



## D1.2

### Requirements report

<b>Project number:</b>	607577
<b>Project acronym:</b>	ECOSSIAN
<b>Project title:</b>	ECOSSIAN: European Control System Security Incident Analysis Network
<b>Start date of the project:</b>	1 <sup>st</sup> June, 2014
<b>Duration:</b>	36 months
<b>Programme:</b>	FP7/2007-2013
<b>Deliverable type:</b>	Report
<b>Deliverable reference number:</b>	ICT-607577 / D1.2 / 1.0
<b>Work package contributing to the deliverable:</b>	WP1
<b>Due date:</b>	February 2015 – M09
<b>Actual submission date:</b>	02 03 2015
<b>Responsible organisation:</b>	Airbus Group (EADS UK)
<b>Editor:</b>	Viktoriya Degeler
<b>Dissemination level:</b>	PU
<b>Revision:</b>	1.0
<b>Security Sensitivity Committee Review performed on:</b>	27 02 2015
<b>Comments:</b>	No

<b>Abstract:</b>	Requirements to ECOSSIAN functionalities, including: legal, technological and technical aspects, approaches to maximize efficiency of information flows and effectiveness of information exchange.
<b>Keywords:</b>	Critical Infrastructures Protection, SOC, CERT, Operational Security Processes, Security Technologies, Monitoring, Situational Awareness, Prevention, Incident Handling, Information Exchange, Secure Gateways, Energy distribution systems, Standards, ICS Security, Information Sharing



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 607577.

## **Editor**

Viktoriya Degeler (EADS UK)

## **Contributors** (ordered according to beneficiary numbers)

Christina Petschnigg, Martin Deutschmann (TEC)

Daniel Meister (EADS)

Florian Skopik, Giuseppe Settanni (AIT)

Konstantin Böttinger (FHG)

Gavin Davey, Mark Carolan (ESPION)

Mirko Sailio (VTT)

Damian Clifford (KUL)

Nicolas Barret (BRT)

Klaus Theuerkauf (IFAK)

Massimiliano Aschi (PI)

Nils Motsch, Thomas Bringewald (CCG)

Reinhard Hutter, Peter Klein (CESS)

## Executive Summary

The goal of ECOSSIAN project is to create a platform that detects, analyses and responds to security incidents and attacks on critical infrastructures, specifically in industrial control systems. The platform should operate on three interconnected levels: operator, national, EU-wide. This document describes the requirements that the ECOSSIAN system should realise in order to successfully deal with this task.

The requirements include both mandatory ones that are essential for a proof-on-concept system, and optional ones that increase the value, capabilities, or user-friendliness of the final system in production.

Chapter 1 describes the characteristics of the ECOSSIAN system. These characteristics form the basis for further requirements. The chapter also introduces the classification of requirements by type and importance.

Chapter 2 contains the list of system and architecture requirements. This includes architectural requirements for the system's construction; data requirements for the format and content of the data, processed at all three levels (operator, national, EU-wide); common operational picture, situation awareness, and visualization requirements; requirements for successful forensic investigations; integration and interoperability capabilities.

Chapter 3 lists functional requirements of the system, which ultimately formulate what the system is supposed to do. The chapter lists functional modules of the system, and explains the detailed functions that each module should have. The modules include organizational and concept requirements; threat monitoring, indication, detection and early warning; risk analysis and impact assessment; cooperation between users and organizations; response capabilities, i.e. threat mitigation, planning, incident management, decision support, and recovery; and training and exercising module.

Chapter 4 contains different non-functional requirements, which include user interface capabilities; performance metrics; security control; legal and regulatory requirements; software licensing requirements; system modelling requirements; change management and organizational requirements.

# Contents

<b>Chapter 1</b>	<b>Introduction and Service Description</b>	<b>1</b>
1.1	Characteristics of ECOSSIAN scenario	1
1.2	Types of Requirements	3
<b>Chapter 2</b>	<b>System &amp; Architecture Requirements</b>	<b>5</b>
2.1	Architectural Requirements	5
2.1.1	Description	5
2.1.2	Requirements	5
2.2	Data Requirements	6
2.2.1	Description	6
2.2.2	O-SOC	6
2.2.3	N-SOC	7
2.2.4	E-SOC	8
2.3	Common Operational Picture/SA/Visualization	10
2.3.1	Description	10
2.3.2	General	10
2.3.3	O-SOC	11
2.3.4	N-SOC	11
2.3.5	E-SOC	12
2.4	Forensics	13
2.4.1	Description	13
2.4.2	O-SOC	14
2.4.3	N-SOC	14
2.4.4	E-SOC	14
2.5	Integration and Interoperability	15
2.5.1	Description	15
2.5.2	O-SOC	16
2.5.3	N-SOC	16
2.5.4	E-SOC	16
<b>Chapter 3</b>	<b>Functional Requirements</b>	<b>17</b>
3.1	Organizational and Concept Requirements	17
3.2	Threat Monitoring, Indication, Detection and Early Warning	19
3.3	Risk Analysis and Impact Assessment	20
3.4	Cooperation between Users/User Organizations	21

3.5	Response: Threat Mitigation, Planning, Incident Management, Decision Support, Recovery .....	24
3.6	Training, Exercising and Lessons Learned .....	27
<b>Chapter 4</b>	<b>Non-Functional Requirements .....</b>	<b>28</b>
4.1	User Interface Requirements .....	28
4.1.1	Real-time Situational Awareness, Early Warning .....	28
4.1.2	Information Sharing, Collaborative Information.....	30
4.1.3	Flexibility and Personalization .....	30
4.1.4	Content Presentation, Reporting .....	32
4.1.5	Usability .....	32
4.1.6	Documentation Requirements .....	34
4.2	Performance Metrics .....	35
4.3	Security .....	38
4.3.1	Access Control.....	38
4.3.2	Cryptography requirements.....	39
4.3.3	Operations Security.....	40
4.3.4	Communications Security .....	41
4.3.5	Systems Development .....	41
4.3.6	Privacy.....	42
4.4	Legal and Regulatory Requirements.....	44
4.4.1	Threat Detection .....	44
4.4.2	Information Sharing.....	50
4.5	Software Licensing.....	54
4.5.1	Types of licenses .....	54
4.5.2	Licensing of the ECOSSIAN system .....	55
4.6	Modelling Requirements .....	56
4.6.1	Software Modelling .....	56
4.6.2	User Interface Modelling .....	59
4.6.3	Business Process Modelling .....	59
4.7	Change Management Requirements .....	60
4.8	Organisational Requirements .....	63
<b>Chapter 5</b>	<b>Conclusions.....</b>	<b>67</b>
<b>Chapter 6</b>	<b>List of Abbreviations .....</b>	<b>68</b>
<b>Chapter 7</b>	<b>Bibliography .....</b>	<b>71</b>
<b>Appendices</b>	<b>.....</b>	<b>73</b>
Appendix I.	UML Diagrams.....	73

---

Appendix II. BPMN Elements .....	80
----------------------------------	----

## List of Figures

Figure 1.1: Requirements hierarchy.....	3
Figure 4.1: UML Diagram Hierarchy .....	57
Figure A.1: UML Activity Diagram.....	73
Figure A.2: UML Class Diagram .....	74
Figure A.3: UML Communication Diagram .....	74
Figure A.4: UML Component Diagram.....	75
Figure A.5: UML Composite Structure Diagram.....	75
Figure A.6: UML Deployment Diagram .....	76
Figure A.7: UML Interaction Overview Diagram.....	76
Figure A.8: UML Object Diagram.....	77
Figure A.9: UML Package Diagram .....	77
Figure A.10: Profile Diagram .....	77
Figure A.11: UML Sequence Diagram .....	78
Figure A.12: UML State Machine Diagram .....	78
Figure A.13: UML Timing Diagram .....	79
Figure A.14: UML Use-case Diagram .....	79
Figure A.15: Notation of different events .....	80
Figure A.16: Notation of different gateways .....	82
Figure A.17: Notation of different data objects.....	82
Figure A.18: Notation of different sequence flows.....	83
Figure A.19: Notation of message flow and association.....	83
Figure A.20: Notation of pool and lane .....	83
Figure A.21: Notation of group and annotation artefacts.....	84
Figure A.22: Notation of different other elements.....	84

## List of Tables

Table 2.1: Architectural requirements .....	6
Table 2.2: Data requirements .....	10
Table 2.3: Common operational picture/SA/visualization requirements .....	13
Table 2.4: Forensics requirements .....	15
Table 2.5: Integration and Interoperability requirements .....	16
Table 3.1: Organizational and concept requirements .....	18
Table 3.2: Threat monitoring, indication and early warning requirements .....	20
Table 3.3: Risk analysis and impact assessment requirements .....	21
Table 3.4: Cooperation requirements .....	24
Table 3.5: Functional response requirements .....	26
Table 4.1: User interface requirements .....	34
Table 4.2: Performance metrics requirements .....	38
Table 4.3: Security requirements .....	44
Table 4.4: Sectorial, Cross-sectorial, pan-European requirements .....	54
Table 4.5: Licensing requirements .....	56
Table 4.6: UML Diagrams .....	58
Table 4.7: Modelling requirements .....	60
Table 4.8: Change Management requirements .....	62
Table 4.9: Security Standards and Best Practices .....	64
Table 4.10: Organizational requirements .....	66
Table A.1: Elements of Flow objects .....	80
Table A.2: Notation of different Activities .....	81



# Chapter 1 Introduction and Service Description

This document combines the requirements of the ECOSSIAN system. We start by analysing the characteristics of the system and types of the requirements in this Chapter. Then we describe system and architectural requirements in Chapter 2. We describe Functional requirements in Chapter 3, and Non-functional in Chapter 4.

## 1.1 Characteristics of ECOSSIAN scenario

When combining requirements for any product, it is important to consider, how the product is supposed to be used, what is its expected added value, what are the scenarios of its usage, etc. If this is well understood, then requirements should follow. Therefore we start our requirements document by analysing the ECOSSIAN main characteristics. Based on the ECOSSIAN Description of Work [1] and the use case scenarios as defined in Deliverable 1.5 [2], we can extract the following requirement characteristics for ECOSSIAN project that will guide further process of requirements collection:

### Event monitoring

The ECOSSIAN system is expected to monitor events. This can be done in real-time if possible. Events come from many different sources, and are different for different critical infrastructure providers. Most of events are collected by already operational systems, some of them legacy. Therefore ECOSSIAN should be able to interface with third-party systems in order to collect event information.

Received events should be processed for storage, fast on-the-fly analysis, anomaly detection and early warnings. The information should be passed further into the system for displaying to users or storing.

### Situational Awareness

ECOSSIAN system must understand the context of events that it processes; i.e. how they affect the current external situation, and how the current external situation affects them.

### Threat detection capabilities

The system should be able to identify anomalies and potential attacks as early as possible. This requires intelligence mechanisms built into event collection system.

### Alert mechanisms

The ECOSSIAN should be characterised by early warning capabilities, which means that if any anomalous activity is detected, it should be automatically assessed for the possibility to pose danger to the system. If danger is deemed to be existing and severe, these activities should be reported immediately, or as soon as possible, to human operators. Otherwise, automated actions may be taken to avoid further spread of potential attack, or to enable extended logging of strange activities for further investigation by human operators.

This capability necessitates several non-functional requirements in terms of speed and extent of initial event processing, and also requires proper alert mechanisms to be present in user interface. However, the system must avoid presenting large number of false or non-essential alerts, as these tend to become an annoyance to operators, which will reduce the usefulness of the tool. The operator should be presented only with events that require immediate actions, preferably with instructions on what actions can be taken.

### **Collaborative**

The ECOSSIAN will be operated by many different operators, which will also combine their data on national, and EU-wide levels. This requires extensive collaboration capabilities, but also necessitates careful handling of sensitive data and extra attention to proper authentication and authorisation issues. Certain level of data anonymisation may be needed before sharing sensitive data.

### **Secure storage**

The goal of the ECOSSIAN system is to be able to store information about events in a secure manner, so that it is possible to use this information later in the court of law. Therefore it requires storing events in secure manner which excludes possibilities to tamper with data, and also allows verifying the credibility and completeness of stored events.

### **Event analysis**

The system should be capable of deeper event analysis in offline mode, especially for forensics purposes. This includes such analysis as deduction of events origins, establishing on a timeline of events, identifying event interdependencies, etc. This requires intelligent analysis mechanisms that are able to work with big data volumes.

### **Report generation capabilities**

All results of event analysis and data storage are expected to be shown to human operators. As the volumes of data can be huge, the data should be aggregated and correlated before generating a report. The requirements include feature support for generating reports, data querying, data display, etc.

### **Visualizable**

Finally, the important characteristic of the ECOSSIAN system is that it should be able to show data in human-readable, easy to grasp form. This inevitably includes requirements to include tools for data visualization.

### **Compliant to privacy regulations**

ECOSSIAN deals with sensitive information. It must be ensured that only those who have authorisation to access the information will have the capability to do so. Information must be sufficiently anonymized if passed further.

## 1.2 Types of Requirements

Requirements can be split into three groups: system and architectural, functional, and non-functional, as shown in Figure 1.1.

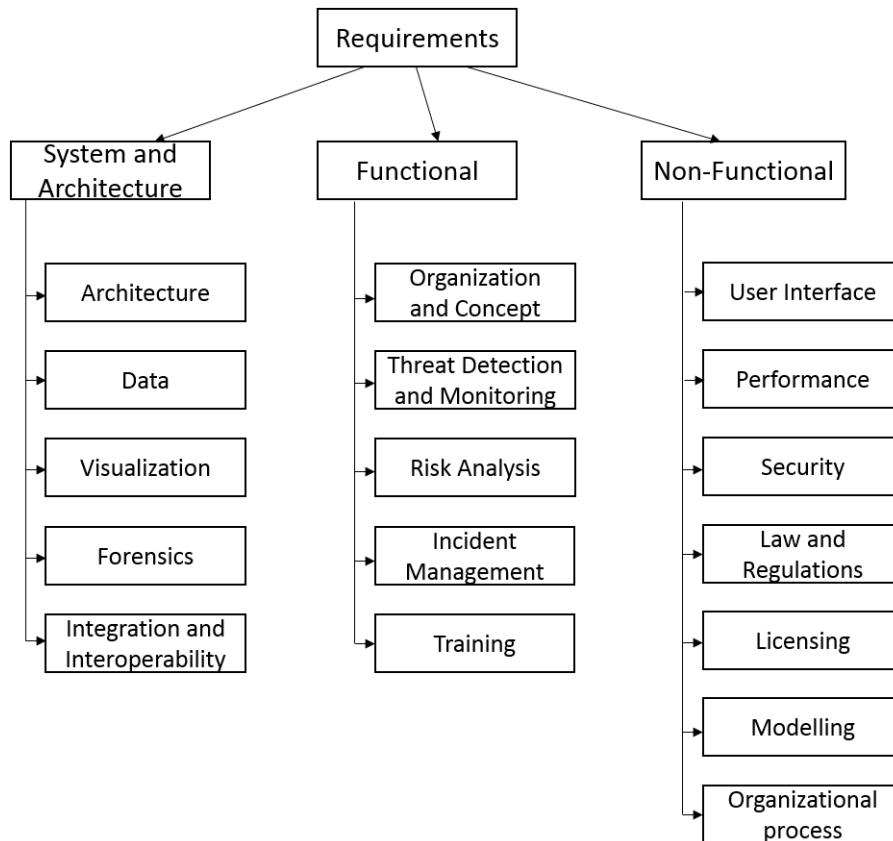


Figure 1.1: Requirements hierarchy

**System and Architecture Requirements** are established when looking at the system from inside and understanding, how the system should be built in order to successfully realise functional requirements. These requirements define, how the system should be supported, maintained, which resources should be available, etc.

**Functional requirements** are explained when answering basic questions “What a product is supposed to do?”, “What features a product should have in order to successfully solve its tasks?” Functional requirements are the most user-centric, as they are directly defined by the expected usage of the final product. As a rule of thumb, the system can be regarded as a black box when defining its functional requirements.

**Non-functional requirements** define the parameters of the system’s modules. They can be found by answering a question “What are the characteristics that a product should have in order to successfully operate and successfully deliver its features?” They also include requirements that define successful process of system’s creation and maintenance.

When speaking about requirements we should also remember that different requirements have different importance level. At the simplest level they can be split on *mandatory* and *optional* requirements.

**Mandatory requirements** are those that, if not fulfilled, render the system fully or partially unusable. They include the main features of the system, essential non-functional requirements, etc. Fulfilment of mandatory requirements is essential for the system to perform its intended tasks. Some of mandatory requirements are critical, which means that if they are unfulfilled, the system is fully unusable and cannot generate any added value. Unlike critical requirements, the system may still be able to partially operate if some of other mandatory requirements are not fulfilled, but one or more features or capabilities of the system will be disabled or unusable. Mandatory requirements are those that require fulfilment for the system to provide 100% of its intended features.

**Optional requirements** are those that provide additional features, not required by the original specifications; provide gradual improvements to the functional or non-functional parameters of the system; or provide increased quality of life for intended users of the system. The system can still be fully operational without fulfilment of optional requirements, yet in the long term performance and acceptance of the system may differ considerably depending on fulfilment of such requirements.

Note that ECOSSIAN project is expected to provide a proof-of-concept implementation. Therefore many of the optional requirements will not be fulfilled within the ECOSSIAN project, even though they may be important for the fully operational production system. Some fulfilments may deviate finally. The tables of requirements within this document state if the requirement is mandatory (M) or optional (O) for fulfilment. The tables also state, to which levels this requirement is important: operational (O-SOC), national (N-SOC), EU wide (E-SOC). Finally, the tables contain work package attribution for all requirements. This shows, which work packages within the ECOSSIAN project either depend on the fulfilment of these requirements, or are responsible for their implementation.

## Chapter 2 System & Architecture Requirements

### 2.1 Architectural Requirements

#### 2.1.1 Description

The ECOSSIAN system needs to follow certain architectural requirements in order to archive its goal while at the same time offer architectural integrity, meaning that the system itself follows a clear paradigm and structure. As the system is distributed, this is even more important, as the complexity increases exponentially with every new interface/component.

#### 2.1.2 Requirements

- The ECOSSIAN System must consist of three layers, which are Operator, National and European. On each of the layers it is assumed, that a SOC, following a CSIRT organization model, is already present.
- The components of the ECOSSIAN system should communicate using open interfaces and data formats.
- The ECOSSIAN system must offer a threat detection module, which allows the detection of cyber-attacks based on sensor (security e.g. IDS) data.
- The ECOSSIAN system must have a data sharing component, which is responsible for reliable and secure data sharing based on the sharing requirements.
- The ECOSSIAN system must have a Situational Awareness component, which allows decision makers to assess complex situations from a high-level perspective.
- The ECOSSIAN system must have a collaboration component that allows all actors participating in the system to communicate in an efficient way.
- The ECOSSIAN system should use the concept of Secure Virtual Private Community Clouds. This should allow to exchange confidential information in a secure way and at the same time minimize overhead and complexity.
- The ECOSSIAN system must be distributed across the partners and also across the different nations collaborating together operating at different geographical locations.
- The ECOSSIAN system should support the Virtual Control Center of Operation approach, allowing remote operators to collaborate similar as they would be when working in the same office.
- The ECOSSIAN system architecture should meet the requirements of all stakeholders involved, from individual, personal level up to strategic level.
- The ECOSSIAN system should offer online monitoring capabilities.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.1.1	Layered architecture with O-SOC, N-SOC and E-SOC level.	M	2,3,4,5,6	X	X	X
REQ-2.1.2	Usage of open interfaces and data formats.	O	2,3,4	X	X	X

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.1.3	ECOSSIAN must offer a Threat Detection Module (TDM).	M	2	X	X	X
REQ-2.1.4	ECOSSIAN must offer a Data Sharing functionality.	M	2,3,4	X	X	X
REQ-2.1.5	ECOSSIAN must offer a Situational Awareness functionality.	M	3	X	X	X
REQ-2.1.6	ECOSSIAN should use Secure Virtual Private Community Clouds.	O	2,3,4	X	X	X
REQ-2.1.7	The ECOSSIAN system must be distributed.	M	2,3,4	X	X	X
REQ-2.1.8	ECOSSIAN should offer a Virtual Control Center of Operation.	O	3,4	X	X	X
REQ-2.1.9	ECOSSIAN architecture must meet all stakeholders' requirements.	M	All			
REQ-2.1.10	ECOSSIAN should allow online-monitoring.	O	2,3	X		

Table 2.1: Architectural requirements

## 2.2 Data Requirements

### 2.2.1 Description

The data format and data sharing are an essential part of the ECOSSIAN system. As the data sharing is the core functionality of ECOSSIAN, appropriate data formats must be selected that allow fulfilling the data sharing requirements. The data requirements will define the necessary characteristics of the data formats so they can be used within the ECOSSIAN system.

Data sharing requirements will be defined to deal with issues, related to the sharing of data.

Interdependencies between infrastructures are considered a special case of data and data sharing, which needs to be stored and processed. The required methods are described as Interdependency Models. Requirements for those models will also be included in the data requirements.

### 2.2.2 O-SOC

- The data formats used in ECOSSIAN should be based on open standards whenever possible.
- The data formats should include all information that can be gathered with the sensors as well as additional information originating from manual analysis and additional user activities.
- The data format must support the tagging of exchanged information with national, EU and ECOSSIAN internal classifications (e.g. EU Confidential).

- The data formats should allow privacy related tagging of the information. This should support *privacy-by-design* requirements. Different types of personally identifiable information (PII) should be considered. It should be possible to add privacy related tags for all individual data fields as well as for the entire message.
- It should optionally be possible to transfer anonymized or pseudonymized data instead of raw data. The data format should allow indicating the use of data that is protected in that way.
- As a pan-European system, it should be possible to state the applicable data protection legislation (e.g. EU + German).
- The data formats must support both, human and machine readable data.
- The data formats should be able to handle information about threats, attacks, TTPs and malware related information including common Indicators of Compromise.
- The data formats must be flexible extendable to support further requirements that might evolve during the continuous improvement of the system and change of requirements.
- The data formats should be able to include operational information about the infrastructure monitored. This should explicitly include non-cyber related events like system faults or natural disasters.
- The data sharing component must ensure that all relevant information can be exchanged between the operator and the N-SOC that it is attached to. This information exchange must be bi-directional, the operator must be able to send information to the N-SOC but also receive information back from it.
- The data sharing component should allow the aggregation of information on the O-SOC layer. It should be possible to share only the aggregated information with the N-SOC instead of all information.

