<td></td>
<td>On-Prem solutions only</td>
<td></td>
</tr>
<tr>
<td>Substation configurations and management in IoT by secured Starlink connection</td>
<td>VPN</td>
<td>Secure private network</td>
<td>Resilient and secure network for substations and IoT devices</td>
<td>Use case provider (infra) specific</td>
<td>Micro segmentation</td>
</tr>
<tr>
<td>Data transfer must be prohibited, and data leaks must be monitored</td>
<td>Data security in transit</td>
<td>Data encryption and signing in transit</td>
<td>Let’s encrypt</td>
<td>Known secure algorithms only</td>
<td></td>
</tr>
<tr>
<td>Unauthorized access must be avoided, internal data must be separated from external networks</td>
<td>Network security</td>
<td>Firewall</td>
<td>Sophos, Palo Alto networks, Cisco PIX, pfSense</td>
<td>Micro segmentation</td>
<td></td>
</tr>
<tr>
<td>Maintenance of electric grid should be run by program, not incidents</td>
<td>Electrical grid maintenance</td>
<td>Maintenance plan</td>
<td>-</td>
<td>Not specified</td>
<td></td>
</tr>
<tr>
<td>Commands must be automatically validated, including time and user</td>
<td>Automatic data integrity protection and verification to verify integrity, time and signer</td>
<td>Command integrity verification</td>
<td>Guardtime’s MIDA</td>
<td>On-Prem solutions only</td>
<td></td>
</tr>
<tr>
<td>For precise timing of instructions time resolution must be as good as latency (1 ms)</td>
<td>System time synchronization for precise timing of instructions</td>
<td>Time synchronization with NTP</td>
<td>NetTime, Time-Sync, NTP syncing tools integrated in OS, GPS sync time</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
<tr>
<td>Extra security layers between local area networks and substations</td>
<td>Advanced network security features</td>
<td>Network segmentation</td>
<td>VLANs, firewall rules to restrict communication between VLANs</td>
<td>Limited access to specific segmented networks</td>
<td></td>
</tr>
</tbody>
</table>

VPN: OpenVPN, Pulse, … On-Prem solutions only.
D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Automated detection solutions to find unidentified devices</th>
<th>Network management and monitoring</th>
<th>Connected device white listing</th>
<th>Monitoring of connected devices</th>
<th>Log management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco PIX, pfSense</td>
<td>segmentated networks</td>
<td>Limited access to specific segmented networks</td>
<td>On-Prem solutions only, Limited access to specific segmented networks</td>
<td>Splunk</td>
</tr>
<tr>
<td>Micro Segmentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Security</td>
<td>Switches and routers with switchport security feature</td>
<td>Limited access to specific segmented networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>OpenVPN, Pulse, ...</td>
<td>On-Prem solutions only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated detection solutions to find unidentified devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network management and monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected device white listing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring of connected devices</td>
<td>ManageEngine OPManager, SolarWinds network performance monitor, Datadog network device monitoring</td>
<td>On-Prem solutions only, Limited access to specific segmented networks, Data confidentiality requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log management</td>
<td>Splunk</td>
<td>On-Prem solutions only, Limited access to specific segmented networks, Data confidentiality requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CINI's SIEM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

| Layers of indicators to detect difference between configuration and actual status of substation/RTU | Configuration immutability monitoring | Version control system | Switches and routers with switchport security feature, USB Block, USBGuard utility | Logging and centrally alerting on port activities | – |
| Configuration immutability monitoring | Version control system | Guardtime’s MIDA | On-Prem solutions only | Limited access to specific segmented networks | 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 | – |

| 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 |

| 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 |

| 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 |

| 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 |
### D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

<table>
<thead>
<tr>
<th>Important substations must have better physical security</th>
<th>Key and access card management</th>
<th>NFC keys</th>
<th>Latest version, updatable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>EDR and XDR solutions</td>
<td>-</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Log management</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Log management</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>EDR and XDR solutions</td>
<td>-</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Log management</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
<tr>
<td>Important substations must have better physical security</td>
<td>Key and access card management</td>
<td>NFC keys</td>
<td>Latest version, updatable</td>
</tr>
<tr>
<td>Security orchestration</td>
<td>Splunk</td>
<td>On-Prem solutions only. Limited access to specific segmented networks. Data confidentiality requirements.</td>
<td></td>
</tr>
</tbody>
</table>
**D3.2 CyberSEAS technical requirements, SELP requirements and system specifications**

<table>
<thead>
<tr>
<th>RTU’s must be detected</th>
<th>Monitoring of configuration using tamper resistant proofs</th>
<th>Guardtime’s MIDA</th>
<th>On-Prem</th>
<th>Guardtime’s MIDA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup management</td>
<td>SCADA backup</td>
<td>Offsite and offline solutions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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: $20\% \leq x < 40\%$
D3.2 CyberSEAS technical requirements, SELP requirements and system specifications

- 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:

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).
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.
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


CyberSEAS technical requirements, SELP requirements and system specifications


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

<table>
<thead>
<tr>
<th>Planned running dates</th>
<th>[start date – end date]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location / site 1</td>
<td>[address]</td>
</tr>
<tr>
<td>Location / site 2</td>
<td>[address]</td>
</tr>
<tr>
<td>Etc.</td>
<td>[address]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Lead contact person</th>
<th>[name]</th>
<th>[company]</th>
<th>[e-mail address]</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Location / site 1</th>
<th>[name]</th>
<th>[company]</th>
<th>[e-mail address]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location / site 2</td>
<td>[name]</td>
<td>[company]</td>
<td>[e-mail address]</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>General description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[free text description]</td>
</tr>
</tbody>
</table>

**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.
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

<table>
<thead>
<tr>
<th>Applicant’s Name</th>
<th>Version number of the application, and date of submission for approval</th>
<th>Applicant’s signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.9.2 Application Process and Log

<table>
<thead>
<tr>
<th>Phase</th>
<th>Date</th>
<th>Action or decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feedback from the Internal Ethics Committee (if any)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resubmission (if any)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval by the Internal Ethics Committee</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.9.3 Application Approval by the Ethics Committee

<table>
<thead>
<tr>
<th>Committee Member’s Name</th>
<th>Version number of the application, and date of approval</th>
<th>Committee Member’s signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.