### 2.2.3 N-SOC

- The data formats used in ECOSSIAN should be based on open standards whenever possible.
- The data formats should include all information relevant for the N-SOC layer as well as information to be passed back to the O-SOC.
- On the N-SOC layer, the data formats should also be capable of holding the information required for interfaces with first responders in the corresponding country.
- The data format must support the tagging of exchanged information with national, EU and ECOSSIAN internal classifications (e.g. EU Confidential).
- The data formats should allow privacy related tagging of the information. This should support *privacy-by-design* requirements. Different types of personally identifiable information (PII) should be considered. It should be possible to add privacy related tags for all individual data fields as well as for the entire message.
- It should optionally be possible to transfer anonymized or pseudonymized data instead of raw data. The data format should allow indicating the use of data that is protected in that way.
- As a pan-European system, it should be possible to state the applicable data protection legislation (e.g. EU + German).
- The data formats must support both, human and machine readable data.
- The data formats should be able to handle information about threats, attacks, TTPs, malware related information including common Indicators of Compromise.
- The data formats must be flexible extendable to support further requirements that might evolve during the continuous improvement of the system and change of requirements.
- The data formats should be able to include operational information about entire infrastructure sectors of one country explicitly also related to non-cyber events.

- The data sharing component must ensure that all relevant information can be exchanged between the ECOSSIAN member organizations and agencies.
- The data sharing component should allow the aggregation of information on the N-SOC layer. It should be possible to share only the aggregated information with the E-SOC instead of all information.
- The ECOSSIAN system must have the possibility to determine dependencies and interdependencies between CI operators. The modelling of those dependencies must be possible in ECOSSIAN. The information sharing component should be able to use dynamic, automatically computed dependency and interdependency paths to allow more efficient data sharing with relevant organizations and agencies.
- The interdependency modelling should support different types of dependencies. [3]
- The modelled dependencies must be available for the ECOSSIAN system to enhance data sharing and visualization. The ECOSSIAN system must provide those information in an easy-to-use format that prescinds the complexity of the infrastructure dependencies.
- The interdependency modelling component must support the simulation of CI failures and their propagation. The interdependency simulation must also be able to simulate the result of targeted attacks on more than one CI operator at a time. On the N-SOC layer, the focus of the interdependency modelling must be on the interdependencies between the CIs of one particular country.
- The interdependency modelling should be capable of modelling inter- and intra sectoral dependencies on infrastructures as well as cross-country relationships between those operators (e.g. electricity, transport).
- The interdependency modelling method must be scalable to allow growing with the ECOSSIAN system.

#### **2.2.4 E-SOC**

- The data formats used in ECOSSIAN should be based on open standards whenever possible.
- On the E-SOC layer, the data formats must support information that is received from all N-SOCs plus the information that is transmitted back into the N-SOC systems.
- The data format must support the tagging of exchanged information with national, EU and ECOSSIAN internal classifications (e.g. EU Confidential).
- The data formats should allow privacy related tagging of the information. This should support privacy-by-design requirements. Different types of personally identifiable information (PII) should be considered. It should be possible to add privacy related tags for all individual data fields as well as for the entire message.
- It should optionally be possible to transfer anonymized or pseudonymized instead of the raw data. The data format should allow indicating the use of data that is protected in that way.
- As a pan-European system, it should be possible to state the applicable data protection legislation (e.g. EU + German).
- The data formats must support both, human and machine readable data.
- The data formats should be able to handle information about threats, attacks, TTPs and malware related information including common Indicators of Compromise.
- The data formats must be flexible extendable to support further requirements that might evolve during the continuous improvement of the system and change of requirements.
- The ECOSSIAN system must have the possibility to determine dependencies and interdependencies between CI operators. The modelling of those dependencies must be possible in ECOSSIAN. The information sharing component should be able to use



dynamic, automatically computed dependency and interdependency paths to allow more efficient data sharing with relevant organizations and agencies.

- The interdependency modelling should support different types of dependencies. [3]
- The modelled dependencies must be available for the ECOSSIAN system to enhance data sharing and visualization. The ECOSSIAN system must provide those information in an easy-to-use format that prescinds the complexity of the infrastructure dependencies.
- The interdependency modelling component must support the simulation of CI failures and their propagation. It should be possible to simulate different types of failures, both accidental and as the result of an attack. The interdependency simulation must also be able to simulate the result of targeted attacks on more than one CI operator at a time. On the E-SOC layer, the focus of the interdependency modelling must be on the effects of large-scale infrastructure failures for one country and also on cross-country effects.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.2.1	Usage of open standards wherever possible.	O	2,3,4	X	X	X
REQ-2.2.2	Coverage of all information, both originating from sensors and manual analysis.	O	2,3,4	X	X	X
REQ-2.2.3	Support tagging of information with data classifications.	O	2,3,4	X	X	X
REQ-2.2.4	Support tagging for privacy protection.	O	2,3,4	X	X	X
REQ-2.2.5	Possibility to use anonymized or pseudonymized data.	O	2,3,4	X	X	X
REQ-2.2.6	Possibility to state data protection framework.	O	2,3,4	X	X	X
REQ-2.2.7	Support machine and human readable data.	O	2,3,4	X	X	X
REQ-2.2.8	Data formats must include all relevant information categories.	M	2,3,4	X	X	X
REQ-2.2.9	Flexibility to extend data formats.	M	2,3,4	X	X	X
REQ-2.2.10	Possibility to include non-cyber information.	O	2,3,4	X	X	X
REQ-2.2.11	Must ensure all information is exchangeable between N-SOC and O-SOC in a bi-directional way.	M	2,3,4	X	X	
REQ-2.2.12	Allow aggregation of information.	M	2,3,4	X	X	X
REQ-2.2.13	Cover all Information needed between N-SOC and O-SOC.	M	2,3,4	X	X	
REQ-2.2.14	Support data exchange with national first responders.	O	4		X	

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.2.15	Data sharing of all relevant information must be possible.	M	2,3,4	X	X	X
REQ-2.2.16	Possibility to store and compute dependencies and interdependencies between CIs.	O	3,4		X	X
REQ-2.2.17	Possibility to support Cyber, Physical, Logical and Geographic dependencies.	O	3,4		X	X
REQ-2.2.18	Information about dependencies should be available in an easy-to-use format (internally).	O	3,4		X	X
REQ-2.2.19	Simulation of CI failures should be possible.	O	3,4		X	X
REQ-2.2.20	Support of inter- and intra sectoral dependencies and cross-country dependencies.	O	3,4		X	X
REQ-2.2.21	Interdependency modelling should be scalable.	O	3,4		X	X
REQ-2.2.22	Learning of interdependencies should be possible based on observations.	O	3,4		X	X

Table 2.2: Data requirements

## 2.3 Common Operational Picture/SA/Visualization

### 2.3.1 Description

The Common Operational Picture (COP) should provide enhanced Situational Awareness (SA). This component of the ECOSSIAN system will be the main interface for the N-SOC and the E-SOC layer. The component must support the SOC staff on the corresponding layers to assess the current security and safety state of the monitored infrastructure. The SA module should allow to visualize non-trivial relationships and situations that otherwise would be an information overload for the operators. The COP should allow the operators to quickly assess the state of their monitored infrastructure.

### 2.3.2 General

- The visualization component should provide different levels of visualization, depending on the ECOSSIAN layer that it is operated at. On the O-SOC layer, the focus should be on the individual organizations security status. On the N-SOC layer, the visualization should give an overview of the different sectors and their status. Relevant disruptions or potentially critical operating states should be highlighted. In case of attacks, critical dependencies between the sectors or big operators will also be pointed out, so that reactive actions can be taken. On the E-SOC layer, the visualization should mainly show the state of entire nations and sectors, with a simplified breakdown of sector per nation. For infrastructure that works cross-border or across significant parts of Europe, information should be displayed on a per-country basis, highlighting problems in one country that could have influence on the whole system.

### 2.3.3 O-SOC

- On the O-SOC layer, the visualization component must support the individual infrastructure operator with assessing the security status of his individual infrastructure. The visualization component should display a simplified set of sensor information relevant for decision making.
- On the O-SOC layer, the visualization should be simplified, allowing also persons with no deep cybersecurity knowledge to understand the criticality of an event.
- It should be possible to display the raw data sensor data used for visualization.

### 2.3.4 N-SOC

- On the N-SOC layer, the COP must provide a high-level overview of its nation states critical infrastructure. For the N-SOC operator, it must be possible to easily detect minor and major failures in all CI sectors.
- The COP must be capable of graphically visualize the status of the attached CIs.
- The COP must be dynamic and should react on changes in the CI status in a near-real-time fashion.
- The COP should use a map to graphically visualize the infrastructures. In case of failures, those must be visible on the map
- The COP component should use the Interdependency Component to compute interdependencies and visualize the results.
- The COP component must be able to receive data from different sources. Open and flexible interfaces must be defined to include such information.
- The COP should be capable of handling different situations simultaneously. For each situation, the view should be dynamically adjustable to fit the individual situation.
- The COP should support the automatic generation of reports. The report format and contents should be dynamic.
- The COP must allow analysts to detect and respond to cyber related incidents.
- The COP should only have a single user-interface that allows the analysts to use most of the systems functions.
- The COP should support decision makers in assessing complex situations
- The COP should support multi-media content. This can include graphics, data or animations.
- The COP should be able to aggregate and consolidate data that is received from various sources according to programmable rules. The aggregation and consolidation should allow the operator to view statistics about the raw data.
- The SA should assist the operator in assessing the Impact on an attack. The impact assessment should allow assessing both, the current impact and the future impact.
- The SA should support the operator in analyzing the vulnerability of the infrastructure. This should help in case of an attack to estimate possible damage and a more efficient reaction.
- The SA should allow tracking the evolution of attacks. This should help the operator to detect trends and predict future behaviour.
- The SA should help to detect the root-course of events. Whenever a critical situation is detected, the SA should help to explain the cause.
- The data of the SA must follow certain quality standards, which are trustworthiness, truthfulness, completeness and freshness.
- The SA component should support attack graphs to allow common attack patterns to be automatically analyzed.
- As data might not be completely available to the system, it must be able to deal with a certain level of uncertainty by working with probabilities.

### 2.3.5 E-SOC

- On the E-SOC layer, the COP must provide a high-level overview of all European CIs as well as all countries participating in ECOSSIAN.
- The SA component should assist the operator in assessing the impact of an attack. The impact assessment should allow assessing both, the current impact and the predicted future impact.
- The SA component should support the operator in analyzing the vulnerability of sectors or states. This should help in case of an attack to estimate possible damage and for more efficient reaction.
- The SA component should allow tracking the evolution of attacks. This should help the operator to detect trends and predict future behaviour.
- The SA component should help to detect the root-course of events. Whenever a critical situation is detected, the SA should help to explain the cause.
- The data of the SA component must follow certain quality standards, which are trustworthiness, truthfulness, completeness and freshness.
- The SA component should support attack graphs to allow common attack patterns to be automatically analyzed.
- As data might not be completely available to the system, it must be able to deal with a certain level of uncertainty by working with probabilities.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.3.1	Allowing different levels of visualization based on ECOSSIAN layer.	M	3,4	X	X	X
REQ-2.3.2	Support visualization of infrastructure status belonging to one operator.	O	3,4	X	X	
REQ-2.3.3	Situational Awareness component should support people with no deep CyberSec know-how.	O	3,4	X	X	
REQ-2.3.4	Possibility to view raw sensor data.	M	2,3,4	X		
REQ-2.3.5	Provide high-level overview of all CIs belonging to one country.	M	3		X	
REQ-2.3.6	Graphical visualization of all CIs.	M	3		X	X
REQ-2.3.7	Dynamic COP that react on changes in near-real-time.	O	3		X	X
REQ-2.3.8	Geographical visualization of CIs belonging to one country.	M	3		X	X
REQ-2.3.9	Visualize results of interdependency modelling.	O	3		X	X
REQ-2.3.10	COP must be able to receive feeds from different source.	M	2,3,4		X	X
REQ-2.3.11	Possibility to handle different situations simultaneously.	O	3		X	X
REQ-	COP must enable the automatic generation of reports.	M	3		X	X

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
2.3.12						
REQ-2.3.13	COP must support analysts with detecting and responding to cyber incidents.	M	2,3,4		X	X
REQ-2.3.14	COP should have a single user interface.	O	3		X	X
REQ-2.3.15	COP must support decision makers with assessing complex situations.	M	3		X	X
REQ-2.3.16	COP should support multi-media content.	O	3		X	X
REQ-2.3.17	COP must aggregate and consolidate data from various sources.	M	3		X	X
REQ-2.3.18	SA should support operators with impact assessment.	O	3,4		X	X
REQ-2.3.19	SA should support operator with vulnerability assessment of CIs infrastructures.	O	3		X	X
REQ-2.3.20	SA should allow tracking of attacks.	O	2,3,4		X	X
REQ-2.3.21	SA should help operators to collect information about adversaries.	O	3		X	X
REQ-2.3.22	SA should support operators finding the root-cause of incidents/events.	O	3		X	X
REQ-2.3.23	Quality standards for Situational Awareness should be followed.	O	3		X	X
REQ-2.3.24	SA should allow generating attack graphs based on common attack patterns.	O	3		X	X
REQ-2.3.25	SA should work without the need of having all information available and must deal with certain levels of uncertainty.	O	3		X	X
REQ-2.3.26	COP must provide high-level overview of all attached CI in Europe.	M	3			X
REQ-2.3.27	COP should help operators to assess vulnerabilities of entire sectors or states.	O	3			X

Table 2.3: Common operational picture/SA/visualization requirements

## 2.4 Forensics

### 2.4.1 Description

The ECOSSIAN system should support its users when conducting threat/incident response activities like forensic investigations. On the different layers of the ECOSSIAN system, the response capabilities will be very different. While on the O-SOC layer, the support offered by the ECOSSIAN system will be dealing with classical incident response (data collection, forensics, containment). On the higher levels of ECOSSIAN, the threat response module will

support nation states to deal with cyber crisis and the coordination of responses against large-scale targeted attacks including physical effects on real infrastructure. On the N-SOC layer, the response capabilities will also include interfaces to first responders in order to deal with severe attacks that have physical effects.

### 2.4.2 O-SOC

- The ECOSSIAN system should include a forensics toolset to support operators in conducting forensic investigations in case a security incident has been detected.
- The forensics module should offer of a Secure Data Storage (SDS) which allows potential evidence to be stored in a forensically sound fashion that allows the data to be used in the court of law.
- The forensics module should allow to receive network monitoring data and store that data in a reliable and forensically sound way in the SDS.
- The SDS must protect the integrity of all data stored.
- The SDS must allow data to be stored *unforgettable*, meaning no data can be deleted without noticing.
- The SDS must protect the authenticity of all data stored.
- All data stored by the SDS must be encrypted.
- The SDS should detect the discontinuity of the logging mechanism.
- The SDS should not leak information during the transmission of data.
- The SDS should not have disruptions over power cycles.
- The SDS should log all events including the state of the logging mechanism.
- The SDS must allow searching for specific events.
- The SDS should allow metadata to be stored with the actual event information for easier search and analysis.
- The forensic component must allow live memory acquisition on Industrial Control Systems components.
- The memory acquisition on devices should be possible without interruption of their operation.
- The SDS should be able to store events received from the Threat Detection Module.

### 2.4.3 N-SOC

- On the N-SOC layer, the SDS should be able to store transmitted messages in a forensically sound fashion identical to the O-SOC SDS.
- For auditing purposes, the SDS should also be able to receive logs that are generated by the ECOSSIAN system.

### 2.4.4 E-SOC

- On the E-SOC layer, the SDS should be able to store transmitted messages in a forensically sound fashion identical to the O-SOC SDS.
- For auditing purposes, the SDS should also be able to receive logs that are generated by the ECOSSIAN system.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-	A Forensics Toolset must be available within ECOSSIAN.	M	4	X	X	X

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
2.4.1						
REQ-2.4.2	Forensics toolset must have a Secure Data Storage module, which allows storing forensic evidence.	M	4	X	X	X
REQ-2.4.3	The forensic module should be able to receive network monitoring data and store it in the SDS.	O	4	X	X	X
REQ-2.4.4	The SDS must protect data integrity.	M	4	X	X	X
REQ-2.4.5	The SDS must store data unforgettable.	M	4	X	X	X
REQ-2.4.6	The SDS must protect data authenticity.	M	4	X	X	X
REQ-2.4.7	The SDS must store data encrypted.	M	4	X	X	X
REQ-2.4.8	The SDS should detect discontinuity of the logging mechanism.	O	4	X	X	X
REQ-2.4.9	The SDS should not leak any information during transmission of information.	O	4	X	X	X
REQ-2.4.10	The SDS should not have disruptions over power cycles.	O	4	X	X	X
REQ-2.4.11	The SDS should log all events including the state of the logging mechanism.	O	4	X	X	X
REQ-2.4.12	Searching must be possible in the data stored in the SDS.	M	4	X	X	X
REQ-2.4.13	It must be possible to store metadata together with the actual data in the SDS.	M	4	X	X	X
REQ-2.4.14	The forensic module should allow memory acquisition on ICS components.	O	4	X		
REQ-2.4.15	It should be possible to acquire the memory without disruption of the operation.	O	4	X		
REQ-2.4.16	The SDS must be able to store events received from the Threat Detection Module.	M	4	X	X	X
REQ-2.4.17	The SDS should also be able to store audit logs of the ECOSSIAN system itself.	O	4	X	X	X

Table 2.4: Forensics requirements

## 2.5 Integration and Interoperability

### 2.5.1 Description

The ECOSSIAN system should be able to integrate with existing solutions that may be in place already on all of the ECOSSIAN layers. Those interfaces can be for different purposes

and have different complexities. The interoperability with those systems is important, as ECOSSIAN should allow data from different sources and systems to be integrated and should allow reactions to be triggered with existing systems.

### 2.5.2 O-SOC

- On the O-SOC layer, the ECOSSIAN system should be able to integrate with existing security products, such as SIEM, IDS and Log-Management systems.
- The integration of ECOSSIAN with existing systems should be possible using open standard interfaces to bidirectional communicate with security products.
- The ECOSSIAN system should be easy to integrate into the existing operator's security landscape.

### 2.5.3 N-SOC

- On the N-SOC layer, the ECOSSIAN system should integrate with existing Situational Awareness and early warning tools. Bi-directional interfaces should be present to exchange information with those systems. The (ECOSSIAN system should just offer these interfaces for later implementation. It is not required to have interfaces for all systems implemented.)
- The ECOSSIAN system should provide interfaces with national first responders. The interface should allow triggering warnings to the relevant entities.

### 2.5.4 E-SOC

- On the E-SOC layer, the ECOSSIAN system should integrate with existing European Situational Awareness and early warning tools. Bi-directional interfaces should be present to exchange information with those systems. The ECOSSIAN system should just offer the interfaces. It is not required to have interfaces for all systems implemented.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-2.5.1	The integration with existing products should be possible using open standards and interfaces.	O	3,4,5	X	X	X
REQ-2.5.2	The ECOSSIAN system should be easy to integrate in the existing security product landscape.	O	3,4,5	X	X	X
REQ-2.5.3	The ECOSSIAN system should be able to integrate with existing national Situational Awareness and early warning tools in a bi-directional fashion.	O	3,4,5	X	X	X
REQ-2.5.4	The ECOSSIAN system should provide interfaces with national first responders.	O	3,4,5		X	
REQ-2.5.5	The ECOSSIAN system should be able to integrate with existing European Situational Awareness and early warning tools.	O	3,4,5			X

Table 2.5: Integration and Interoperability requirements



## Chapter 3 Functional Requirements

Functional requirements ultimately formulate *what* the system is supposed to do. For this chapter, the ECOSSIAN System is assumed to contain a set of interacting Functional Modules which react on or help the user to react on disturbing, disabling or destructive events in or towards CIs. Functional requirements describe the need for performing functions which are required for the world, external to the ECOSSIAN ICT system. This outside world is represented by the problems the system has to solve or support, and the end users. Main addressees are the system's operators with whom the system communicates via the user interface(s).

It should be mentioned that the ECOSSIAN system will be the product of an applied research project. Different from a commercial IT or software project, partial deviations of the final system functions from the original requirements as formulated here will occur, which may result from different causes, e.g.

- new findings during the research process
- solutions which treat the problem differently than originally assumed
- limitations in time and resources
- unexpected complications in solving a functional task
- no or limited access to proprietary systems and data which would be needed

Therefore it seems advisable not to overload the requirements document with a huge amount of nice-to-haves. So we concentrate here on requirements which appear to be fulfillable. At the end of this chapter, an early qualitative estimation is given on how the numerous functional requirements are expected to be finally fulfilled. It also indicates that requirements may be of different relevance for the 3 levels: Critical Infrastructure (CI) Operator, National, EU Here also will be requirements, which are important for a future fully operational system, however, cannot be realized or not fully realized within the ECOSSIAN project. How far requirements will finally be fulfilled will be demonstrated in the use case experiments in WP5. The evaluation criteria to be applied will be derived from and correspond to, the functional requirements formulated here and the performance metrics (Section 4.2).

The main functional requirements in Sections 3.2, 0, and 3.5 are correlated to the system development work packages WP2, WP3, and WP4, respectively, (in brief: detection, evaluation, response), with additional overarching functional requirements of the coordination and cooperation functions (Section 3.4) which are needed in all phases of a possible CI disturbance or disruption, and at all levels..

The basic architecture and components of the ECOSSIAN system are described in the DoW, and is assumed to be known.

### 3.1 Organizational and Concept Requirements

The overall requirement to the ECOSSIAN project is to design a functional command and control system for threat monitoring, detection, evaluation, mitigation and incident management. The ECOSSIAN system should be based on a generic architecture of the 3-level (or 3-tier) approach representing and serving the levels of

- Objects and processes, Industrial Control Systems and networks of certain CIs including their O-SOCs

- National SOCs
- A generic European SOC

The system needs to provide functional support in all 3 "classical" tactical areas of command and control, which are (in brief here):

- detection
- evaluation
- response

Further, so-called cross-cutting functions also need to be supported, too, including cooperation and coordination, but also to some extent training, best practices and lessons learned functions.

Security needs to be treated carefully, from a *policy* point of view: Generally in security and specifically in sensitive sectors like CIs, and on national SOC level, ECOSSIAN cannot assume that we will have access to the real operations centres or CERTS etc. and their technologies. There are often unsurpassable confidentiality restrictions, limits coming from proprietary rights, the fear of being publicly exposed, denial of interfering with or hampering of daily CI operations, or the tendency of disclosing information, e.g. by competitors or politicians. At EU level we will have to live with certain assumptions, as the role of the EU in CIP, and the rules to apply are still evolving.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-3.1.1	Functional support in all 3 "classical" tactical areas of command and control: (1) Monitoring, detection, capturing; (2) Threat and damage assessment; (3) Response and recovery.	M	1	X	X	X
REQ-3.1.2	Cross-cutting function, including cooperation and coordination, information management, best practices capturing.	M	1	X	X	X
REQ-3.1.3	A clear identification of (a) overlapping and (b) distinction of the system functionalities at the 3 levels of O-SOC, N-SOC and E-SOC.	M	1	X	X	X
REQ-3.1.4	Operation capability with simulated use cases independent from real SOCs; self-contained functionality.	O	1	X	X	
REQ-3.1.5	Simulation capabilities of and/or interfaces to external simulators and/or SOCs. Needs to be detailed during system architecture design.	O	1	X		
REQ-3.1.6	System open to different CIs and different national and international organizations: While mainly operating in the limited environment of ECOSSIAN end-users and national rules, the system needs to show no or limited amount of hard-frozen functions, be they organizational, procedural or technical.	M	1	X		

Table 3.1: Organizational and concept requirements

## 3.2 Threat Monitoring, Indication, Detection and Early Warning

Monitoring, detection, early warnings and effective information provision and handling concerning cyber-attacks to a CI component are key functions of the ECOSSIAN demonstrator as well as of any industrial system which aims at cooperation between the three levels O-SOC, N-SOC, E-SOC. The communication between the three levels comprises quick and reliable status information from the O/N-level to the N/E-level as well as information and potentially briefing/instruction in the opposite direction.

The demonstrator not only monitors the situation and indicates and detects treats but shall also extract trends (from the history) for the near future concerning certain threats and impacts.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-3.2.1	A Threat Detection Module (TDM) will at O-SOC level be developed with a user definable list of different kinds of critical (cyber) events such that the TDM is able to detect each critical event on CI level.	M	2	X		
REQ-3.2.2	Each critical event is logged with all relevant data and stored in a separate Aggregation Module (AM).	M	2	X	X	
REQ-3.2.3	The AM fetches all incoming event reports from the TDM and stores them in a central database for a given minimum time.	M	2	X		
REQ-3.2.4	AM contains a configurable set of criteria to examine and evaluate a critical event in terms of its credibility in the actual context. Examination and evaluation are based on historical data (learning system).	M	2	X		
REQ-3.2.5	The result of the evaluation is shown and reported in real time. A replay of the monitored steps of the event is possible for the operator shortly after the event has been reported.	O	2	X	X	
REQ-3.2.6	In case of a positive evaluation AM raises an optical and acoustic alarm to the operator.	O	2	X		
REQ-3.2.7	TDM monitors and stores data traffic continuously. Reporting to a definable set of users is possible at any time.	M	2	X		
REQ-3.2.8	TDM calculates, based on shortly detected critical events, a potential trend for possible future attacks (near future), concerning their frequencies and origins.	M	2	X	X	
REQ-3.2.9	TDM will contain supporting mechanisms for human operators to provide relevant incident information to N-SOC or E-SOC level.	M	2		X	X
REQ-3.2.10	TDM outcomes shall be compatible with those of the standard assessment tools.	O	2	X		
REQ-3.2.11	All monitoring and detection activities will be performed without negative impact on the control processes' performance.	M	2,4	X		

Req. #	Description	Import	WP	Relevant for		
REQ-3.2.12	A Threat Mitigation Module (TMM) will be developed which localizes the origin of critical event and the probable aim of the attack including dependent CIs and reports the result in real time.	O	2,4	X	X	
REQ-3.2.13	While managing an incident in the actual CI TMM generates early warnings to operators and adjacent CIs which might be affected as well. This shall be done throughout the cooperative network, according to the rules to be established. Alerting media shall be flexible (e.g. E-Mail, Web-Interface)	M	2	X		
REQ-3.2.14	TMM suggests and can initiate countermeasures after an attack with damages and monitors whether they are running etc. A report is produced.	O	2,4		X	X
REQ-3.2.15	A Correlation Module (CM) must be developed which can analyse the AM database in terms of correlating past and present attacks against multiple CIs.	O	2,3		X	
REQ-3.2.16	A module AACM will be developed which can detect hidden threats with fatal impacts via an analysis and combination of several but non-connected critical events.	M	2	X	X	
REQ-3.2.17	A Visualization Module (VM) will be developed which visualizes the overall security situation for the operator on a monitor including critical events, IT and other devices, interdependencies etc.	O	2,3			
REQ-3.2.18	The detection module should be able to decode and parse specific Industrial Control network protocols.	O	2			
REQ-3.2.19	The detection module should be able to compare network traffic against a protocol specification. Deviations from the specification should generate an alert.	M	2	X		
REQ-3.2.20	The detection module must be easily extendable. New attack patterns, new or attack models must be loadable in the system.	O	2	X		

Table 3.2: Threat monitoring, indication and early warning requirements

### 3.3 Risk Analysis and Impact Assessment

Risk analysis is within ECOSSIAN an analytic tool operating with data that have been collected during the daily operation (e.g. TDM, AM) and combines and interprets them in a systematic way. The analysis of risks not only refers to the frequencies and consequences of dedicated critical events but includes the assessment of complete scenarios as well; such scenarios may consist of a sequence of and distribution of events. Additionally the risk analysis shall be based on and correlated with the most critical assets and business processes affected or expected to be affected.

Whereas such a risk analysis function allows an assessment of monetary risks for the future (derived from many past events), incident management and impact assessment refer directly to a present incident and assesses and calculates financial and other types of impacts of this incident under the present conditions.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-3.3.1	An Incident Management Module (IMM) will be established which collects, analyses, categorizes evaluates AM reports and a list of CI assets and critical processes and from these information assesses the expected actual damage (impact) if an incident occurs.	M	3,4	X		
REQ-3.3.2	IMM will also take into account interdependencies with adjacent CIs.	M	3	X	X	
REQ-3.3.3	All IMM analyses and assessments performed will be stored and made available for later forensics.	M	3	X	X	
REQ-3.3.4	A Risk Assessment Module (RAM) will be established to integrate standard risk assessment tools the ECOSSIAN system	M	2	X	X	X
REQ-3.3.5	The RAM must use and evaluate data collected in the IMM, the AM, and the CM in a learning mode (from historical data).	M	2	X		
REQ-3.3.6	The RAM damage assessment will also take into account damages caused in dependent CIs.	O	2	X		

Table 3.3: Risk analysis and impact assessment requirements

## 3.4 Cooperation between Users/User Organizations

### Organizational requirements

The ECOSSIAN system needs to provide functions which facilitate cooperation and coordination between different stakeholder organizations. This will comprise "*horizontal*" cooperation, i.e. between peer organizations like different CI SOCs or between different nations, and "*vertical*" cooperation in the 3-tier hierarchy of CIs, N-SOC(s) and E-SOC. Information exchange and coordination will be in all directions, up, down and lateral. One of the most important organizational instruments will be public-private-partnership (PPP) frameworks [4].

PPPs in CIP are essential, as it must be assumed that CIs can be vital targets of deliberate attacks or accidental disablers. Vulnerabilities in CIs plus cascading effects caused by interdependencies could cause serious CI breakdowns that create disasters of catastrophic dimension, both, economically and politically. Well planned and organized, on the other hand, PPP<sup>1</sup> produces a win-win-win situation between government, industry and society, at least in principle and depending on the individual objectives, preferences, and agreements reached.

Different progress in erecting PPPs has been made European MS<sup>2</sup> but despite EPCIP and other initiatives, no common standard nor good coverage across Europe exist.

<sup>1</sup> More on the role and importance of PPP will be analysed in ECOSSIAN Task 7.3

<sup>2</sup> MS: Member States; to our knowledge, the Netherlands were one of the first to officially establish operational PPP regulations

## The C2 Cycle

A systematic generic description of requirements is given in [5].

The need for trusted information exchange and cooperation therefore is the top driver of the ECOSSIAN project. Cooperation needs to be facilitated and supported by the ECOSSIAN system horizontally as well as vertically as defined above. This requires the common development and agreement on policies and rules to be followed for information and task sharing. They must be based on a common analysis and model on mutual interdependencies of related CIs, data conventions and visualization in the Common Operational Picture (COP) adaptive to the hierarchical cooperation.

Cooperative functions need to be available for all phases of an incident cycle, monitoring, detection, alerting, assessment, response and recovery.

The functional support of cooperation and coordination should have a number of characteristics which need to be supported by the ECOSSIAN system:

- Definition of schemes on what is *sharable*. This includes criteria of confidentiality, situational criticality, relevance for the coordination process, impact assessment and expected escalation and damage forecast.
- Scale up, processing and transmission of local event information for the different SOC levels and to peer CIs.
- Provision of timely information; including real-time where necessary, depending on the threat situation.
- Means for correlation of information between different organizations to improve the overall COP and enrich the overall awareness.
- A commonly agreed joint warning, alerting and escalation scheme throughout the different SOCs and the different CIs.
- Alert handling and communication means, preferably based on existing, common standards.

## Cooperation characteristics

Good coordination schemes need to base on two-way or multi-way sharing via trusted collaborative networks for cross-organizational and cross-national information sharing. It is necessary in ECOSSIAN to assume and establish a generic organizational policy which represents a compromise between different typical organizations from member states. Shared information must be filtered and processed in a *hierarchical model* according to the needs at the different levels included. Rules for propagation in the hierarchical order need to be implemented.

But cooperation schemes are not only reactive to actual incidents an associated information sharing. They also should implement an appropriate continuity planning process in the ECOSSIAN framework and its associated O-SOCs, N-SOCs and the E-SOC, implementing an appropriate management system with people, process and technology controls, and developing cross-jurisdictional roles and responsibilities for ensuring governance over the continuity process. Also, the forensic framework should work across the various industries and SOCs.

Ultimately, it is expected that ECOSSIAN will contribute to developing Pan-European strategies to include policies, procedures and response teams' interaction and data sharing. This response interaction should be based on rules for *intelligent* shared information, resources and shared responsibilities. Intelligent meaning

- selective, depending on stakeholder role and SOC level

- reactive, depending on actual situation and forecast of threat and damage development
- flexible, to cover different scenarios and use cases, at least a selected spectrum
- supportive, providing useful decision support, e.g. recommendations to the cooperating end-users

And finally, ECOSSIAN should show that also the connectivity between EU member states and associated countries should be improved.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-3.4.1	Facilitate horizontal and vertical cooperation, i.e. e. between interdependent CIs, between different N-SOCs, and across the 3 –tier levels of O-SOCs, N-SOCS, and the E-SOC	M	4	X	X	X
REQ-3.4.2	Up, down and lateral Information exchange in this functional network will require rules for information filtering and regulated communication patterns	M	4	X	X	X
REQ-3.4.3	Applicability and support of cooperation needs to be demonstrated at all levels	M	4	X	X	X
REQ-3.4.4	Joint objectives, policies and rules (e.g. for information and task sharing, use of joint resources, respecting political restrictions etc.) need to be defined and followed	M	4	X	X	X
REQ-3.4.5	For an overarching and balanced cooperation in the defined manner, a model on mutual interdependencies of related CIs is indispensable	M	4	X	X	
REQ-3.4.6	Cooperative functions need to be available for all phases of an incident cycle, including monitoring, assessment, alerting, mitigation	O	4	X	X	X
REQ-3.4.7	Definition of schemes on what is sharable, e.g. shared responsibilities, shared resources, shared risks	M	4	X	X	X
REQ-3.4.8	A Collaboration function should be based on a common ground logic according to the requirements above. It should be scalable for the different SOC levels	M	4	X	X	X
REQ-3.4.9	A time scheme needs to be agreed which defines what timely information, at the different levels and for different event types mean, including real-time requirements where necessary	M	4	X	X	X
REQ-3.4.10	The system needs to assure that information between different organizations involved is correlated and consistent	M	4	X	X	X
REQ-3.4.11	Joint warning, alerting and escalation scheme and alert handling, joint meaning both, coordinated among different participating CIs at operational level, and across the hierarchies along an agreed alerting scheme	M	4	X	X	
REQ-3.4.12	Situational information is a complex vector of information which will be technically, procedurally, economically and/or politically relevant The system needs to filter information in a hierarchical model according to the needs at the different	M	4	X	X	X

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
	levels and roles					
REQ-3.4.13	The system needs to support continuity planning and management of cooperation between affected CIs as a support function for international cooperation	O	4	X	X	
REQ-3.4.14	The system needs to support an intelligent scheme of shared entities of information, resources and shared responsibilities. Intelligent meaning e.g. selective, supportive, flexible, reactive	M	4	X	X	X

Table 3.4: Cooperation requirements

### 3.5 Response: Threat Mitigation, Planning, Incident Management, Decision Support, Recovery

This chapter summarizes functions needed for the phase of incident response and recovery. By this functional support, system users will be enabled to generally improve the response to an incident by mitigating its causes and origins, limiting or reducing imminent or forecast/future damages. Recovery and restoration will only be briefly addressed here as it is not an ECOSSIAN system functionality offered in the DoW.

#### Criticality

The response toolkit needs to start with identifying and assessing information and information sources which are critical for reaction. The response function then needs to assess in a process model for mitigation which delivers recommendations of response measures. This model will be different on CI, national, or EU level. Criticality should regard both, the threat event and its likely development as well as the damages caused and the forecast of damage development. This information will be handed over from the evaluation modules.

The response function will be a decision support system which merges critical information with response options available giving recommendations on actions to be taken. This needs to include an analysis of the inventory of possible response measures, and mapping them against the threat and damage spectrum.

#### Forensics

Beside decision support, the ECOSSIAN system will also include a Forensics Toolset. This forensic analysis and reporting tool needs to operate at any of the O-SOC, N-SOC or E-SOC levels and needs to trace back events to their origin and to create timelines and identify gaps. It needs to correlate information from different sources relevant to for forensic analysis and conclusions. Beside forensic information logging and management, the system should give recommendations on forensic incident response.



## **Continuity planning of the ECOSSIAN system**

It is understood that continuity here means continuity of operation of the ECOSSIAN system at all levels throughout its European application scenario(s). It will mainly be an information gatherer and logger in support of (future) evidence finding in court prosecution.

The ultimate goal of this functionality is to contribute to Pan-European strategies to include policies, procedures and response teams' interaction and data sharing to ensure a minimum level of services is maintained during a disruption to the ECOSSIAN platform. Minimum levels of continuity need to be defined and maintained at all levels. Continuity standards like ISO 22301 or BS 25999 should be applied or at least regarded. Governance of this continuity process needs to be provided via an organization of defined roles and responsibilities.

## **Mitigation Measures**

Technical mitigation measures at CI level will be assumed in place in the CIs' O-SOCS. This chapter only addresses requirements for what the ECOSSIAN system could and should do above or aside these existing proprietary CI mitigation tools and measures.

From the ECOSSIAN point of view, an overall process model for mitigation at EU level is required. This will be necessary or is at least strongly advised because CIs across Europe are under different management (public, private, mixed), most operate trans-nationally and CIs may have different business models and business objectives. The main function of the mitigation module, therefore, should be a mechanism which provides a balanced assessment of the criteria of SLAs (if in place) or equivalent levels of performance of the CI systems.

The system is required to limit incident and consequences propagation by mapping CI interconnections and interdependencies and by identifying criticalities which require coordination between dependent CIs and mitigation coordination from above CI level.

The ultimate goal of this function should be to provide input to a well-balanced CIP service and supply level throughout Europe in case of disruption or degradation of the infrastructures in question. This should be supported by overarching contingency and continuity management.

Further mitigation requirements selected from the generic use cases.

ECOSSIAN needs to predict the actual aim of a distributed attack against multiple CIs. It needs to derive the actual aim of an attack based on known CI interdependencies. For that purpose, it will analyse the map of interdependencies between CIs in terms of the aim of a distributed attack and identify the most probable aim of the distributed attack, and distribute the aim throughout the system.

## **Warning**

ECOSSIAN must warn partners that employ a vulnerable component. In case of an attack targeted at a specific component, ECOSSIAN warns all participants employing the same or similar component. This should trigger the search to identify all components that are vulnerable to the attack and attack trend detected.

## **Monitor Countermeasures**

After the attack and trend has been identified, appropriate countermeasures have to be initiated, implemented and controlled whether they have been started and are running properly. Success (and failure) needs to be identified and reported.

## Summary of Functional Response Requirements

Requirements on concrete response functions summarized here are still somewhat generic. The functional focus of the ECOSSIAN system will be on monitoring, detection, analysis and assessment and on cross-sector and international coordination. The requirements mainly extracted from WP4 will be only partially implemented in the system (e.g. 3.5.10). Others will be limited to offline evaluation and messaging of information (e.g. 3.5.2, 3.5.3).

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-3.5.1	Assessment and extraction of information which are critical for reaction. based on threat and damage assessment and forecast	M	4	X		
REQ-3.5.2	A process model for mitigation which delivers recommendations of response measures.	O	4	X		
REQ-3.5.3	A decision support system which merges critical information with response options by analysis and mapping possible response measures against the threat and damage	M	4	X		
REQ-3.5.4	A forensic analysis and reporting tool operating at all levels with trace back function, creating timelines and producing recommendations on forensic incident response.	M	4	X		
REQ-3.5.5	Ensure continuity of operation of the ECOSSIAN system at all levels providing a minimum level of services; applying standards defining roles and responsibilities	M	4	X		
REQ-3.5.6	An overall process model for mitigation at EU level	O	4			X
REQ-3.5.7	A mechanism which provides a balanced assessment of the criteria of SLAs (if in place) or equivalent levels of performance of CIs	M	4	X		
REQ-3.5.8	The system is required to limit incident and consequences propagation	M	4	X		
REQ-3.5.9	Provide input to a well-balanced service and supply level of CIs throughout Europe	O	4	X	X	X
REQ-3.5.10	Identify and/or predict the aim and origin of a distributed attack and map it against interdependencies	M	4	X		
REQ-3.5.11	Warning of all participants employing the same or similar vulnerable component(s)	M	4	X		
REQ-3.5.12	Countermeasures have to be initiated, implemented and controlled; effects reported	M	4	X		

Table 3.5: Functional response requirements

### **3.6 Training, Exercising and Lessons Learned**

A training module and capability is not included is the scope of the system to be developed in ECOSSIAN.

Lessons learned and best practices will be part of the final evaluation in WP5. Measures of effectiveness (MoE) will be derived from the metrics as requested in Chapter 4.2. Along these MoEs, the proven and expected future benefits of the system will be stated and the potential for improvements be discussed.

Good practices will be evaluated in terms of ease of learning and user acceptance. The main characteristics and the outlook to future use of the system will be characterized by evaluating the system's growth potential, interoperability with legacy systems, flexibility and transferability to other CI sectors and scenarios, and adherence to standards.

An important MoE will be the potential of the ECOSSIAN system to contribute to the harmonization of CIP across Europe in the future.

Finally, the evaluation needs to explain the compliance of the ECOSSIAN system with the EU plans and policy in CIP, particularly of the EPCIP.

## Chapter 4 Non-Functional Requirements

### 4.1 User Interface Requirements

In this section we present non-functional user interface requirements. While expected features are presented in Functional Requirements chapter, this section provides information on general parameters and capabilities that the ECOSSIAN user interface should have in order to successfully operate.

While some parts of ECOSSIAN system are designed to operate autonomously, it is designed so that a user can access all parts of the system to get the information that is collected, stored, or being processed. User interaction with the system can happen in offline mode, to analyse existing data, or in online mode, to react on latest events. In this section, we describe the most important capabilities of the ECOSSIAN user interface.

#### 4.1.1 Real-time Situational Awareness, Early Warning

One of the biggest added values of ECOSSIAN project is the ability to make incident management easier and help in becoming aware of incidents faster. User interface should be designed in order to help this paradigm.

An interface for monitoring and incident response management should include:

- Alert system that provides sufficient alert level when out of ordinary behaviour is detected. This can include visual, audio signals, bringing pop-ups on screen, colour-coding alerts with red colour, requiring a user to respond to the alert before other actions can be taken, etc.
- A dashboard that provides all necessary information to identify the type of the incident, known parameters, such as affected sites, possible cause, distribution pattern, timeline, etc.

Collaboration tools to pass information about the alert and given response to other operators or to country and EU-wide level, to help preventing similar incidents on other sites.

Many use cases of ECOSSIAN involve real-time monitoring and assessing of a situation. The essential feature of real-time awareness interfaces is the ability to update information on the fly. First of all, this means that users of the system should not be required to perform any action (e.g. reload a web-page, or press the “Update” button) for the interface to update with the newly arrived information.

There are two established mechanisms for automated information update, *pull* and *push*, both having their pros and cons.

#### Pull update mechanism

Pull mechanism requires the interface application to periodically contact the information provider, i.e. a server, or a data application, and ask if there is any new information that should be shown. If there is any, the interface application downloads this information and shows it as required.

**Pros:**

- No active connection (such as a web-socket) should be kept between a data server and an interface application. A data server should have an open point of contact (for example a port that receives HTTP requests), and all interface applications contact the server via this point of contact.
- A data server knows nothing about interface applications (except information that is required for proper authentication and credentials check).
- Information can be transferred in batches, instead of transferring every new update separately.

**Cons:**

- There is a delay for an update to reach an interface application until the next polling time, which may be unacceptable for critical updates.
- If updates are very rare, pollings should still happen periodically, even if they do not transfer any new information.

**Push update mechanism**

Push mechanism requires a server, or a data application to contact an interface application whenever there is any update and send them the new information. Usually push mechanisms are realised via publish-subscribe mechanisms, i.e. an interface application contacts the server once and provides its credentials. The server now knows how to contact the application (it should have an open point of contact for this), and which information is interesting to the application. Whenever an interface application receives an update, it can immediately display it to a user.

**Pros:**

- Push update happens immediately, therefore there is no delay between receiving the new event and displaying it.
- If updates are rare, every data transfer will happen only when there is something to transfer.

**Cons:**

- A server should keep the information about all interface points.

Real-time information update may be of two types: *normal update*, i.e. the changes of the operational environment do not require a follow-up action and happen as expected, pushing the newest values to the screen; and *alert*, which corresponds to anomalous changes that require immediate user attention or any change or event that requires a follow-up action.

Alerts should happen in a way that ensures attention of a system's operator. The attention may be need to be immediate for the most severe alerts, which may require producing a corresponding alert sound, creating a pop-up with explained urgency, blocking a screen to require a user to respond to the alert before continuing, etc. Due to the nature of this type of alerts, they should usually be implemented using push mechanisms. In this way it can be ensured that alerts will reach the intended recipient as soon as they are generated.

Less severe alerts that do not constitute an immediate danger can be shown as notifications, open tasks that require resolution, etc. Updates that do not constitute any danger, but require a follow-up action, can be usually classified to this category as well. Depending on the timeframe to respond to these alerts and on the general amount of such alerts, push or pull mechanisms can be used. If the timeframe to respond to the alert is sufficiently long and the

amount of alerts is sufficiently big, pull mechanism usually works better, by polling the server from time to time, and collecting all new alerts. If the timeframe to respond is small, push mechanism may work better to avoid delays. Also, if the amount of such alerts is very small, and most of the time there will be no alerts generated when periodically polling the servers, push may work better. In this case, the server will push a new alert when necessary, so there is no need to constantly poll the server without getting any new information.

Normal updates that do not normally require any follow-up actions, usually should happen in a way that does not attract unnecessary attention, unless users themselves want to check the updated information. No particular notifications should be created for such updates. Push or pull mechanisms may both work for these type of changes, depending on the amount of changes to be transferred and the general dynamicity of an environment, i.e. how often the new information arrives.

#### **4.1.2 Information Sharing, Collaborative Information**

Another important user interface requirement follows from the functional requirement to have the ability to share information between multiple parties, i.e. operator-operator, operator-state, state-EU, etc.

Collaboration includes two or more parties that share data, responsibilities, or expertise, in order to achieve goals that would not be possible (or possible, but much harder) to achieve separately. In order to process shared information, there must be a possibility to collect it from other organizations, and draw conclusions based on it that are helpful within this particular organization. There is a high probability that data models across different organizations will have differences, due to diverse nature of events, or possible security attacks. However, in a collaborative environment it is important to find common points in data models and common security vectors to identify the information that can be interesting to other parties. This means data transfer tools should support information transformation from one data model to another, finding common data points (for example, names of the same data fields can be different across organizations, or a certain transformation is necessary, e.g. distances are stored in miles vs. kilometres, or energy is stored as power in Watts, or in Joules as power over time). In this regard, the user interface should support displaying the information that is transformed from other data sources. Such information can be incomplete, or show parameters that are uncommon for this particular organization.

User Interface should have tools that allow sending and receiving of events and alerts from other parties. Communication mechanisms between operators of different organization, such as support of video conferencing, or collaborative file access help to mobilize common efforts to repel an attack on secure infrastructures.

#### **4.1.3 Flexibility and Personalization**

The ECOSSIAN system is planned on three levels: operator level, country level, and EU-wide. This already means inevitable differences in requirements about which information should be represented on every single level, and importance of the particular information. For example, while on operator level the investigation into an incident may require to show a full timeline of all events in the system, on country level it is usually the aggregated information about events that is required. But even on the same level, operators and critical infrastructure providers will assign different importance levels to different types of information. This inevitably leads to the next user interface requirement: the flexibility in information representation to suit particular needs of a particular user, and ability to personalize the presented information.

User interface flexibility should happen on at least three levels:

## Organization level

Here “organization” also includes country level and EU-wide level. Every organization has particular needs in terms of required capabilities and information representation. For example, a railway network maintenance company may require having access to several video surveillance cameras, and therefore requires the interface that allows customizing which cameras to show, bring up the main camera, switching between cameras, switching modes of operation (real-time surveillance vs. post-incident analysis), etc. While for a gas provider company real-time video surveillance will not be of importance, but the reporting of over-time gas consumption, or real-time consumption energy spikes will be, which requires different set of interfaces.

It may be the case that some operators have third-party interfaces already available to them, therefore ECOSSIAN system may need to accommodate connection to third-party interfaces, in order to gather information for further processing within the system.

## User groups

As in many other frameworks, ECOSSIAN contains different types of users who will access the system. These users require different information and capabilities in order to perform their tasks. For example, data analysts need access to event data, and ability to aggregate, analyse and visualize it; IT security specialists need to access and modify system configuration, event monitoring parameters; law enforcers need access to metadata that can prove the integrity of data; etc. These types of users can be clustered into *user groups*, where each group has certain goals, is expected to perform certain activities, and has certain needs in terms of the information access and functionality.

Each user group requires access to different interfaces, and the system should be able to provide it. It is also possible for the same person to be a member of several user groups, therefore the user interface should be capable of combining access to several functionalities, e.g. by creating a reference to pages that the user has access to.

## Personal level

This level involves particular user operators of the system who will assess the information and make decisions based on it. Flexibility on personal level includes:

- Ability to customize homepage or personal dashboard, e.g. with different *widgets*. This especially involves ability to view together all basic information that is required for making daily decisions, and ability to send operational commands without leaving the screen with all information that those commands are based on.
- Ability to create shortcuts. Depending on navigational capabilities of the system and on range of responsibilities of a particular operator, shortcuts to different modules or pages of the system can considerably ease the complexity of daily usage.
- Look and feel of the application.

Also, such a feature as saving the current state of the application, and ability to return to this state later already provides huge benefits in term of environment personalization. The current state of the application that is to be saved can include currently open windows, current parameters for data representation, data filters, created alerts, etc.

#### 4.1.4 Content Presentation, Reporting

As with any project that deals with big amounts of data and data analysis, ECOSSIAN project relies heavily on ability of user operators to understand gathered data, analyse it, and draw correct conclusions out of it. This can be achieved by using different data dashboards.

Dashboards can be loosely split on two types, online and offline:

- **Online dashboards:** This type of dashboards allows users to monitor current state of the system, and enables real-time situational awareness. Such dashboards usually show latest values of system parameters, recent changes and trends, etc.
- **Offline dashboards:** Dashboards of this type are designed for offline analysis of data. They usually involve getting data from databases, data aggregation, querying and filtering capabilities, etc.

It is sometimes hard to estimate in advance the type of analyses that data analysts will try to perform. Therefore possibility of customization in data appearance is very important to enable richer analytics capabilities. For online dashboards it is also important to be able to combine all data that is deemed important for decision making on the same screen. Recently this is usually achieved by having a main page that supports *widgets*, i.e. smaller windows that can be combined in any order, each of which is designed to show some particular information. For offline analysis especially, when there can be hundreds of events, the ability to filter the data is indispensable, as is the ability to compare the data that comes from different sources, even if sources provide data with gaps, in different formats, etc.

Sometimes many steps should be made to allow to arrive to the cause of a certain event by looking at the consequences, or to allow correlating seemingly unrelated events. These can be made much easier by having the ability to perform complex queries on data. For example, a user may want to query “Show me all users that started working in the last two years, that have a laptop access to the energy control mechanism, and executed a certain command, and also there was a sudden energy spike event in the time window of fifteen minutes after the execution of this command”.

Finally, any big amounts of data require tools to visualize this data, so that the aggregated properties of it can be grasped at the first glance.

To summarize, these are the requirements for data representation on dashboards to enable proper analysis and decision making:

- Customization
- Filtering
- Data aggregation, e.g. a timeline of events
- Data comparison, also from different sources
- Complex querying
- Data visualization

#### 4.1.5 Usability

There are several parameters that constitute usability of the system: the ease of learning features on the fly, the ease of using the system, and the ease of avoiding errors.



## **Ease of learning**

A proper easy to learn user interface should guide its users in performing intended tasks even if users did not have a chance to do it previously or did not have formal training on these features.

This requirement can be achieved by many different things. Among them is the usage of self-describing icons on available actions; displaying of hints when moving the mouse over a possible action; context-aware menus, that show only those actions that are available at this point of time; etc.

Discoverability of features is very important to make such self-learning possible. This parameter shows how easy it is for a user to understand, how to do something they want to do, even if they did not know how to do it beforehand.

Standard conventions, such as colour-coding (green for intended actions, red for stopping an actions, etc.), usage of shapes, order, etc. are all very helpful in increasing the discoverability. This also includes consistency among displaying conventions in different parts of the system, and consistency in terminology.

It is also important to mention, that user interface should allow certain reversibility and wrong action handling. Irreversibility of actions is the single hugest factor that discourages users from discovering features by themselves.

## **Ease of use**

Unlike ease of learning, ease of use handles standard daily usage, and actions that users are performing regularly and are comfortable with. In this case the maximum speed of actions takes precedence, i.e. how fast a user can perform an action, how fast a user can switch from one activity to another, etc. This parameter, if not handled properly, can easily become a bottleneck in the system's throughput.

Among features that help to increase the speed of daily usage are:

- Fast navigation between pages and different types of actions
- Keyboard shortcuts
- Storing of recently visited places to return to them faster
- Possibility of bulk actions with multiple similar items
- Possibility to macro a set of actions to perform them with one command
- Other

## **Ease of avoiding errors**

This parameter shows how easy it is for users to realise that they perform an action that is not intended, or will lead to unintended consequences.

One of the best ways to reduce error potential of user interface actions is to have clearly defined consequence of every action, avoid assigning double or triple purposes to actions, avoid hidden changes that the user may not know about, etc.

Automated validation can be implemented to check if actions look plausible. Examples of such validation are spellchecking of text, verification of input fields (such as email, telephone number), etc.

For high-impact actions confirmation dialogs can be implemented to verify the intent of users. However, it should be noted that this can decrease the speed of performing actions, i.e. the ease of use, therefore this trade-off should be carefully considered.

Reversibility of actions is already mentioned in the ease of learning paragraph, and deserves another mention here, as irreversible actions can cause potentially devastating results for the system, if a wrong action is performed accidentally, and cannot be reversed.

#### 4.1.6 Documentation Requirements

No matter how self-describing the interface is planned to be, there will always be things that are not self-explanatory and will raise questions on how to properly use them. Therefore documentation should be available that allows users to learn interface deeper or to use the documentation as a reference to quickly answer a question a user may have about the interface usage.

Having tutorials is helpful for both new users, and experienced users who try to refresh their knowledge of particular features that they did not use much previously.

The standard feature of most modern interfaces is to use “F1” button to bring up contextual help for the current window with quick explanation of available actions.

Indexing and keyword search allow for broader feature discoverability.

Proper documentation should be able to answer on at least two types of questions:

- “How can I do something?”, in case users know what they try to do, but are unsure of how to do it. Indexing of commands, search by keywords, listing all available actions are all helpful to answer this type of questions.
- “What does this feature do?”, in case users see a possible action, but are unsure of what are the consequences of this action. Context menu that can go to a page with detailed explanation of the action can be helpful here.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.1.1	Monitoring UI must update in real-time and provide visual distinction between normal updates and anomaly alerts.	M	2	X		
REQ-4.1.2	UI should provide ability to share information between multiple parties, e.g. a mechanism to send/receive alerts to other parties	O	2	X	X	X
REQ-4.1.3	UI should be flexible and personalizable, to cater to different requirements of different organizations	O	2,3,4	X	X	X
REQ-4.1.4	UI must provide sufficient content presentation and reporting capabilities (e.g. dashboards, data querying, filtering, etc.), to support operator’s decision making	M	3	X	X	X
REQ-4.1.5	UI should be constructed to support three usability pillars: ease of learning, ease of use, ease of avoiding errors	O	3	X	X	X
REQ-4.1.6	UI should be sufficiently documented, by providing manuals, tutorials, context help (e.g. by pressing ‘F1’), indexing and keyword search.	O	2,3,4	X	X	X

Table 4.1: User interface requirements

## 4.2 Performance Metrics

Performance metrics are to measure the quality of functions performed and results/impact produced by the ECOSSIAN system. Developing performance metrics usually follows a process of

1. Establishing critical processes and/or customer requirements (in ECOSSIAN: Mainly the Use Cases)
2. Identifying specific, quantifiable outputs/results of work (The difference which the ECOSSIAN system makes when dealing with the use case)
3. Establishing targets against which results can be scored

This chapter describes the criteria against which the performance of the ECOSSIAN system could be measured [6]. Not knowing at this stage of the project how the detailed functionality of the system, its architecture and modules will be finally implemented and work, a detailed specification and quantification of the *target performance* (point 3 above) is not possible.

Therefore, here only identifications of criteria can be given which are expected to be measurable in the later phases of development, testing and demonstration.

On a macro level, e.g. from a higher business point of view, metrics could include safety, time, cost, resources, scope, quality, and actions [6]. But these would require analysis and methods of applied economics and therefore they are not adequate for a research project like ECOSSIAN. Rather, we have selected a number of metrics categories which we ultimately expect to be able to either be quantifiable or at least be described rather precisely along a number of criteria. Criteria may finally be measured quantitatively (e.g. headcounts; Euros; hours) or qualitatively (e.g. like fully – medium- marginally satisfactory, or high-medium-low). The metrics categories for the ECOSSIAN system are

- Capacity
- Availability
- Latency
- Maintainability
- Portability/Scalability
- Disaster Recovery & Business Continuity
- Monitoring
- Operations

The formulation of concrete Measures of effectiveness (MoE) and measures of performance (MoP) will build on the metrics criteria. It is part of WP5, Task 5.8 Evaluation Methodology which will start in Month 10. This work on the evaluation methodology will build on the metrics categories and criteria named here. A typical multi-criteria assessment methodology has been developed in the project ValueSec [7]. It may be modified and applied for ECOSSIAN. During this work it will also be analysed and decided, which criteria are finally valid for the ECOSSIAN system, which will be quantifiable and which will be measured only qualitatively. The following are lists of candidate metrics criteria, to be evaluated later.

### Capacity

- Number of different CIs that can be handled simultaneously.
- Number of national SOCs that can be handled in parallel.
- Number of typical end- users simultaneously working with the system.

- Complexity of scenarios which can be handled, e.g. expressible in number of simultaneous or closely related multiple attacks.
- Any quantifiable limitations in the ICT architecture, e.g. number of scenarios, variances of output results, storage and processing capacity.

### **Availability**

- MTBF and MTTR<sup>3</sup> - includes the term *Technical Reliability*
- Ease of setting up the system, manning and operation
- Possibility and degree of distributed operation
- Continuity of operation in a complex (multiple CI and 3-level-SOC) environment
- Redundancy of critical components
- Fail safe capability
- Built-in tolerances

### **Latency**

- Response time to typical incidents
- Real-time characteristics (where necessary); lead time(s)
- Time for messaging to higher echelons (National; EU)
- Fallback positions/ default rules for critical processes
- Emergency mode
- Emergency power supply
- Quality of Service (QoS)

### **Maintainability**

- Mean time to repair (MTTR)
- Use of IT-standards
- Use of COTS products
- Use of proven components
- Features for (external) diagnosis, error detection and repair
- Built-in diagnosis and repair capabilities
- Degree of automation of diagnostics and repair
- Quality of required maintenance Personnel
- Ease of diagnosis and inspection
- Remote maintenance capability

---

<sup>3</sup> Meantime between failure; meantime to repair: The classical technical definition is: Availability= MTBF/(MTBF+MTTR), which may not be adequate here.

- Patching philosophy in case of IT security incidents
- Openness and transparency of the whole architecture
- Monitoring best practices and lessons learned concerning maintenance

### **Portability/Scalability/Flexibility**

- Degree of independence form specific CI domains
- Possibility to port the system to a different ICT environment (Platforms, networks, etc.)
- Source code & object code portability
- Effort of transportation of the system to a different site/ different sites
- Effort to create a multiple-site configuration
- Effort to scale down (e.g. for a simpler SME or CI environment)
- Effort to scale up to a different or more complex CI environment
- Flexibility to integrate new organizations
- Adaptability to changing threats
- Expected effort to refine simplifications, approximations, shortcuts etc. existing in the ECOSSIAN system
- Technical reserves and limitations for extensions

### **System Recovery & Continuity**

It is assumed that we speak here about the recovery and continuity of the ECOSSIAN System operations, not of the CIs supported by the ECOSSIAN system. Some additional criteria may be:

- Continuity of operation in a complex (multiple CI and 3-level-SOC) environment
- Events of loss of control: Frequency, seriousness, etc.
- Fail-safe capacity: Automatic; Manual control
- ECOSSIAN system QoS criteria

### **Operations**

- Number of persons required to set up and operate
- Skills required to setup and operate
- Infrastructure required to set up and operate
- effort for standard monitoring operations
- Scale-up in cases of threat indications
- Scale-up in case of major attacks/disasters

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.2.1	Capacity: Numbers of organizations, users; limitations	M	2,3,4	X	X	
REQ-4.2.2	Availability: Redundancies, degree of distribution, fail safe, continuity of operations, etc.	M	2,3,4	X	X	X
REQ-4.2.3	Latency: response times, default rules, QoS.	O	2,3,4	X		
REQ-4.2.4	Maintainability: use of COTS components, diagnosis support, remote maintenance	O	2,3,4	X		
REQ-4.2.5	Portability/Scalability/Flexibility: independence from specific CI; scale-up/scale-down capability, handling of changing threats and risks	M	2,3,4	X		
REQ-4.2.6	System Recovery & Continuity QoS, automated fail safe	O	2,3,4	X	X	X
REQ-4.2.7	Operations: Setup effort, required skills, required infrastructure	M	2,3,4	X		

Table 4.2: Performance metrics requirements

## 4.3 Security

### 4.3.1 Access Control

In this section we discuss the requirements for access control in both IS and SCADA sections of the ECOSSIAN system.

#### ECOSSIAN access control

The access control requirements for ICS in this section are based on the ENISA and IEC 62443 frameworks.

#### Implementation control

An access control policy will be used, documented and reviewed based on ECOSSIAN processes and security requirements for access to the system.

- Account management and administration – Method associated with establishing, granting and revoking access accounts, maintain the permissions and privileges provided to access specific functions and resources to physical, logical assets, network resources or systems. Access accounts should be function or role based and assigned to an individual or group of individuals.
- Identification and authentication management – Identification and authentication to positively identify users, devices, hosts, applications, services and resources so they can be granted the rights associated with their accounts under administration. There are several types of authentication methods and ECOSSIAN should enforce strong authentication policies.

- Use control and authorisation – Grants access privileges to resources upon successful identification and authentication of the users account. ECOSSIAN should grant privileges based on the account configuration in the initial administration configuration setup.

### **ECOSSIAN requirements for access control**

- The objective is to control access to the ICS and protected information within the ECOSSIAN platform and its members.
- Access to ICS, data and processes should be controlled on the basis of ECOSSIAN security requirements.
- Access control rules should take into account policies for data distribution, data control and ICS authorisation.
- ECOSSIAN must use AAA (Authentication, Authorisation and Accounting) for authentication security architecture.
- ECOSSIAN must implement a policy of 'least privilege'; this is where users get the sufficient level of access and rights to perform tasks and operate the system without having too much permissions.
- ECOSSIAN must implement identity and access management.
- ECOSSIAN must enforce privilege escalation attack prevention.

### **4.3.2 Cryptography requirements**

#### **Objective**

Utilise cryptography within the ECOSSIAN platform in order to ensure the C-I-A triad (Confidentiality, Integrity and Availability) within the various systems.

#### **Implementation control**

Cryptographic controls in ECOSSIAN can help to ensure the following IS goals:

- Confidentiality (VPN)
- Integrity (digital signatures)
- Availability
- Authentication
- Non-repudiation

ECOSSIAN must define and implement a policy on the use of cryptography for the protection of all data and services.

The following criteria for cryptography usage must be considered:

- The criteria and principles for encryption within ECOSSIAN
- Implement encryption based on risk assessments and vulnerability of information
- Encrypt all data on mobile (laptop) and removable devices (USB etc.)

- Roles and responsibilities for encryption implementation and management
- Impact of encryption controls on services, e.g. anti-virus, email scanning etc.
- Legal requirements for encrypted traffic across jurisdictional boundaries

### **ECOSSIAN requirements for cryptography**

- ECOSSIAN must use link encryption between sites, e.g. site to site VPN.
- ECOSSIAN must use VPN client to gateway connections with 2FA for remote access.
- ECOSSIAN must encrypt all data held in databases. Any data kept in storage for the ECOSSIAN system should be encrypted.
- Simple hashing alone is not sufficient for the ECOSSIAN system.
- ECOSSIAN must use TLS for any web based http services.

### **4.3.3 Operations Security**

#### **Objective - Protective monitoring**

When it comes to logging and alerting for the ECOSSIAN system, the ICS and IT environment should be monitored vigorously with security maintained by administrators and security analysts.

#### **Implementation control**

Depending on what network devices, server applications and ECOSSIAN system components are deployed in the ICS environment, will dictate what configuration will be necessary by the ECOSSIAN administrators to provide log data.

Logging is tantamount to a strong security posture, capturing and monitoring accurate data in the logs is vital. Network, system and server logs are important with server and node logging providing further enhancement to specific data flow events

### **ECOSSIAN requirements for operational security**

ECOSSIAN logs should provide:

- All logging mechanisms within the ECOSSIAN system should adhere to the forensic requirements detailed in the forensic requirements policy.
- Log and track all events and actions in the ECOSSIAN system.
- Log and track all events and actions within the ECOSSIAN environment.
- ECOSSIAN must provide evidence of events in post event analysis or response management.
- ECOSSIAN must provide data for forensic analysis or legal evidence.
- ECOSSIAN should have an optional module for rule correlation across the sub SOC levels.
- ECOSSIAN must be built with logging in mind and use syslog output.
- ECOSSIAN must encrypt data at rest.



- All systems generating log data within the ECOSSIAN infrastructure should employ Network Time Protocol (NTP) in order to maintain time is synchronised with an accurate source. The time stamps on all log data events, is extremely important.

#### **4.3.4 Communications Security**

##### **Objective**

Protection of all the information and information processing systems within ECOSSIAN should be addressed in communications security.

##### **ECOSSIAN communications security requirements**

ECOSSIAN must implement controls in order to protect the network and its associated system components. ECOSSIAN must ensure the following criteria are met:

- Assign ownership and responsibility for networking equipment
- Controls implemented in order to ensure the C-I-A triad of all information and services
- Implement controls for logging and monitoring of all activity
- All systems attached to ECOSSIAN should require authorisation and access logging
- Access to the network should be restricted

For ECOSSIAN interconnection and third party access all network traffic must be:

- Authenticated, encrypted and controlled with firewalls and IDS
- Meet ECOSSIAN minimum levels of network security
- Access and services restricted to pre-defined source, destination and application port.

#### **4.3.5 Systems Development**

##### **Objective**

It is recommended that the ECOSSIAN system should be developed using the principles laid out in ISO27001.

##### **ECOSSIAN security requirements**

ECOSSIAN security control requirements as they apply to Systems Development should be analysed and specified, including web applications and transactions. Particular attention should be paid to:

- Data Encryption in transit and at rest
- Use of EU Certified secure COTS products
- Use of relevant Security Enforcing Functions (SEFs) e.g. Firewalls, Gateways, AAA, Intrusion Detection, Malware protection, File Integrity and Database Security Monitoring tools
- Extensive use and correct management of Audit Logging

## Security in ECOSSIAN development and support processes

Rules governing secure software/systems development should be defined as policy. In particular:

- Development staff background checks
- Secure development environment
- Secure coding techniques
- Any outsourced development should be controlled
- Software packages should ideally not be modified, and if they are, controlled from an ongoing support perspective
- Secure system engineering principles should be followed around Dev, Test, UAT, FAT commissioning
- System security should be tested and acceptance criteria defined to include security aspects.
- Changes to systems (both applications and operating systems) should be controlled.
- In addition to the core ECOSSIAN system security policies, assistance should be made available to member organisations dictating a *code of connectivity* covering:
  - Application development languages to be used and supported,
  - Approved (secure) operating systems

## Test data requirements

Test data should be carefully selected/generated and controlled. This includes:

- Representative Test data from member organisations who may use significant data
- Suitably obfuscated data to satisfy member country privacy laws
- Secure storage and deletion of test data

### 4.3.6 Privacy

#### Objective

ECOSSIAN must ensure privacy and protection of PIA that meets the legal requirements and of all member countries.

#### ECOSSIAN privacy and personable identifiable information (PII) requirements

ECOSSIAN PII data policy for needs to be defined and implemented from the outset, perhaps if there are differing levels of protection in the member states, then ECOSSIAN could adopt the most stringent of all legal requirements. That means the system would not require different PII policies in each country; of course, this should only be carried out if feasible and makes good business practice. This policy should be communicated with all people involved with handling PII within ECOSSIAN. If no relevant legal or regulatory guidelines exist for the information defined, then ECOSSIAN must enforce a PII protection policy to safeguard all associated PII stored or handled by the system.

ECOSSIAN must define and implement a PII protection policy which should be communicated with all agents of ECOSSIAN handling PII. Suitable management and control

processes will have to be put in place in order to ensure that ECOSSIAN complies with not only the relevant legal and regulatory privacy policies but also its own ECOSSIAN PIA policy.

ECOSSIAN should appoint a data compliance officer to oversee that the system adheres to all processes necessary and individuals' responsibilities are being met. ECOSSIAN must implement any relevant processes in technology in order to ensure compliance with data privacy.

More detail on the collating, processing and storage of PII can be found in ISO 29100, this contains a high level framework to support implementation.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.3.1	ECOSSIAN access control - Access accounts should be function or role based and assigned to an individual or group of individuals.	M	2,3,4	x	x	x
REQ-4.3.2	ECOSSIAN must implement identity and access management.	M	2,3,4	x	x	x
REQ-4.3.3	ECOSSIAN should grant privileges based on the account configuration in the initial administration configuration setup for use control and authorisation.	M	2,3	x	x	x
REQ-4.3.4	The objective is to control access to the ICS and protected information within the ECOSSIAN platform and its members.	M	2,3	x	x	x
REQ-4.3.5	Access control rules should take into account policies for data distribution, data control and ICS authorisation.	M	2,3,4	x	x	x
REQ-4.3.6	ECOSSIAN must use AAA for authentication security architecture.	M	2,3,4	x	x	x
REQ-4.3.7	ECOSSIAN must implement a policy of 'least privilege'. ECOSSIAN must enforce privilege escalation attack prevention.	M	2,3	x	x	x
REQ-4.3.8	ECOSSIAN must use link encryption between sites, e.g. site to site VPN.	M	2,3,4	x	x	x
REQ-4.3.9	ECOSSIAN must use VPN client to gateway connections with 2FA for remote access.	M	2,3,4	x	x	x
REQ-4.3.10	ECOSSIAN must encrypt all data held in databases. Any data kept in storage for the ECOSSIAN system should be encrypted.	M	2,3,4	x	x	x
REQ-4.3.11	ECOSSIAN must use TLS for any web based http services.	M	2,3,4	x	x	x
REQ-4.3.12	All logging mechanisms within the ECOSSIAN system must adhere to the forensic requirements detailed in the forensic requirements policy.	M	2,3,4	x	x	x
REQ-4.3.13	Log and track all events and actions in the ECOSSIAN system and environment.	M	2,3,4	x	x	x
REQ-4.3.14	ECOSSIAN must provide evidence of events in post event analysis or response management.	M	2,3,4	x	x	x
REQ-	ECOSSIAN must provide data for forensic analysis or legal	M	2,3	x	x	x

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
4.3.15	evidence.		4			
REQ-4.3.16	ECOSSIAN should have an optional module for rule correlation across the sub E-SOC levels.	O	2,3	x	x	x
REQ-4.3.17	ECOSSIAN must be built with logging in mind and use syslog output.	M	2,3,4	x	x	x
REQ-4.3.18	ECOSSIAN must encrypt data at rest.	M	2,3,4	x	x	x
REQ-4.3.19	All systems generating log data within the ECOSSIAN infrastructure should employ time stamps or Network Time Protocol (NTP).	M	2,3,4	x	x	x
REQ-4.3.20	All systems attached to ECOSSIAN should require authorisation and access logging.	M	2,3,4	x	x	x
REQ-4.3.21	For ECOSSIAN interconnection and third party access all network traffic must be: Authenticated, encrypted and controlled with firewalls and IDS	M	2,3,4	x	x	x
REQ-4.3.22	ECOSSIAN must enforce a personally identifiable information (PII) protection policy to safeguard all associated PIA stored or handled by the system.	M	2,3,4	x	x	x

Table 4.3: Security requirements

## 4.4 Legal and Regulatory Requirements

This section of the analysis provides a brief overview of the legal requirements analysed in detail in Deliverable 7.2 Legal Requirements. The analysis will outline the key requirements in summary form as applied to the context of ECOSSIAN. Cyber-attacks and the disruption of critical information infrastructures have become risks of significant importance [10]. One of the key objectives of ECOSSIAN is to design and develop prevention and detection tools that facilitate preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management in a privacy compliant manner.

Accordingly, in relation to the nature of the ECOSSIAN solution the legal concerns and requirements can be divided into two clear sections: concerns relating to threat detection and prevention and the privacy concerns associated with a breach (and thus the sharing of threat/breach information and other associated requirements). Accordingly the analysis will be divided as such with particular reference to the specific issues relevant to critical infrastructure protection and privacy and data protection in the given context.

### 4.4.1 Threat Detection

#### Privacy and Data Protection

At the threat detection phase it is clear that mechanisms in operation must respect the requirements provided for under the Privacy and Data Protection Framework where personal data is processed. Accordingly, the data quality principles established in Article 6 of the Data

Protection Directive<sup>4</sup> must be satisfied. In summary; fair and lawful processing, purpose specification and limitation, data minimisation, data accuracy and the principle relating to retention.<sup>5</sup> Each of these will need to be balanced in the context of the processing undertaken in ECOSSIAN and it is thus necessary to observe their importance in relation to any particular data processing which may occur in the context of threat detection. To illustrate, the purpose specification and limitation principle provides that personal data can only be collected for clear and visibly defined purpose. Accordingly, any personal data collected for threat detection cannot be later re-used for a different purpose. In relation to the data minimisation principle, the data controller (in this context the O-SOC level) should strictly restrict the gathering of personal data to that which is necessary for the purpose pursued by the processing. Thus, this prevents the indiscriminate gathering of data and the casting of an overly broad net in the analysis of a threat. Finally, the limited retention of data principle essentially provides that there is limit on the length of time personal data can be kept. More specifically it can only be kept for a period proportionate with the purposes of the collection i.e. the data can only be kept for a period that is reasonable in which the results can be achieved and the time needed for deletion. However, this does not prevent the storage of anonymised data. As such, this has clear relevance at the N-SOC, O-SOC and E-SOC levels as any storage of personal data resulting from the ECOSSIAN system must only kept for a proportionate time period. In addition, the storage of this personal data must also respect the security requirements.

According to Article 17(1) the data controller must ensure that “appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing” are implemented. This provision goes on to provide that the necessary level of data security is ascertained by:

- The state of the art in the given industry
- The costs of implementation; and
- The sensitivity of the data being processed

In order to gain a more accurate indication of the security requirements and to understand the practical implications of the state of the art requirements, one must consider the particular obligations applicable in the context of critical infrastructure protection. This issue will now be discussed in detail.

### **Security and protection of Critical Infrastructures**

The requirements imposed by the Critical Infrastructure Directive<sup>6</sup> and the Directive on attacks against information systems<sup>7</sup> are targeted towards the Member States thus requiring implementation at the national level. The framework determines that the application of cyber-security measures is largely at the discretion of the stakeholders. The responsibility for protecting European Critical Infrastructures lies with the Member States and the owners or operators.<sup>8</sup> Although the Directive only establishes obligations for Member States, certain de

---

<sup>4</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>5</sup> Article 6 Data Protection Directive

<sup>6</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 23 December 2008, L 345, 75-82.

<sup>7</sup> Directive on attacks against information systems (2013/40/EU)

*facto* requirements are established for the operators relating to ensuring the implementation of certain security measures. According to the Directive, Member States are required to:

- Ensure that European Critical Infrastructures possess and implement an operator security plan<sup>9</sup>;
- Conduct a threat assessment;
- Ensure that a security liaison officer or equivalent is designated for each ECI<sup>10</sup>;
- Appoint an ECI protection contact point.<sup>11</sup>

From these requirements it is clear that the operators have clear obligations in aiding the successful completion of each of the requirements. Despite this, the legislation does not specify any particular information security requirements in respect of critical infrastructure protection.

However, at an EU and MS level there are certain industry standards and best practice documents that have been developed and provide guidance and this practice has been encouraged by the European Commission.<sup>12</sup> In addition ENISA has repeatedly encouraged the development and sharing of best practices. In their recent report on crisis management one of the key recommendations advocated for the supporting of activities for enhanced sharing of information, best practices and the development of cyber crisis management procedures [13]. Furthermore, the proposed Directive on Network Information Security (NIS Directive)<sup>13</sup> aims to foster the prevention and resilience of the information systems by expressly stating that Member States shall “*Encourage the use of standards and/or specifications relevant to networks and information security*”. Under the proposed NIS Directive, Member States have several key obligations and from these certain *de facto* requirements emerge for the operators of critical infrastructures.<sup>14</sup> Of particular relevance to our current discussion on security and threat detection is Article 14(1) which states that:

*Market operators must “take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.”<sup>15</sup>*

Therefore, operators are required to implement such measures in order to ensure the security of the critical infrastructure and in the context of ECOSSIAN it is required that the systems are proportionate and in line with accepted state of the art. Similar to the privacy

---

<sup>8</sup> Recital 6 Directive 2008/114/CE.

<sup>9</sup> The operator security plan (‘OSP’) procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II. Article 5 and Annex II Directive 2008/114/CE.

<sup>10</sup> The officer serves as the contact point between the owner/operator of the ECI and the Member State authority concerned. The purpose is to allow for the exchange of information regarding the risks and threats relating to the ECI.

<sup>11</sup> Article 10. Directive 2008/114/CE.

<sup>12</sup> With the objective to promote a single market for cyber-security products in the EU - through the document ‘*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*’.

<sup>13</sup> Directive Of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union; Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD)

<sup>14</sup> Article 2 (8)

<sup>15</sup> Article 14 (1)

and data protection framework, the Critical Infrastructure Protection Framework leaves the specific choices up to the operator. However, it is significant to note that, from a data protection and privacy perspective, ECOSSIAN aims to implement a solution that is based on the notion of privacy by design and default. The principle is referred to in the draft Data Protection Regulation and will come into force if adopted.<sup>16</sup> However, the implementation of measures complying with this principle is also a key objective of ECOSSIAN and must therefore be given particular attention. The aim of privacy by design is to “*protect privacy by embedding it into the design specifications of information technologies, accountable business practices, and network infrastructures, right from the outset.* [11]” Therefore, privacy is part of the system and integrated in a way which does not result in a loss of functionality [12]. In order for a true implementation of this principle the privacy requirements need to be considered at the very outset. In this regard one must thus conclude that the existence of privacy enhancing technology concepts or implementations are insufficient as privacy cannot be guaranteed by technology alone especially if this technology merely consists of a few components embedded in a larger ICT system [13]. As such our attention must turn the practical application of the principle of privacy by design to the protection of critical infrastructures.

### General objectives for Privacy by Design

However, before delving into the practical issues it is important to note the seven general objectives highlighted by the Article 29 Working Party as important when deciding on the design of a processing system, its acquisition and the running of such a system:

- **Data Minimisation:** data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- **Controllability:** an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
- **Transparency:** both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
- **User Friendly Systems:** privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- **Data Confidentiality:** it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
- **Data Quality:** data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- **Use Limitation:** IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

---

<sup>16</sup> See Article 23 of the proposed Regulation

The implementation of accountability under Article 22 of the proposed Data Protection Regulation<sup>17</sup> as further enhances the privacy by design principle. Indeed if the proposal is adopted operators will be required to adopt policies and implement *appropriate measures* to ensure and be able to demonstrate compliance with data protection rules (Article 22). In this regard, the draft provisions proposes the following minimum measures:

- Keeping documentation of all processing operations (Article 28).
- Implementing data security requirements (Article 30).
- Performing data protection impact assessments (Article 33).
- Complying with requirements for prior authorisation or consultation of the supervisory authority wherever relevant (Article 34(1) and (2)).
- Appoint a Data Protection Officer (Article 35(1)).

Having considered the general legal requirements our attention must now turn to a practical application of their consequences in the context of critical infrastructure protection and ECOSSIAN.

### **ECOSSIAN – Threat detection requirements**

In the context of the threat detection and security aspects of ECOSSIAN the implementation of certain practical features should be considered. In an analysis of the application of these objectives and the principle of privacy by design Hoepman developed 8 privacy design strategies and distinguishes between data orientated strategies and process orientated strategies [14]. These are as follows:

#### Data Oriented Strategies

1. Minimise: Only the minimum amount of personal data should be collected. A common designs that implement this are the 'select before you collect' [15].
2. Hide: Personal data and their interrelationships should be hidden from plain view thereby reducing the risk of abuse (an example of such an identifier would be an IP address). There are a variety of means of implementing this strategy namely: the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation or techniques to unlink the relationship between related events.
3. Separate: The processing of the personal data should be in a distributed fashion, this would prevent the completion of full profiles of individuals. However, currently no design patterns for this strategy are known.
4. Aggregate: The highest level of aggregation should be used including the least amount of detail as this will restrict the amount of personal data that remains. For instance examples of such technologies include dynamic location granularity, *k*-anonymity [16] and other anonymisation techniques.

#### Process Oriented Strategies

1. Inform: This corresponds to the principle of transparency and the requirement to inform the data subject of the processing. Data breach notification processes are a design pattern in this regard.
2. Control: This states that data subjects should have agency over their personal data however given the nature and aims of ECOSSIAN this may not be practical in certain contexts.
3. Enforce: A privacy policy should be available and enforced.

---

<sup>17</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)



4. Demonstrate: This is in order to show compliance with the privacy policy and the legal requirements, for example this could be achieved through auditing.

However, one must consider how these strategic recommendations could be achieved in practical terms for the ECOSSIAN system. ENISA in their recent report on the implementation of the privacy and data protection by design highlight certain privacy techniques which should be examined [13]. Of particular significance to the threat detection privacy considerations are ENISA's recommendations on privacy in databases, storage privacy, and privacy preserving computations. The report splits database privacy in three: Respondent privacy (preventing the re-identification of the respondents), Owner Privacy (this relates to two or more autonomous entities being able to compute queries across their databases) and User Privacy (guaranteeing the privacy of queries to interactive databases to prevent profiling and re-identification).

As the first of these relates more the disclosure of data to third parties like the general public its impact is perhaps not as high in relation to ECOSSIAN. Regarding owner privacy this may have applicability if the O-SOC, N-SOC and E-SOC databases are shared. ENISA highlights the importance of privacy-preserving data mining and its benefits for data and knowledge hiding and such technologies should be examined in the context of ECOSSIAN [13]. In relation to user privacy solutions the issues surround private information retrieval are mainly based on cryptography. ENISA's recommendation in relation to storage privacy are of clear significance as a major challenge in implementation is to prevent unauthorised access [13]. Given that the ECOSSIAN solution will be connected to a network localised storage is out of the question. The report outlines the following storage mechanisms for consideration: local encrypted storage, format preserving encryption, stenographic storage and secure remote storage. Regarding privacy-preserving computations ENISA analyses the benefits of homomorphic encryption and secure multi-party computation. These recommendations should be considered in the assessment of the appropriate implementation of ECOSSIAN and the evaluation of the state of the art [13].

In applying these strategies certain requirements can be ascertained. These could involve the following:

- Privacy should proactive and not reactive and thus should be implemented as a default setting embedded into the design. This could involve the implementation of an automated anonymisation process.
- The security of the personal data should be protected throughout the data lifecycle and this could involve encryption and also the coordination of Privacy Impact Assessments.
- Encryption should be employed throughout with the default state of data being unreadable if there is a data leak. This encryption should be applied automatically.
- Access to the personal data should be on a need-to-know basis only and should be restricted to specific employees. This could be achieved through authentication protocols with privacy features such as the Just Fast Keying protocol.
- The Creation of measures (technological, policy and procedural) which bar the linking of personal data thereby respected the data minimisation and purpose limitation principles by default and design. This should especially be observed the use of analytics and personal data should only be used where necessary.
- All personal data should be securely disposed of at the end of its life-cycle in compliance with the limited retention of data principle. This should leave no trace of personal data in order for the process to be truly complete and compliant with the legal requirements relating to personal data retention and minimisation principles.

Having now analysed the threat detection and security requirements in the context of ECOSSIAN it is now necessary to analyse the information sharing processing and the

associated requirements following an attack in addition to the more general notification requirements.

#### **4.4.2 Information Sharing**

In essence, in the context of ECOSSIAN information sharing is divided into two: the positive notification requirements as imposed by law and the requirements associated with the sharing functionality to be implemented as part of the project. Despite the increasing importance of the digital economy and the smooth running of critical infrastructures for the overall benefit of society, small cyber incidents are rarely reported and often go undetected. As noted in an ENISA document on Incident Reporting this lack of transparency is effectively counter-productive as it makes it more difficult for policy makers to truly appreciate the scale of the problem and the potential associated threat [17]. Nevertheless, currently there is only a positive duty to inform authorities of breaches in certain clearly defined situations.

However, the EU legislator has seen the need for change in this regard and certain key proposals aimed at bridging this notification requirement gap. These measures focus on breach/incident notification as opposed to incident response. Incident response includes the plans and activities taken to eliminate the cause or source of an infrastructure event. As noted by ENISA, as “it comes after the fact, assesses the total impact; identifies root causes; documents the actions taken; and describes lessons learned” and is therefore of more value to mitigating the effects of an attack as it allows for the sharing of valuable information to the relevant interested parties [17]. As such the general requirements as provided by legislation for the two types of information sharing relevant for ECOSSIAN highlighted above will be outlined and will then be practical applied to the project.

#### **Notification - Sharing Requirements**

Currently in the context of data protection and privacy, notification requirements are restricted in application to the Communications sector with both the E-Privacy Directive<sup>18</sup> and the recent Data Breach Notification Regulation<sup>19</sup> providing such obligations and the provision of a communications network or service to the public.<sup>20</sup> However, as the operations in ECOSSIAN remain outside the scope of their application (i.e. ECOSSIAN is neither a public communications network nor a service provider) these requirements have no effect. Aside from this, at a national level there are a certain number of best practice guidelines in operation vis-à-vis breach notification but at a legislative level there are no currently no general requirements to notify.

The Critical Infrastructure Protection Directive does lay down some positive requirements with regard to notification for Member States which may have applicability, namely to:

- Identify potential ECIs<sup>21</sup> and inform the Commission and the owner/operator<sup>22</sup> and the Member states (which may be significantly affected by a potential ECI) about its identity and the reasons for designating it as a potential ECI;

---

<sup>18</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

<sup>19</sup> COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

<sup>20</sup> See E-Privacy Directive Article 4(2) and 7(3) (in addition to the Clarification provided in Regulation No. 611/2013) and the Framework Directive Article 13a.

<sup>21</sup> According to Article 4.6, the identification and designation process of ECIs should have been completed by 12 January 2011, and reviewed on a regular basis. Directive 2008/114/CE.

- Participate in bi/multilateral discussion with other potentially affected MSs when identifying a potential European Critical Infrastructure<sup>23</sup>;
- Provide a report every two years to the Commission including generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which there is an identified and designated ECI<sup>24</sup>;

Aside from this, there are some proposed changes that need to be considered. The draft Data Protection Regulation proposes the introduction of an obligation to notify personal breaches in Articles 31 and 32. This establishes the requirement that personal data breaches must be notified to the relevant parties “without undue delay”. Given the increased frequency of data breaches this is one of the least controversial reforms in the proposal. The requirement is further reflected in the proposed Police and Criminal Justice Data Protection Directive.<sup>25</sup> Also of note in this regard is the specific notification requirements seen in the draft Network and Information Security Directive. As all of these legislative reforms are likely to be implemented during the lifecycle of the project it is important to weigh their impact accordingly. Some of the specific requirements as provided for by the NIS Directive are for Member States are as follows:

- to adopt a national network and information security (NIS) strategy defining the objectives and the policy and regulatory measures necessary to achieve and maintain a high level of NIS;<sup>26</sup>
- to designate a national competent authority responsible for monitoring the application of the Directive at a national level;<sup>27</sup>
- to establish a Computer Emergency Response Team (CERT) to handle incidents and risks;<sup>28</sup>
- And to cooperate within a network that enables secure and effective coordination (including coordinated information exchange, detection and response at an EU level).

Through this network, Member States should exchange information and cooperate to counter NIS threats and incidents on the basis of the European NIS cooperation plan. From these requirements certain de facto requirements can be extrapolated for the operators of the Critical Infrastructures:

- Market operators must notify to the competent authority incidents having a significant impact on the security of the core services they provide.<sup>29</sup>
- Market operators must: “(a) provide information needed to assess the security of their networks and information systems, including documented security policies; (b)

---

<sup>22</sup> Article 4 Directive 2008/114/CE.

<sup>23</sup> Article 4 Directive 2008/114/CE.

<sup>24</sup> Article 7 Directive 2008/114/CE.

<sup>25</sup> Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

<sup>26</sup> The strategy should include *inter alia* the following matters: (i) a definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis; (ii) a governance framework to achieve the strategy, including a definition of the roles and responsibilities of the public bodies and relevant agents; (iii) the identification of the measures on preparedness, response and recovery, including cooperation mechanisms between public and private sectors. The national NIS strategy shall include a national NIS cooperation plan. Both, the strategy and the cooperation plan shall be communicated to the Commission

<sup>27</sup> Article 6 and 15.

<sup>28</sup> Article 7 - The requirements and tasks of the CERT are included in Annex I of the proposal.

<sup>29</sup> Article 14(2)

undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.”

Accordingly regarding cyber-security, the NIS Directive establishes that market operators will have to provide the necessary information for assessing the security of their networks and information systems, including documented security policies. They also have an obligation to undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.

Therefore, as the notification of security and personal data breaches are likely to become part of the legal framework during the project lifecycle it is important to consider sharing functionalities within the design of the ECOSSIAN solution. A reporting mechanism that respects the privacy and data protection concerns is key. This is discussed further through the lens of privacy by design in the final section.

### **ECOSSIAN's Sharing Functionality**

As noted *supra* there are clear requirements for the processing of personal data under the Privacy and Data Protection Framework. Given that ECOSSIAN aims to share information one must also consider the effect of these requirements if it involves personal data. However, as the transfers in question are due to occur within the EU, restrictions or prohibitions on the free flow of data between Member States for data protection reasons are prohibited by Article 1(2) of the Data Protection Directive. Moreover, the complex debates surrounding transfers to third party countries does not come within the scope of the project. Nevertheless, there are still positive requirements for at the O-SOC, N-SOC and E-SOC level. Similar to the above the data protection principles and grounds for processing must be satisfied. The additional concerns relate predominantly to the security of the processing itself and the requirements provided for under Article 17(1). These requirements are further supplemented by the obligation for confidentiality as found in Article 16 of the Data Protection Directive, which concerns any controller processor relationship. Accordingly, in addition to the security requirements discussed *supra*, the confidentiality requirement extends to the N-SOC and E-SOC levels in addition to any third party processor that may be involved. However, these are rather legalistic concepts and the practical solution for the project must consider the implementation of a sharing functionality that respects the privacy by design model. Thus the effective security measures must once again consider the state of the art regarding the security of communications and the implementation of any such functionality in a manner respecting the privacy by design principle.

### **Impact of data sharing on ECOSSIAN**

From a practical perspective, in the context of ECOSSIAN one must consider certain key issues regarding the security of communications and the state of the art in this regard. As both the positive notification requirements and the ECOSSIAN's sharing functionality will both have to guarantee the secure transfer of data it is important to consider this issue.

In relation to communications ENISA makes certain recommendations vis-à-vis the implementation of secure private communications and highlights basic encryption models such as Transport Layer Security protocol as well as the Secure Shell protocol [13]. It is also certain end-to-end encryption technologies such as The Pretty Good Privacy software which would be capable of protecting messaging [13]. In relation to the protection of the meta-data left exposed by end-to-end encryption certain anonymous communications are also highlighted by ENISA namely: single proxies and VPNs, Onion Routing, Mix-networks and Broadcast schemes [13]. Thus it is key for the purpose of ECOSSIAN that the following operation requirements are implemented in order to guarantee a privacy by design implementation:

- All communications should be encrypted in line with the above discussion.
- Personal data are only transmitted as frequently as necessary for the system to operate and any such transfer should be encrypted and anonymised (if it does not detract from the purpose).
- Systems should be designed to ensure that even where personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered out or removed.
- Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being performed.

In the practical application of these requirements it must be understood that they should be assessed as each particular level (i.e. to the relevant authority or within the O-SOC, N-SOC and E-SOC levels). In addition in relation to internal transfers, given the nature of the data flow each O-SOC, N-SOC and the E-SOC should consider filtering at each stage both in the flow of the information up the chain to the E-SOC and the distribution back out to the relevant N-SOCs and O-SOCs. This would ensure that only the relevant parties receive the information without any superfluous personal data. In the implementation of a sharing functionality the creation of a sharing mechanism capable of filtering and selecting recipients of the data would be beneficial.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.4.1	Only the minimum amount of personal data must be collected. The highest level of aggregation must be used including the least amount of detail as this will restrict the amount of personal data that remains.	M	2,3	X	X	X
REQ-4.4.2	Personal data and their interrelationships should be hidden from plain view. There are a variety of means of implementing this strategy namely: the encryption of data, the use of mix networks to hide traffic patterns, the use of anonymisation or techniques to unlink the relationship between related events.	O	2,3	X	X	X
REQ-4.4.3	The processing of the personal data should be in a distributed fashion to prevent the completion of full profiles of individuals. Currently no design patterns for this strategy are known.	O	2,3	X	X	X
REQ-4.4.4	Authentication protocols with privacy features must be implemented.	M	2,3,4	X	X	X
REQ-4.4.5	The security of the personal data must be protected throughout the data lifecycle. Encryption must be employed throughout with the default state of data being unreadable if there is a data leak.	M	1	X	X	X
REQ-4.4.6	Personal data must be securely disposed of at the end of its life-cycle or anonymised in compliance with the limited retention and data minimisation principles.	M	1	X	X	X
REQ-4.4.7	All communications must be encrypted.	M	3	X	X	X
REQ-	Systems must be designed to ensure that even where	M	3	X	X	X

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
4.4.8	personal data are transmitted, any data elements which are not necessary to fulfil the purpose of the transmission are filtered out or removed.					
REQ-4.4.9	Systems should be designed so as to allow access to the transferred personal data only to the extent necessary for the role being performed.	O	3	X	X	X

Table 4.4: Sectorial, Cross-sectorial, pan-European requirements

## 4.5 Software Licensing

As software licenses are legal instruments that state the terms of how software can be installed, used and distributed it is vital to think of requirements people must fulfil in order to be eligible to install certain software and to agree on the type of license under which the software can be used and distributed. Another important aspect in terms of software licenses is the license agreement. Without those agreements software owners may remain vulnerable to certain scenarios like legal claims due to the fact that users do not realize which limitations the owners are trying to enforce [9].

The aim of software licensing is on the one hand to ensure that consumers can use certain software products without hindrance but on the other hand software publishers should not lose their rights on the developed software. These can impose two conflicting requirements on licenses therefore it is wise to choose the type of software license carefully as different licenses basically safeguard different interests.

### 4.5.1 Types of licenses

The licence terms strongly depend on the type of software licence. There are three main types:

- Proprietary licenses
- Free and open source licenses
- Hybrid and Multi-Licensed Software

The choice of the licence type mainly depends on the nature of the software and the software publisher. Possible parameter to determine the appropriate form of licensing may include whether the software is intended to be used for commercial purposes, whether user should be able to update the software themselves, etc.

#### Proprietary Licenses

The aim of proprietary licenses is to protect the intellectual property of software while providing its functionality to users. This form of licensing is quite restrictive as the ownership and the source code of the software remain with the software publisher. In most cases even the examination of the source code is forbidden for users. For this reason, providers often offer support services for their software as customers are not able to update the software by

any means. In addition, these licenses usually contain a number of restrictions e.g. a restriction on installations allowed through activation or copy protection. Further, the end-user must agree to use the software only for its stated purpose and is not allowed to redistribute the software or create derivatives which use parts of the work. For the above reasons, proprietary licenses are commonly used for commercial software [8].

### **Free and Open Source Licenses**

In contrast to proprietary licenses the aim of free and open source licenses is to maximize the openness of software use. Therefore, these licenses allow the modification and redistribution of the software and the source code under predefined terms. The licensed software is not necessarily free of charge even though it is often the case. Free and open source licenses do not discriminate against any category of user so the software can be used for private and commercial purposes. There are two main types of free and open source licenses. On the one hand there are the permissive licenses which impose minimal requirements on how the software can be redistributed. On the other hand there are copyleft licenses that grant the openness of the software by ensuring that derivative software is redistributed under the same license terms as the original work [8].

### **Multi-Licensed Software**

Another form of software licensing is called multi-licensing. The scheme of multi-licensing differs from single licensing in that way that software is distributed under two or more different types of licenses. An open source as well as a proprietary license should be part of the set of licenses. Generally, there could be more licenses in the set. The end-user can then decide under which of the provided licenses the software should be purchased. Thus, end-users can decide for the type of license that best suits their needs. In this way, publishers of derivative software are given more freedom when it comes to choosing the type of license they want to use for their work. Therefore, this form of licensing is convenient in terms of license compatibility and market segregation.

#### **4.5.2 Licensing of the ECOSSIAN system**

As it is not yet clear whether the whole ECOSSIAN system will be licensed and the license model itself strongly depends on the tools used to develop the ECOSSIAN system it is not yet possible to make clear assumptions on potential license models for the whole system at this stage of the project. However, there are some factors to bear in mind when it comes to licensing the ECOSSIAN system:

- Type of license of the tools used
- Stated purpose of the tools used
- Costs of the licensing model

### **Tools used**

Some open source licenses, namely copyleft licenses, demand derivative software to be published under similar license terms as the original software. Strong copyleft licenses even demand that all derivative works which link or incorporate the original work are published under compatible open source license. Due to the fact that copyleft licenses aim at preserving the freedom of software and derivative software, these licenses are mainly used for free software. As the ECOSSIAN system is developed for commercial use permissive licenses should rather be used. For this reason, tools published under copyleft licenses

should be avoided in the final system because these may affect and restrict the choice of license for the system.

### Stated purpose

Another important point to consider is that certain licenses state an intended use of the software which might not include the application in CIs. This is a response to publishers' fear of legal consequences in case that a failure of their software causes an incident in a CI or delay the alerting process after an incident. For this reason, certain tools might not be allowed to be used within CIs or their warning systems by the license terms of the software. However, this does not necessarily cause problems in case of the ECOSSIAN system as these software tools might still be used when it can be argued that the ECOSSIAN system complements the already existing alerting practices. This means that even if a used software tool fail early warning and alerting still works.

### Costs of the license model

Further, it would be a clear advantage if the costs of the whole license model were rather low as an expensive license model entails higher a pricing of the whole system. This could decrease the overall attractiveness of the system for potential customers such as CI operators. Again certain licenses can cause problems in this context especially when they make demands on the license of derivate software.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.5.1	Type of license for the system or parts of the system should be permissive	O	2,3,4,5	X	X	X
REQ-4.5.2	Tools used in the system should not be licensed under a copyleft license	O	2,3,4,5	X	X	X
REQ-4.5.3	The whole license model should be rather inexpensive	O	2,3,4,5	X		

Table 4.5: Licensing requirements

## 4.6 Modelling Requirements

This chapter describes requirements regarding the modelling of software, systems, business processes as well as IT processes and IT organisation. For each of the corresponding modelling scopes, introducing examples will be provided along with a recommendation of dedicated tools.

### 4.6.1 Software Modelling

This visualisation should support the entire software development process, e.g. Requirements > Design > Implementation > Verification > Maintenance as well as for documental purposes.



## UML Overview

With the UML Superstructure Specification [19], first language entities are introduced. An entity covers a set of modelling elements, enabling the user to model a dedicated aspect of a system according to a specified formalism.

Based on the language entities, UML provides a set of diagrams enabling the user to model the structure behaviour of systems as well as the interaction between those components.

## UML Diagrams

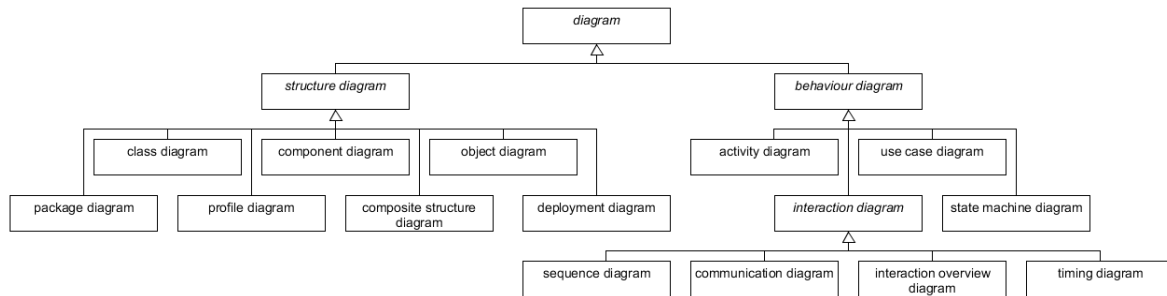


Figure 4.1: UML Diagram Hierarchy

UML provides three classifications of UML diagrams:

### Behaviour diagrams

A type of diagram that depicts behavioural features of a system or business process. This includes activity, state machine, and use case diagrams as well as the four interaction diagrams.

### Interaction diagrams

A subset of behaviour diagrams which emphasize object interactions. This includes communication, interaction overview, sequence, and timing diagrams.

### Structure diagrams

A type of diagram that depicts the elements of a specification that are irrespective of time. This includes class, composite structure, component, deployment, object, and package diagrams.

Table 4.6 provides quick description of different types of UML Diagrams. More details and examples of every diagram type can be found in Appendix I.

Diagram	Description
Activity Diagram	Depicts high-level business processes, including data flow, or to model the logic of complex logic within a system.
Class Diagram	Shows a collection of static model elements such as classes and types, their contents, and their relationships.
Communication Diagram	Shows instances of classes, their interrelationships, and the message flow between them. Communication diagrams typically focus on the structural organization of objects that send and receive messages. Formerly called a Collaboration Diagram.
Component Diagram	Depicts the components that compose an application, system, or enterprise. The components, their interrelationships, interactions, and their public interfaces are depicted.
Composite Structure Diagram	Depicts the internal structure of a classifier (such as a class, component, or use case), including the interaction points of the classifier to other parts of the system.
Deployment Diagram	Shows the execution architecture of systems. This includes nodes, either hardware or software execution environments, as well as the middleware connecting them.
Interaction Overview Diagram	A variant of an activity diagram which overviews the control flow within a system or business process. Each node/activity within the diagram can represent another interaction diagram.
Object Diagram	Depicts objects and their relationships at a point in time, typically a special case of either a class diagram or a communication diagram.
Package Diagram	Shows how model elements are organized into packages as well as the dependencies between packages. See Package diagram guidelines.
Profile Diagram	Operates at the meta-model level to show stereotypes as classes and profiles as packages
Sequence Diagram	Models the sequential logic, in effect the time ordering of messages between classifiers. See UML Sequence diagram guidelines.
State Machine Diagram	Describes the states an object or interaction may be in, as well as the transitions between states. Formerly referred to as a state diagram, state chart diagram, or a state-transition diagram.
Timing Diagram	Depicts the change in state or condition of a classifier instance or role over time. Typically used to show the change in state of an object over time in response to external events.
Use Case Diagram	Shows use cases, actors, and their interrelationships. See UML Use case diagram guidelines.

Table 4.6: UML Diagrams

#### 4.6.2 User Interface Modelling

Since user interface modelling is a dedicated science and there exist no overall standard modelling language for the specification of user interfaces covering the design of webpages as well as desktop applications no dedicated requirements will be stated here.

Since Microsoft Office was selected as the toolset for documentation purposes, user interfaces shall be designed with Microsoft Visio or Microsoft PowerPoint.

#### 4.6.3 Business Process Modelling

**BPMN Overview:** BPMN is maintained by the Object Management Group (OMG), which is a not-for-profit industry standards consortium with expertise in wide range of computer technologies. BPMN modelling helps to design the diagram of business processes in flowcharts with a specific set of graphical notations. So it simplifies the presentation of business processes, activities and their flow of information for business users and developers or implementers.

**BPMN Elements:** For consistent comprehensibility of the business processes in graphical form, BPMN 2.0 defines different elements, and also categorizes them. There are eventually five basic categories of elements in BPMN [20]:

1. Flow Objects
2. Data
3. Connecting Objects
4. Swim lanes
5. Artefacts

Detailed description of BPMN elements can be found in Appendix II.

**BPMN software:** There are plenty of commercial and open source software for BPMN 2.0 modelling. Here we only present those that are available in free version and up-to-date (in alphabetic order):

- **Activiti Modeler** is an open source cross-platform solution that provides BPMN 2.0 process modelling. It is developed by Alfresco and the Activiti community.
- **Bizagi Modeler** supports 100% of BPMN notations and developed by Bizagi, which is one of the copyright holders of the BPMN 2.0 specification document provided by OMG. It works only on Windows machine, and supports drag-and-drop design features.
- **Bonita BPM Community Edition** is an open source solution that provides BPMN 2.0 process modelling. It is developed by Bonitasoft. It works on Windows, Mac OS and Linux, and supports drag-and-drop design features.
- **Camunda BPMN 2.0 Modeler** is an open source BPMN 2.0 compliant modelling tool. It is developed by camunda Services GmbH. It works on Windows, Mac OS and Linux, and supports drag-and-drop design features.
- **Eclipse BPMN2 Modeler** is a cross platform solution built on Eclipse Graphiti. It supports BPMN 2.0 specification provided by OMG. It is developed by The Eclipse Foundation. It supports drag-and-drop design features.

- **Modelio** is an open source solution that provides BPMN 2.0 process modelling elements to design BPMN2 diagrams. It is developed by Modeliosoft, and works on Windows, Mac OS and Linux.
- **Yaoqiang BPMN Editor** is an open source BPMN editor fully compatible with BPMN 2.0 specification of OMG. It also supports all elements of the BPMN 2.0, and provides drag-and-drop features. It works on Windows, Mac OS and Linux.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.6.1	In order to provide a standard way to visualize the design of software parts and other systems the Unified Modelling Language (UML) version 2.4.1 or later must be used.	M	2,3,4	X	X	X
REQ-4.6.2	All business processes, activities and their flow of information should be presented in Business Process Model and Notation version 2.0 (BPMN 2.0). It will allow every member of the consortium to present their business processes in a consistent way readily understandable by others.	O	2,3,4	X	X	X
REQ-4.6.3	For modelling of user interfaces, common Microsoft Office products (Visio, PowerPoint) shall be used.	O	2,3,4	X	X	X

Table 4.7: Modelling requirements

## 4.7 Change Management Requirements

Requirements in this section are only relevant once the ECOSSIAN system will be built in a real-world production scenario. For the demonstrator and project phase, a simplified process should be used.

### General

Change management is an important part of systems and/or organizations. To ensure continuous development and maintainability of the system, the change management has to be integrated into the organization as an integral part of it. An intelligent process should be designed, that is lightweight but at the same time ensures the targets of the change management are met. This chapter gives an overview about the most important requirements to be met by ECOSSIAN in order to ensure that change is managed in an optimal way. Even if the golden rule for IT-Systems is “never touch a running system”, in practice it is necessary to conduct changes on a frequent basis. The Change Management is an essential tool to manage change as good as possible.

### Requirements

Change Management Requirements:

- A formal change management must be part of the ECOSSIAN system. As a European system, the complexity of ECOSSIAN is very high. Many different interfaces will be present and the layered and distributed nature of the system makes it even more complex. With many different partners involved and very critical

information that is being processed by the system, changes must be carefully planned and managed.

- The Change Management must ensure, that the impact of changes will be analyzed and monitored. It is very important that changes will not affect the running system in an unexpected way. All affected parties have to be notified about upcoming changes and must be able to express their opinion about the change. Changes on one component of the system must not interfere with the operation of the system at another component. On the other hand, the Change Management should also ensure, that only those changes are executed, that are economically reasonable.
- The change management should use a Request for Change (RFC) format to request and document all changes. The RFC should contain the following information:
  - Unique change identifier
  - List of affected items
  - Justification of change
  - Consequences of “no change”
  - Priority
  - Contact person
  - Timestamp of request and approval
  - Planned change date
  - Back-Out plan
  - Status information
  - Signature(s)
- An approval process for changes should be established. The approval process should be designed in accordance to the priority of the change. For changes with a low priority, a change manager is responsible for approving and coordinating all changes. For changes with a higher priority, a Change Advisory Board (CAB) must be established, which has to review and approve all changes. Because of the layered architecture of ECOSSIAN, the CAB must be divided into smaller CABs, which are responsible for changes that only have interactions within the respective layer. For changes having impact on more than one layer, a dedicated CAB should be established, involving all partners.
- It has to be assured, that only persons with adequate qualifications are included in the CAB and other relevant bodies.
- For time critical (emergency) changes, a special approval and documentation procedure needs to be developed and followed at all time, which allows the required flexibility but at the same time, ensures a proper management and documentation of all emergency changes.
- A testing procedure needs to be developed and integrated into the change process. All changes made to hardware, software and configurations need to be tested prior to implementation. The change Management process should include mandatory tests prior to change implementation. In case of emergency changes, testing can be replaced by other appropriate steps.
- A catalogue of criteria must be available, explaining how to prioritize requests and how to qualify for an emergency level change. Based on that classification, the document must also define approval rules.
- The formal change management must be established at all ECOSSIAN member organizations.
- All dependencies and relationships with other organizational processes must be identified and documented. The change management should integrate with all other

management processes (e.g. configuration management).

- Reports must be created on a regular basis, allowing to monitor the change management process and all changes.
- Regular audits of the change management process have to be conducted to ensure that the change management process is followed.
- For all non-minor changes, a Post Implementation Review (PIR) has to be conducted reviewing the results and the implementation of the change. The PIR should ensure a continuous improvement of the change management process and a controlling of all changes. The PIR results should be monitored by the CAB and other relevant bodies.

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.7.1	Formal change management should be part of ECOSSIAN.	O	N/A	X	X	X
REQ-4.7.2	The change management should track (potential) impact of all changes.	O	N/A	X	X	X
REQ-4.7.3	The change management should use a Request for Change template.	O	N/A	X	X	X
REQ-4.7.4	An approval process for changes should be established for ECOSSIAN as part of the change management.	O	N/A	X	X	X
REQ-4.7.5	Only qualified persons should be included in the Change Advisory Board.	O	N/A	X	X	X
REQ-4.7.6	Special approval process should be developed for emergency changes.	O	N/A	X	X	X
REQ-4.7.7	Testing for all changes should be assured.	O	N/A	X	X	X
REQ-4.7.8	Change prioritization criteria should be documented.	O	N/A	X	X	X
REQ-4.7.9	The change management should be established at all ECOSSIAN member organizations.	O	N/A	X	X	X
REQ-4.7.10	Dependencies of change management processes with other organizational processes should be identified and documented.	O	N/A	X	X	X
REQ-4.7.11	Reports about all changes should be generated regularly.	O	N/A	X	X	X
REQ-4.7.12	Audits of the change management should be performed regularly.	O	N/A	X	X	X
REQ-4.7.13	A Post Implementation Review should be conducted for all changes.	O	N/A	X	X	X

Table 4.8: Change Management requirements

## 4.8 Organisational Requirements

### Conventions and Agreements

In order to increase the value of the exchanged information in the ECOSSIAN platform, international conventions and agreements should be signed between the ECOSSIAN management and the most relevant stakeholders:

- Critical Infrastructures
- Law enforcement and intelligence agencies
- Economics-based interest group (i.e. companies that mainly operate independent within their common economic principles for-profit)
- Manufacturer, supplier and infrastructure provider
- Security service provider and response teams (i.e. security companies, CERTs/CSIRTs, National CERTs, CERT networks)
- Public and sovereignty interest groups that are not mainly economical oriented but foremost acts in a holistic socially interest. (i.e. European bodies, governmental institutions, other info-sharing initiatives, sector-specific interest groups, etc.)
- Research institutes and Universities
- Media and Press Agencies

Each organization has its own needs and expectations towards a suitable framework enabling a compliant exchange of security-related information across multiple administrative domains. According to their economic interests, the resulting needs depend on organization's legal and regulatory situation as well as on their own internal obligations, policies, governance structure and business model. Hence:

### Certification & Security Standards

Meeting industry standards to prevent disclosure of sensitive data, adopting sector best practices and gaining third party certifications are essential elements not only from a technical point of view, but also from an organizational perspective, in order to strengthen the level of trust users may have in the ECOSSIAN eco-system.

Several international information security standards, already analyzed in Deliverable 1.1, should be taken into consideration while developing, deploying and operating the ECOSSIAN framework, such as:

Category	Standard/best practice
Identification of threats to Industrial Control Systems	BSI-CS 010 [21]
Guidelines for process control and security	VDI/VDE 2180 [22], VDI/VDE 2182 [23], ISO/IEC TR 27019:2013 [24]
Technical provisioning and security capabilities	IEEE 1686-2013 - Standard for Intelligent Electronic Devices Cyber Security Capabilities [26], BDEW White Paper [27], CEN-CENELEC-ETSI SGCG Smart Grid Information Security [28], NAMUR-Worksheet [29], EDSA-310 [30]

Category	Standard/best practice
Security Information Sharing standards and best practices	ITU-T CYBEX [31][32][33], ETSI ISG ISI [34], IETF SACM/NIST SCAP [35], CEF, CAIF [39], EISPP, DAF, MITRE: STIX [36], TAXII [37], CybOX [38], CVE & CWE, CPE & CCE, CEE, NIST SP 800-150: Guide to Cyber Threat Information Sharing
IETF Extended Incident Handling Working Group	IDMEF, CVRF [24], ENISA [24]

Table 4.9: Security Standards and Best Practices

### Resiliency of the ECOSSIAN platform and framework services

Framework services should be resilient, in order to be of use during cyber-crisis events. Appropriate organizational measures should be also adopted to guarantee framework services availability in term of underlying resources (i.e. IT systems, communication channels and networks, personnel, facilities, utilities, etc.).

### Personnel and users training

Training content for operators should be developed in order to gain the competencies needed to operate the ECOSSIAN framework services and infrastructure.

Training content for users should be developed on framework services and tools usage.

Accordingly, adequate Training Plans should be developed to outline who will deliver training to operators and users, when and where.

### Communication

A cyber-crisis Communication Plan should be developed in order to manage any situation that threatens the integrity or reputation of ECOSSIAN (i.e. cyber-incident, legal dispute, theft, accident, fire, flood, manmade disaster) but also to support ECOSSIAN users in case of cyber-crisis events.

### Technical service, security monitoring and user support of the ECOSSIAN platform

An important requirement concerning the availability of the ECOSSIAN platform/services is a well-developed and consistent service structure for users. Additionally, user activities should be constantly monitored in order to prevent and detect abuses of the ECOSSIAN services/platform and to manage cyber-crisis events.

### Multilingual environment

The ECOSSIAN framework operates in a cross-organisational, cross-national environment; data, metadata, documentation, software, and other components will need to support and operate in multiple languages.



## Staff requirements

- *Manager(s)*: coordinate activities, report to stakeholders (decisions), advocate the facility, and dialog with users.
- *IT administrators*: setup, maintain and operate the ECOSSIAN technical infrastructure, monitor and control systems and user activities in order to prevent and detect system malfunctions, prevent misuse or unauthorized access.
- *Dedicated SOC operators*: monitor user activities in order to prevent and detect system anomalous user behaviours (misuse), abuses or unauthorized accesses to the ECOSSIAN systems/tools.
- *Training support team*: design training content, deliver on-site training or using virtual training environments, help user accessing and using the environment, periodically monitor ECOSSIAN framework usability in order to identify possible areas of improvements. A Training plan should be developed accordingly.
- *Knowledge manager(s)*: maintain and moderate the collaborative environment, feed the public/internal web site, participate in monitoring ECOSSIAN framework usability activities.
- *Support staff*: for user lifecycle management, Single Point of Contact for law enforcement and intelligence agencies, users/stakeholders reporting, contracting, legal advising, compliance enforcement, general administration, etc.

## Skill requirements

ECOSSIAN staff suggested skills are the following:

- *ECOSSIAN manager*: Project Management, Team building, Incident Management & Reporting, Information Sharing Best Practices, fluent English
- *IT administrators*: System & Network administration and monitoring, Security tools, applications and infrastructure, Business Continuity and Disaster Recovery, Patch management
- *SOC operators*: Perimetral defence systems, SIEMs, Data analysis & correlation, Log analysis, Vulnerability Management, Penetration Testing
- *Training support team*: Strong communication, Customer management, ECOSSIAN framework (strong), Education & Training, Awareness building, fluent English, good command of another EU official or working language (i.e. Dutch, French, German, Italian, etc.), Usability
- *Knowledge manager*: Strong communication, Web content management, Collaboration, fluent English, Usability
- *Support staff*: Accounting, Legal, Administration

Req. #	Description	Importance (M/O)	WP	Relevant for		
				O-SOC	N-SOC	E-SOC
REQ-4.8.1	A suitable process and service framework for information exchange should adapt to existing business and service delivery processes to enable a minimal invasive amendment for inter-organizational information flow whilst respecting compliance issues.	O	N/A	X	X	X
REQ-4.8.2	A security plan covering the entire ECOSSIAN eco-system domain, should be prepared to document adopted protective measures and standards. The plan should be updated as needed and revised periodically (at least each year).	O	N/A	X	X	X
REQ-4.8.3	Contingency Organizational Plans should be developed and integrated in the BCM plan in order to guarantee service continuity and recovery of possibly disrupted services also from an organizational point of view.	O	N/A	X	X	X
REQ-4.8.4	The Training Plan should at least specify: (1) the training prerequisites and requirements; (2) the competencies to be obtained; (3) the training paths to be undertaken; (4) the training delivery modes to be employed.	O	N/A	X	X	X
REQ-4.8.5	A cyber-crisis Communication Plan should be developed.	O	N/A	X	X	X
REQ-4.8.6	Personnel Allocation Plan and Organization Plan should be developed.	O	N/A	X	X	X
REQ-4.8.7	An Internationalization Plan should be designed.	O	N/A	X	X	X
REQ-4.8.8	Appropriate staffing plan should be developed.	O	N/A	X	X	X

Table 4.10: Organizational requirements

## Chapter 5 Conclusions

This document provided a comprehensive list of requirements to build a system as originally envisioned in ECOSSIAN Description of Work [1] and ECOSSIAN Use Case Scenarios [2].

The system should be constructed on three main levels, and some of the requirements differ depending on the level of the system: on critical infrastructure operators' level, on national level, and on EU level. Therefore every requirement contains attribution to the levels it affects. For easier navigation within the ECOSSIAN system, the work package attribution marks the work packages that are either responsible for implementing the requirement, or are affected by its successful implementation. Also of note is the importance level that is assigned to every requirement. While the mandatory (M) requirements present the framework of the system and must be fulfilled, many of the optional (O) requirements are either only important for the system that is operated in production (as opposed to a proof of concept system), or are outside of the scope of the ECOSSIAN project.

It should be noted that, as with every system that is a part of ongoing research, these requirements may sustain changes as the system goes further into development. Normally, in such cases further documentation will provide reasonable explanation for why such changes were necessary.

## Chapter 6 List of Abbreviations

AAA	Authentication, Authorisation, and Accounting
AACM	Aggregation, Analysis, and Correlation Module
AM	Aggregation Module
BPMN	Business Process Model and Notation
C2	Command and Control
CAB	Change Advisory Board
CI	Critical Infrastructure
C-I-A	Confidentiality, Integrity and Availability
CIP	Critical Infrastructure Protection
CM	Correlation Module
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf (products)
CSIRT	Computer Security Incident Response Team
DoW	Description of Work
ECOSSIAN	European Control System Security Incident Analysis Network
EPCIP	European Programme for Critical Infrastructure Protection
E-SOC	European Security Operations Center
FAT	Factory Acceptance Testing
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IMM	Incident Management Module
MoE	Measure of Effectiveness
MS	Member States

MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
N-SOC	National Security Operations Center
NTP	Network Time Protocol
OMG	Object Management Group
O-SOC	Operator's Security Operations Center
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PIR	Post Implementation Review
QoS	Quality of Service
RAM	Risk Assessment Module
RFC	Request for Change
SA	Situational Awareness
SCADA	Supervisory Control And Data Acquisition
SDS	Secure Data Storage
SEF	Security Enforcing Function
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Small- and Medium-sized Enterprises
SOC	Security Operations Center
SSL	Secure Sockets Layer
TDM	Threat Detection Module
TMM	Threat Mitigation Module
TTP	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UML	Unified Modelling Language
VM	Visualization Module

VPN	Virtual Private Network
-----	-------------------------

## Chapter 7 Bibliography

- [1]. ECOSSIAN DoW-Description of Work
- [2]. ECOSSIAN Deliverable 1.5 – Use Case Scenario Report
- [3]. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K., Identifying, understanding, and analyzing critical infrastructure interdependencies, Control Systems, IEEE , vol.21, no.6, pp.11,25, Dec 2001, url: <http://user.it.uu.se/~bc/Art.pdf>
- [4]. Public Private Partnerships for Critical Infrastructure Protection: [http://csis.org/files/publication/130819\\_PPP.pdf](http://csis.org/files/publication/130819_PPP.pdf) , part4
- [5]. Loren Dietrichsen, "Command and Control: Operational requirements and System Implementation", 2000, Information and Security, Vol.5, 2000
- [6]. [http://en.wikipedia.org/wiki/Performance\\_metric](http://en.wikipedia.org/wiki/Performance_metric)
- [7]. <http://www.valuesec.eu/>
- [8]. Laurent, Andrew M. St. Understanding open source and free software licensing. O'Reilly Media, Inc., 2004.
- [9]. Morin, Andrew, Jennifer Urban, and Piotr Sliz., A quick guide to software licensing for the scientist-programmer. PLoS computational biology 8.7 (2012): e1002598.
- [10]. World Economic Forum, Global Risks 2014. Ninth Edition, Geneva, 2014, p17, [http://www3.weforum.org/docs/WEF\\_GlobalRisks\\_Report\\_2014.pdf](http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf).
- [11]. A. Cavoukian, Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers, Information and privacy commissioner of Ontario, Canada, 2011.
- [12]. A. Cavoukian, Privacy by design: the 7 foundational principles, Information and privacy commissioner of Ontario, Canada, 2009.
- [13]. ENISA report: The implementation of the Privacy and Data Protection by Design – from policy to engineering, DOI 10.2824/38623
- [14]. Jaap-Henk Hoepman. Privacy design strategies – (extended abstract). In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings, pages 446–459, 2014.
- [15]. Bart Jacobs, 'Select before you collect', Ars Aequi, 54:1006-1009, December 2005
- [16]. Latanya Sweeney, 'k-anonymity: A model for protecting privacy', International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5) (2002) 557-570
- [17]. ENISA, Cyber Incident Reporting in the EU: An overview of security articles in EU legislation, August 2012, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu>.
- [18]. DISO/IEC 19505-2:2012, Information technology - Object Management Group Unified Modeling Language (OMG UML), Superstructure, 2012.
- [19]. ISO/IEC 19510:2013, Information technology - Object Management Group Business Process Model and Notation, 2013.
- [20]. ISO/IEC 19505-1:2012, Information technology - Object Management Group Unified Modeling Language (OMG UML), Infrastructure, 2012.

- [21]. BSI-CS 010, Empfehlung: IT IN DER PRODUKTION, Industrial Control System Security, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 2012. English Version: German Federal Office for Information Security – BSI, RECOMMENDATION: FACTORY-IT, Industrial Control System Security, Top 10 Threats and Countermeasures, 2012, URL: [http://www.allianz-fuer-cybersicherheit.de/ACS/DE/downloads/techniker/hardware/BSI-CS\\_005E.pdf](http://www.allianz-fuer-cybersicherheit.de/ACS/DE/downloads/techniker/hardware/BSI-CS_005E.pdf)
- [22]. VDI/VDE-Richtlinien, Safeguarding of industrial process plants by means of process control engineering, VDI/VDE 2180 Part 1 bis Part 5, 2010
- [23]. VDI/VDE-Richtlinien, Informationssicherheit in der industriellen Automatisierung, VDI/VDE 2182 Blatt 1, 2009. English Version: IT-security for industrial automation, General model, VDI/VDE 2182 Part 1, 2011, URL: [http://www.vdi.de/uploads/tx\\_vdirili/pdf/1728597.pdf](http://www.vdi.de/uploads/tx_vdirili/pdf/1728597.pdf)
- [24]. ENISA, «Technical Guideline on Incident Reporting,» European Network and Information Security Agency, 2011.
- [25]. ISO/IEC TR 27019:2013: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, ISO/IEC 2013.
- [26]. IEEE 1686-2013: Intelligent Electronic Devices Cyber Security Capabilities, IEEE, 2013
- [27]. BDEW: White Paper, Requirements for secure Control and telecommunication Systems, version 1.0, BDEW - Federal Association of Energy and Water Industries, Berlin, 2008
- [28]. CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Information Security, November 2012
- [29]. NAMUR: IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries, NAMUR Worksheet NA115, 2006
- [30]. ISA Security Compliance Institute: EDSA-310 - Embedded Device Security Assurance – Common requirements for communication robustness testing of IP-based protocol implementations, Version 1.7, 2010
- [31]. ITU-T, «ITU-T in brief» [Online]. Available: <http://www.itu.int/en/ITU-T/about/Pages/default.aspx>
- [32]. ITU-T, «Study Group 17 at a glance,» [Online]. Available: <http://www.itu.int/en/ITU-T/about/groups/Pages/sq17.aspx>
- [33]. ASMONIA project, «D1.4 - Validation of cooperative methods,» 2011.
- [34]. P. D. Lutiis, «ETSI ISG ISI Standardization,» in 8th ETSI Security Workshop, 2012.
- [35]. NIST, The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.2, NIST Special Publication 800-126 Revision 2, 2011.
- [36]. MITRE, «Structured Threat Information eXpression,» [Online]. Available: <https://stix.mitre.org>
- [37]. MITRE, «Trusted Automated eXchange of Indicator Information,» [Online]. Available: <http://taxii.mitre.org/>
- [38]. RUS-CERT, University of Stuttgart, Germany, «CAIF - COMMON ANNOUNCEMENT INTERCHANGE FORMAT,» [Online]. Available: <http://www.caif.info>
- [39]. ICASI, «The Common Vulnerability Reporting Framework,» [Online]. Available: <http://www.icaso.org/cvrf>



## Appendices

### Appendix I. UML Diagrams

*Activity diagrams* represent workflows in a graphical way. They can be used to describe business workflow or the operational workflow of any component in a system. Sometimes activity diagrams are used as an alternative to State Machine diagrams.

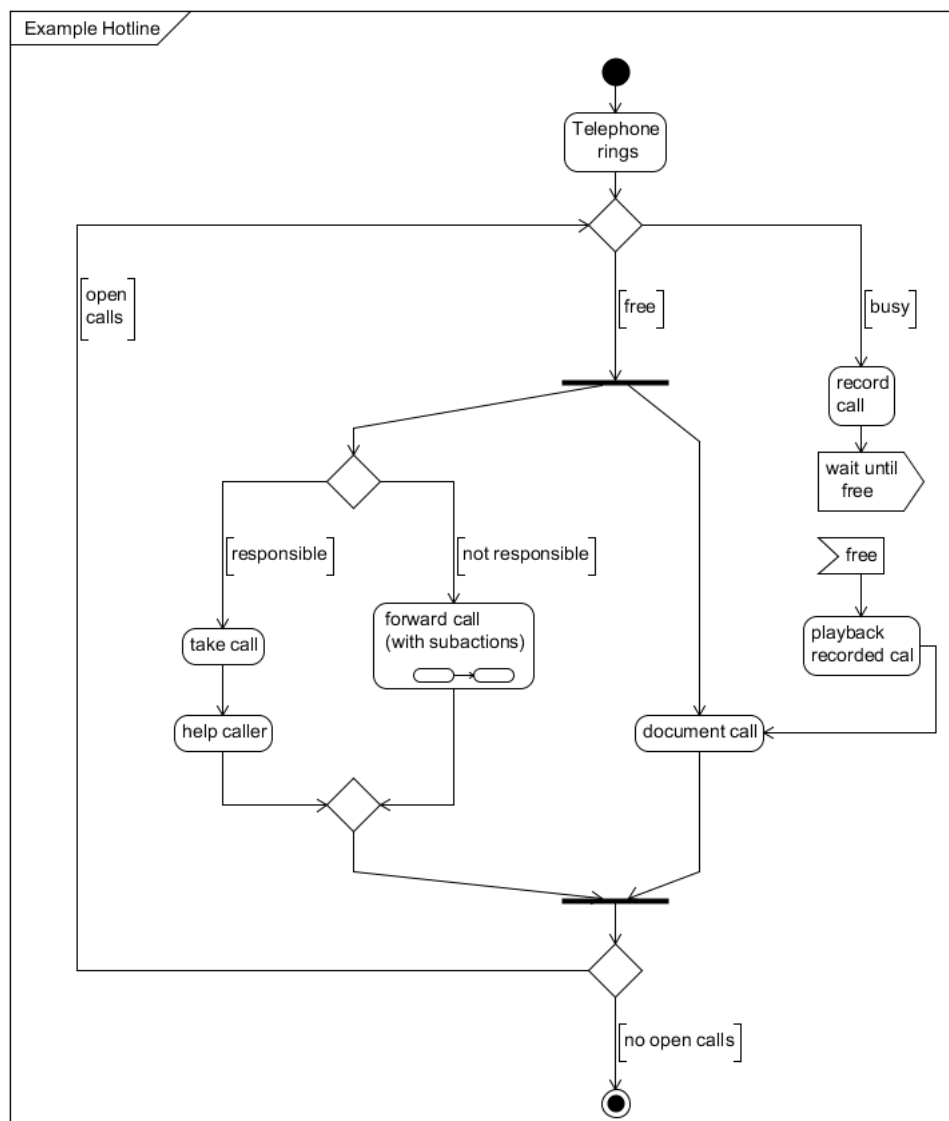


Figure A.1: UML Activity Diagram

*Class diagrams* are arguably the most used UML diagram type. It is the main building block of any object oriented solution. It shows the classes in a system, attributes and operations of each class and the relationship between each class.

In most modelling tools a class has three parts, name at the top, attributes in the middle and operations or methods at the bottom. In large systems with many related classes, classes are grouped together to create class diagrams. Different relationships between classes are shown by different types of arrows.

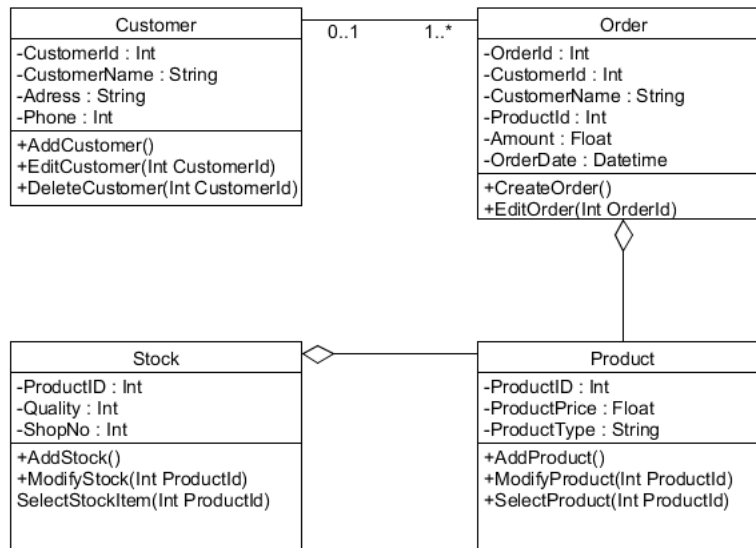


Figure A.2: UML Class Diagram

Communication diagram was called collaboration diagram in UML 1. It is similar to sequence diagrams but the focus is on messages passed between objects. The same information can be represented using a sequence diagram and different objects.

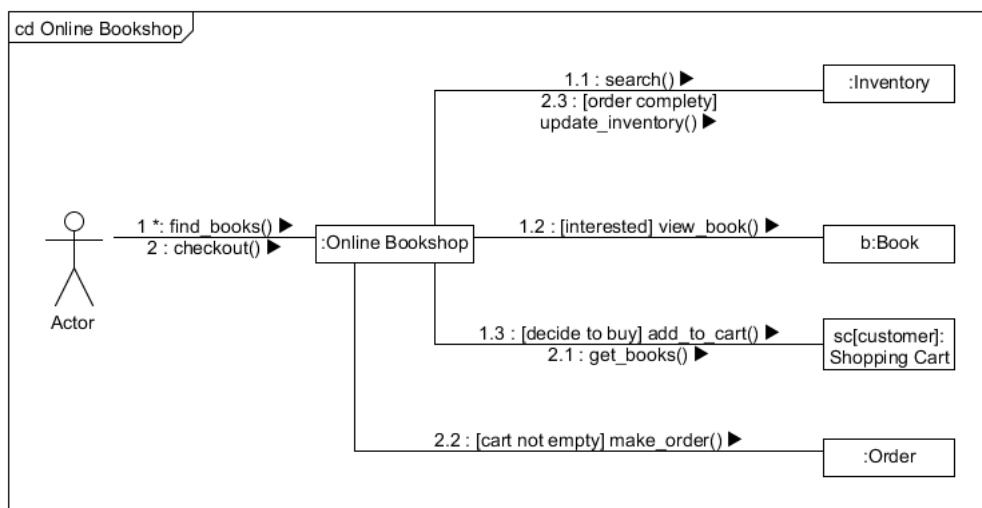


Figure A.3: UML Communication Diagram

A component diagram displays the structural relationship of components of a software system. These are mostly used when working with complex systems having many components. Components communicate with each other using interfaces. The interfaces are linked using connectors.

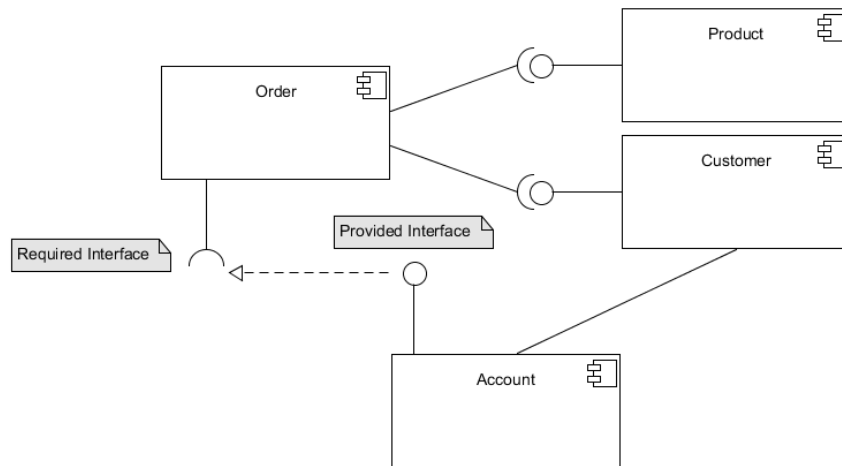


Figure A.4: UML Component Diagram

Composite structure diagrams are used to show the internal structure of a class.

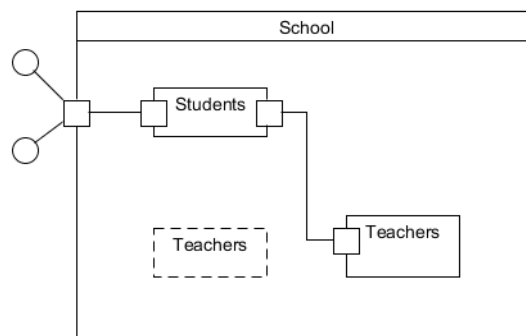


Figure A.5: UML Composite Structure Diagram

Deployment diagrams show the hardware of your system and the software in that hardware. Deployment diagrams are useful when your software solution is deployed across multiple machines with each having a unique configuration.

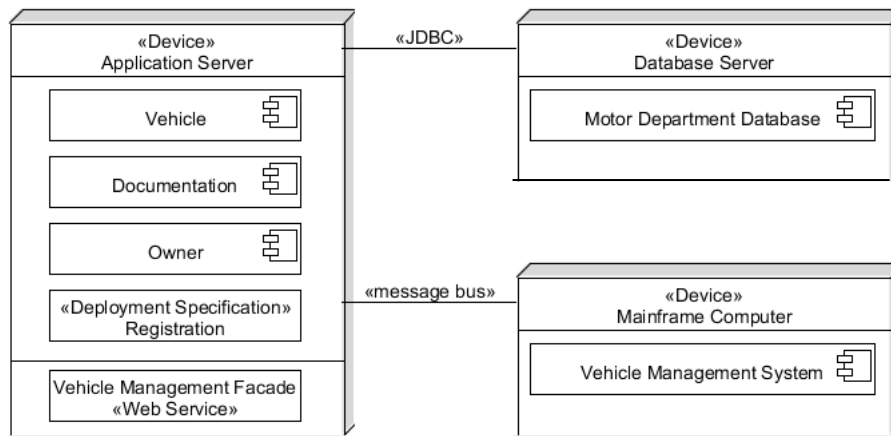


Figure A.6: UML Deployment Diagram

*Interaction overview diagrams* are very similar to activity diagrams. While activity diagrams shows a sequence of processes Interaction overview diagrams shows a sequence of interaction diagrams. In simple term they can be called a collection of interaction diagrams and the order they happen.

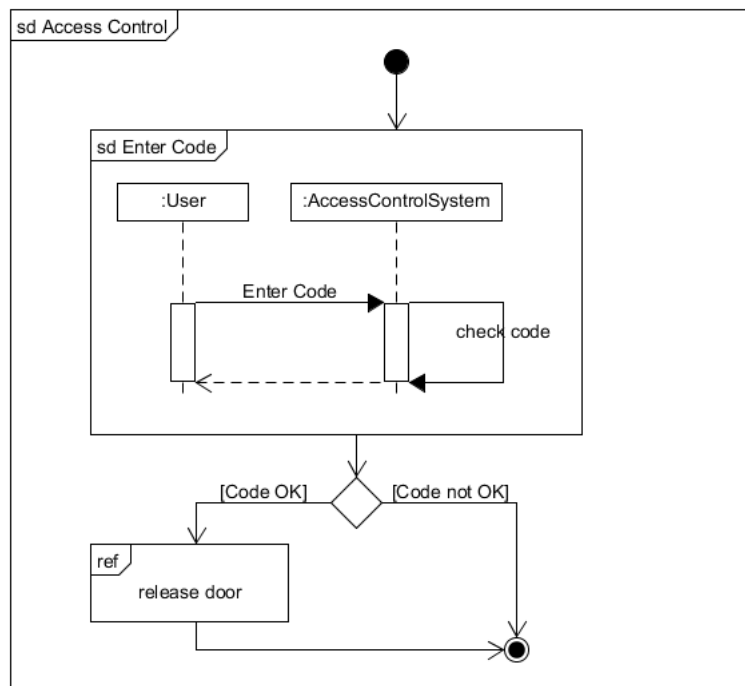


Figure A.7: UML Interaction Overview Diagram

*Object Diagrams*, sometimes referred as Instance diagrams are very similar to class diagrams. As class diagrams they also show the relationship between objects but they use real world examples. They are used to show how a system will look like at a given time. Because there is data available in the objects they are often used to explain complex relationships between objects.

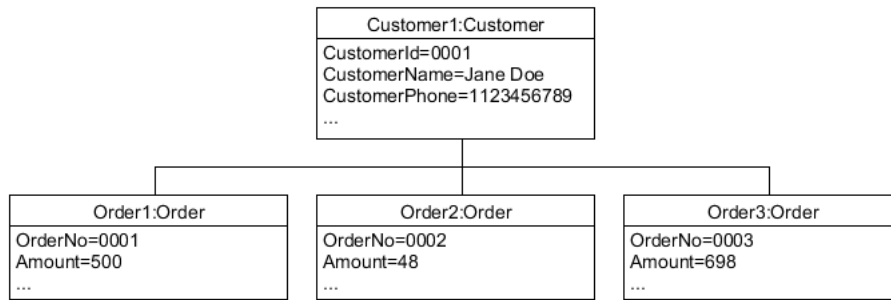


Figure A.8: UML Object Diagram

As the name suggests, package diagrams show the dependencies between different packages in a system.

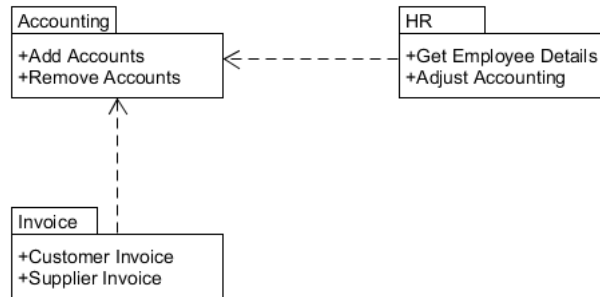


Figure A.9: UML Package Diagram

Profile diagram is a new diagram type introduced in UML 2. This is a diagram type that is very rarely used in any specification.

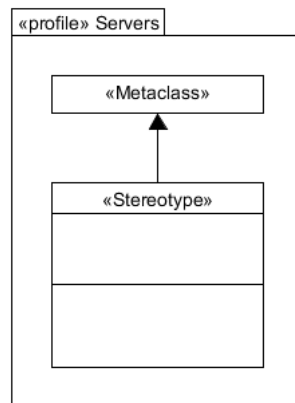


Figure A.10: Profile Diagram

Sequence diagrams in UML shows how object interact with each other and the order those interactions occur. It's important to note that they show the interactions for a particular scenario. The processes are represented vertically and interactions are show as arrows.

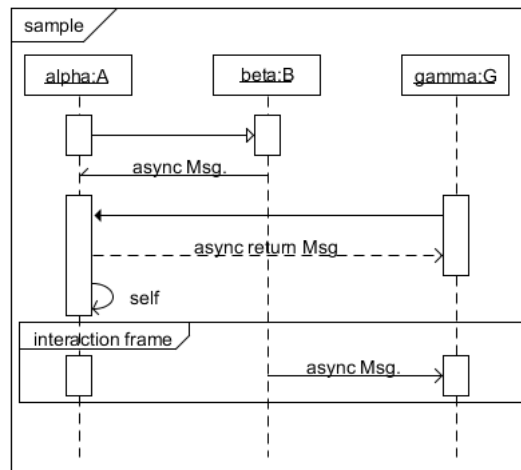


Figure A.11: UML Sequence Diagram

State machine diagrams are similar to activity diagrams although notations and usage changes a bit. They are sometime known as state diagrams or start chart diagrams as well. These are very useful to describe the behaviour of objects that act different according to the state they are at the moment.

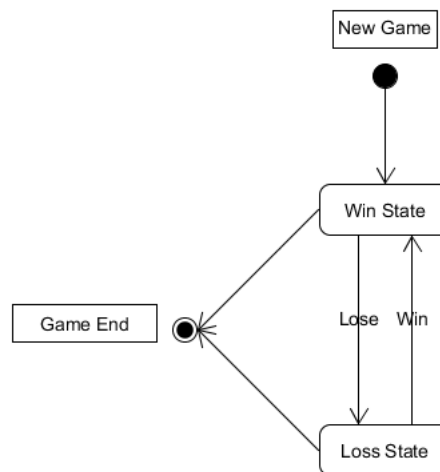


Figure A.12: UML State Machine Diagram

Timing diagrams are very similar to sequence diagrams. They represent the behaviour of objects in a given time frame. If it is only one object the diagram is straight forward but if more than one objects are involved they can be used to show interactions of objects during that time frame as well.

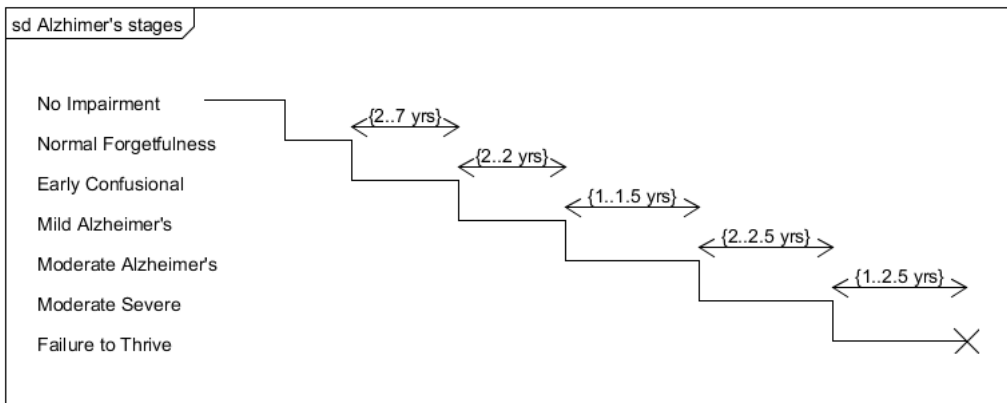


Figure A.13: UML Timing Diagram

Most known diagram type of the behavioural UML diagrams, *use case diagrams*, gives a graphic overview of the actors involved in a system, different functions needed by those actors and how these different functions are interacted.

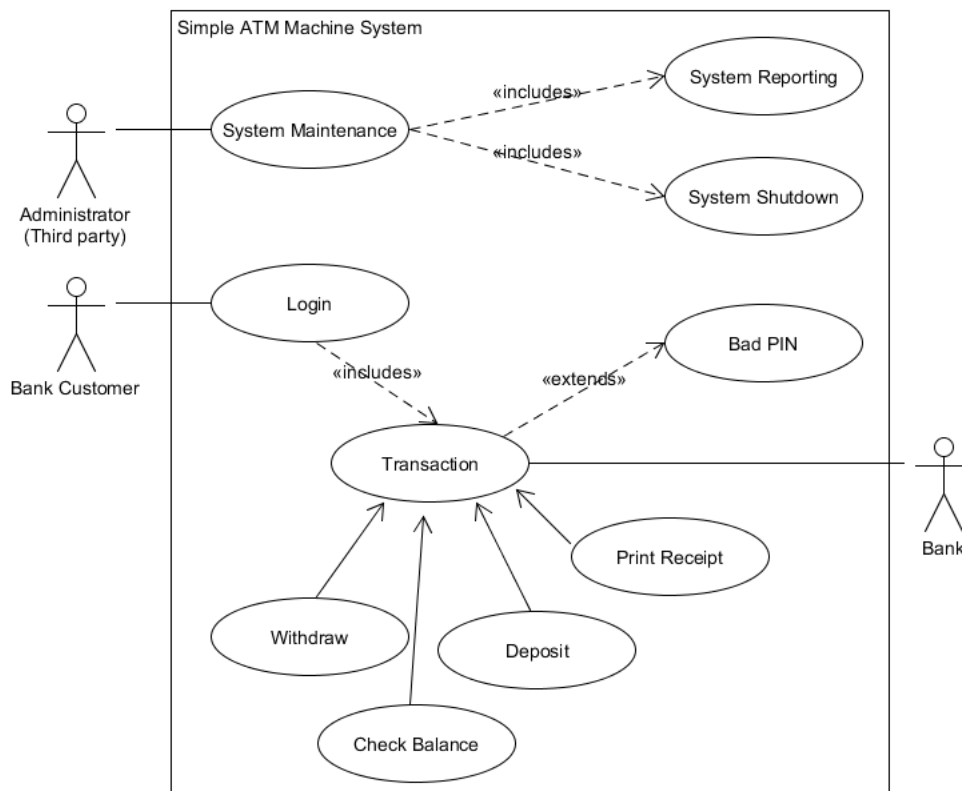


Figure A.14: UML Use-case Diagram

## Appendix II. BPMN Elements

These are available BPMN elements:

1. Flow Objects: Flow objects define the main graphical representations of business processes. It consists of Events, Activities and Gateways. The following table provides these three elements and their basic notations:

Element	Notation
Event	
Activity	
Gateway	

Table A.1: Elements of Flow objects

- a) *Event*: Event is something that occurs during the lifetime of a process. An event can be triggered by another process (a.k.a. *catch*). Otherwise, an event can generate a result (a.k.a. *throw*). There are three types of events based on their occurrence during the process flow - start, intermediate and end. The start event generally initiates a process. There is no “throw” for the start event, and it can only be triggered when necessary. It is indicated by a narrow border, as depicted in Figure A.15. The intermediate event can have either *catch* or *throw* triggers, and it is presented by double border. On the contrary, the end event can only generate a result, and it is always drawn with a thick border. In addition, there are different types of events that can be categorized in these three general events. The following figure describes those events and their notations:

Events	Start	Intermediate	End
	Catching	Throwing	
Message			
Timer			
Error			
Escalation			
Cancel			
Compensation			
Conditional			
Link			
Signal			
Terminate			
Multiple			
Parallel Multiple			

Figure A.15: Notation of different events



As the BPMN 2.0 standard illustrated, the markers are unfilled for catching triggers. On the other hand, the throwing result markers are filled.

- b) **Activity:** Activity is something that the company performs in a process. It can be atomic task or non-atomic sub-process. The task is generally used when the details of the process is not presented. There is a choreography task notation which represents the message exchange between two or more participants (or business entities) for a single task.

The sub-process notation is used when the details of the process is given in finer details. When multiple participants (or business entities) are involved in information exchange for a process, we need to use sub-choreography notation for that process. There are two types of notation for sub-process or sub-choreography- collapsed and expanded. Collapsed sub-process or sub-choreography is indicated by a *plus* sign inside the rounded rectangle, which suggests that there exists a lower level of details. However, the expanded sub-process or sub-choreography provides the details within its boundary. But one thing we have to consider that no sequence flows can cross the boundary of the expanded sub-process or sub-choreography. Table A.2 describes the notation of different activities:

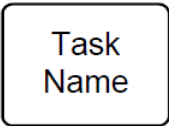
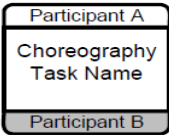
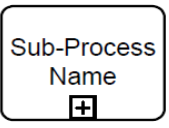
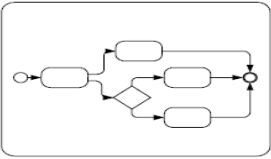
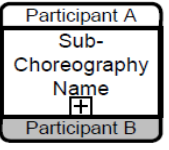
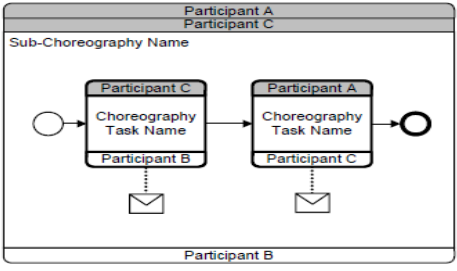
Element	Notation
Task	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>Task</p> </div> <div style="text-align: center;">  <p>Choreography Task</p> </div> </div>
sub-process	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>Collapsed</p> </div> <div style="text-align: center;">  <p>Expanded</p> </div> </div>
sub-choreography	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>Collapsed</p> </div> <div style="text-align: center;">  <p>Expanded</p> </div> </div>

Table A.2: Notation of different Activities

- c) **Gateway:** Gateway controls the sequence flows in a process. It can represent merging, forking, branching or joining of sequence flow paths. Exclusive Gateway is used in a situation where only one of the alternative paths needs to be taken based on a condition, like *if-else* statement in programming language. Inclusive Gateway

evaluates all alternative paths, like independent *if* statement in programming language. Event based Gateway is used when an event initiates the merging or forking. The event that activates the gateway can be controlled by another process. Parallel Gateway follows parallel paths without evaluating any condition. Complex Gateway is used for complex situations that cannot be represented by other Gateways.

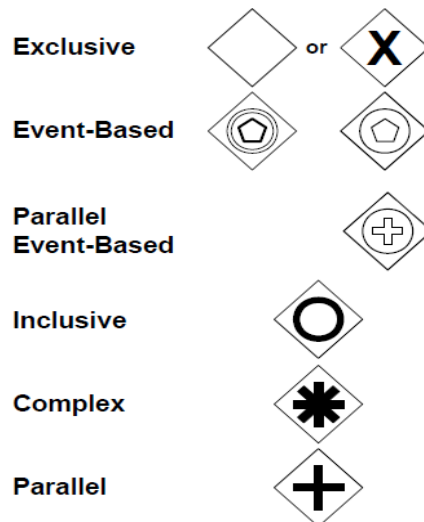


Figure A.16: Notation of different gateways

2. **Data:** A process requires data or generates data during its operation. Data objects can be a single data object or a collection of data object. It can also represent data input to an activity, or data output and data store by an activity. Data store is usually the place from where an activity can retrieve data or store data in persistent way. The notations for different data objects are:

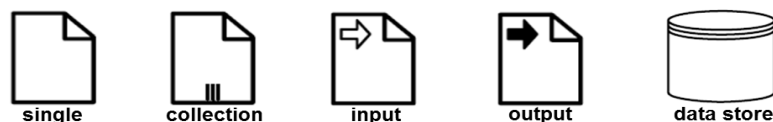


Figure A.17: Notation of different data objects

3. **Connecting Objects:** To produce a flowchart like graphical representation in BPMN, we need to connect the flow objects. There are four type of connecting objects that can connect flow objects- sequence flows, message flows, associations and data associations. Sequence flow connects activities to show the order of their operation in a process. There are several sequence flows. Normal sequence flow connects flow objects, but it does not start from an intermediate event. Uncontrolled sequence flow is used without any condition or gateway. Conditional sequence flow is used when the flow leaves an activity based on some conditional expression. Besides, we need to use default sequence flow mainly in alternative paths when the last path is chosen because of all other conditional flows are not true (mainly with exclusive and inclusive gateways). Exception sequence flow is the opposite of normal sequence flow, so it is the outgoing flow from an intermediate event which is attached to the boundary of an activity.

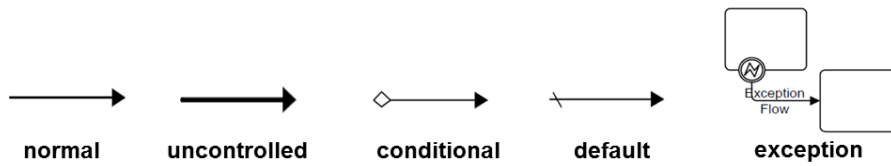


Figure A.18: Notation of different sequence flows

Message flow is used between two participants to show the exchange of information, and associations are used to link information or artefacts (additional information about the Process) to graphical elements of the diagram. There is a notation for compensation association that act like the exception sequence flow but only for association purposes.



Figure A.19: Notation of message flow and association

4. **Swim lanes:** Swim lanes help to create groups of the modelling elements. There are two types of grouping mechanism in swim lanes- pools and lanes. A pool acts like a container for a set of activities with sequence flows, that means sequence flows cannot cross the boundary of a pool, but message flows can cross the boundary. A pool can provide internal details (a.k.a., white box) or it can be empty (a.k.a., black box). Whereas a lane is used to partition a pool to organize or categorize the activities. A lane can be aligned vertically or horizontally through the length of entire process level.

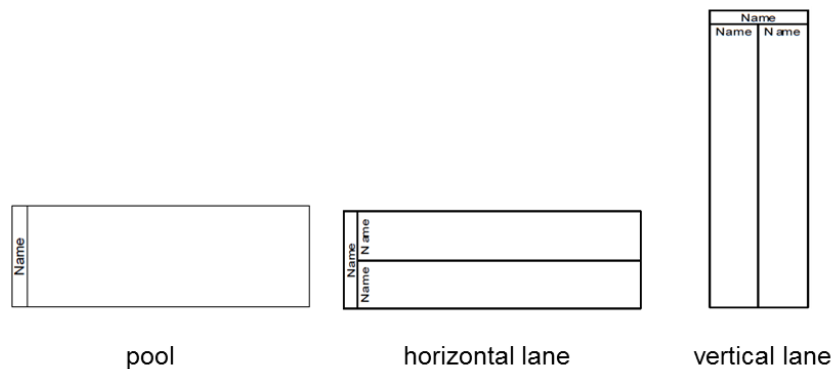


Figure A.20: Notation of pool and lane

5. **Artefacts:** Artefact supplies additional information about a process. The standard provides two artefacts- Group and Annotation. Group helps to collect elements of similar categories, but it does not restrict sequence flows within the group. Annotation helps to provide additional information regarding the diagram.

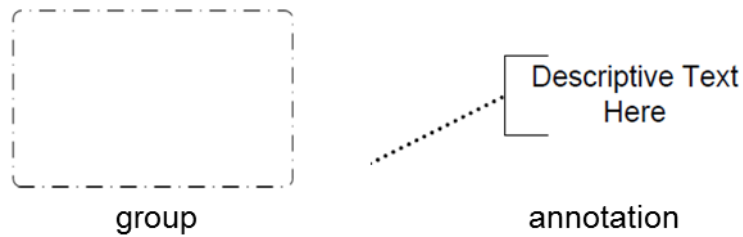


Figure A.21: Notation of group and annotation artefacts

In addition there are other elements in the BPMN 2.0 notation model that are used very often in designing business model. The widely used notations from those elements are described below.

Activity looping describes a task or sub-process which is repeated during operation. A small looping sign at the bottom-centre of an activity indicates the repeated behaviour. Also multiple instances of an activity can execute in sequential or parallel mode, and both of them can be represented with specific notations. Sometime a sub-process can be agreed to complete or cancel by all participants, then such activity is described as transaction and represented by a double border activity symbol. Furthermore, there are two off-page connector notations that describe the continuation of the sequence flow in the next page.

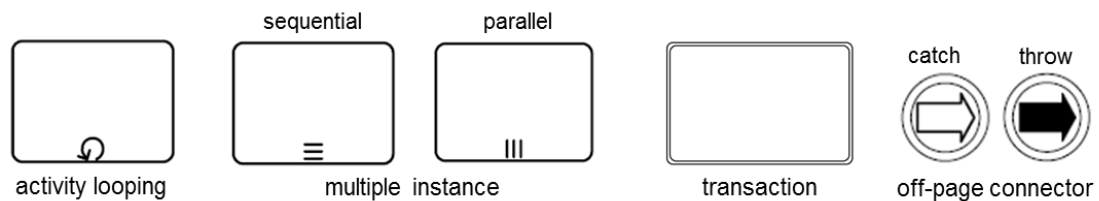


Figure A.22: Notation of different other elements