



A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures

## D6.1 Use cases settings and demonstration strategy (IT-1)

Document Identification			
Status	Final	Due Date	31/08/2021
Version	1.0	Submission Date	01/10/2021

Related WP	WP6	Document Reference	D6.1
Related Deliverable(s)	D2.2	Dissemination Level (*)	PU
Lead Participant	OPT	Lead Author	Antonis Gonos
Contributors	ATOS, SYN, TID, SONAE, ALTRAN, UMinho, XLAB, TUBS, POLITO	Reviewers	Antonio Pastor, TID
			Panagiotis Karkazis, SYN

### Keywords:

Pilot scenario, validation methodology, validation metrics, use cases, validation plan, pilot requirements

This document is issued within the frame and for the purpose of the FISHY project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 952644. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the FISHY Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the FISHY Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the FISHY Partners.

Each FISHY Partner may use this document in conformity with the FISHY Consortium Grant Agreement provisions.

(\*) Dissemination level: **PU**: Public, fully open, e.g. web; **CO**: Confidential, restricted under conditions set out in Model Grant Agreement; **CI**: Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

## Document Information

List of Contributors	
Name	Partner
Joao Pita Costa	XLAB
Lucija Korbar	XLAB
Aleš Černivec	XLAB
Anže Žitnik	XLAB
Jasenska Dizdarevic	TUBS
Panos Trakadas, Panagiotis Athanasoulis	SYN
Ruiz, Jose Francisco	ATOS
Jose Soriano Diaz	ALTRAN
Guillermo Jimenez Prieto	ALTRAN
Henrique Santos	UMINHO
Ana Machado Silva	SONAE
José Duarte	SONAE ARAUCO
Lourdes Luque Canto	TID
Daniele Canavese	POLITO

Document History			
Version	Date	Change editors	Changes
0.1	2021-02-09	Antonis Gonos (OPT)	ToC and initial structure
0.2	2021-02-19	Panagiotis Trakadas	Contribution to section 3.2
0.3	2021-03-19	Ilias Kanakis, Antonis Xagorakis	Integrated inputs from SONAE and ALTRAN
0.4	2021-05-20	Panagiotis Trakadas (SYN), Antonis Xagorakis (OPT)	Inserted contributions for F2F in chapter 3 and 4
0.5	2021-06-30	SONAE, POLITO, ALTRAN	Inserted contributions in WPTVC and SADE use cases
0.6	2021-07-08	Synelixis (Panagiotis Athanasoulis, Panagiotis Karkazis)	Contribution to section 5.2 and 6.2
0.7	2021-07-21	OPT (Ilias Kanakis, Antonis Xagorakis)	Updates to chapters 3, 4, 5 based on decisions made in the last GA
0.8	2021-8-14	OPT	Integrated inputs from SONAE and ALTRAN and comments from TUBS and UPC
0.9	2021-09-30	OPT	Revised version addressing the comments received from internal reviewers (SYN, TID)
1.0	2021-10-01	Jose Francisco Ruiz, Juan Alonso (Atos)	Quality assessment and final version to be submitted.

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	2 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Antonis Gonos (OPT)	30/09/2021
Quality manager	Juan Alonso (ATOS)	01/10/2021
Project Coordinator	Jose Francisco Ruiz (ATOS)	01/10/2021

# Table of Contents

Document Information.....	2
Table of Contents .....	4
List of Tables.....	6
List of Figures .....	8
List of Acronyms .....	9
Executive Summary .....	10
1 Introduction .....	11
1.1 Purpose of the document.....	11
1.2 Relation to other project work packages.....	11
1.3 Structure of the document .....	11
1.4 Glossary adopted in this document and clarification of terms .....	11
2 FISHY platform evaluation methodology .....	13
3 Use case scenario context and description .....	14
3.1 Introduction.....	14
3.2 Farm-to-Fork (F2F) Supply Chain .....	15
3.2.1 Introduction.....	15
3.2.2 Scenarios to be tested/piloted using the FISHY IT-1 .....	16
3.2.3 UML diagram .....	17
3.2.4 UML Use cases.....	18
3.3 Wood-based Panels Trusted Value-Chain (SONAE) .....	22
3.3.1 Introduction.....	22
3.3.2 Scenarios to be tested/piloted using the FISHY IT-1 .....	25
3.3.3 UML diagram .....	26
3.3.4 UML Use cases.....	27
3.4 Securing Autonomous Driving Function at the Edge (SADE) ALTRAN .....	30
3.4.1 Introduction (SADE) .....	30
3.4.2 Scenarios to be tested/piloted using the FISHY IT-1 .....	30
3.4.3 UML Diagrams (SADE).....	31
3.4.4 UML Use cases (SADE) .....	32
4 Business and Technical Validation Metrics .....	35
4.1 Introduction.....	35
4.2 Farm-to-Fork Supply Chain .....	35
4.3 Wood-based Panels Trusted Value-Chain.....	36
4.4 Securing Autonomous Driving Function at the Edge (SADE).....	38
5 Mapping of piloting activities to FISHY offerings.....	41
5.1 Introduction and functionality-to-SC case map .....	41
5.2 Farm-to-Fork Supply Chain .....	41
5.3 Wood-based Panels Trusted Value-Chain.....	43
5.3.1 UC1 – IoT devices management: .....	44
5.3.2 UC2 - Vulnerability Management: .....	44
5.3.3 UC3 – Incident Management: .....	45

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	4 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

5.4	Securing Autonomous Driving Function at the Edge (SADE).....	45
5.4.1	UC1 - ACTIVATION: .....	45
5.4.2	UC2 – POWER ON: .....	46
5.4.3	UC3 – Software Patch Level Certification .....	46
5.4.4	UC4 – Software Patch Level correction.....	48
5.4.5	UC5 – Car compromised .....	48
6	Infrastructure set up .....	49
6.1	Introduction.....	49
6.2	Farm-to-Fork Supply Chain .....	49
6.3	Wood-based Panels Trusted Value-Chain.....	50
6.4	Securing Autonomous Driving Function at the Edge (SADE).....	52
7	Conclusions .....	54
8	References .....	55

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	5 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

## List of Tables

Table 1: Scenario description template .....	14
Table 2: UML-Use case description template .....	15
Table 3: Farm to Form Supply Chain Scenario 1 .....	16
Table 4: UML Use cases FSC_UC1 .....	18
Table 5: UML Use cases FSC_UC2 .....	19
Table 6: UML Use cases FSC_UC3 .....	19
Table 7: UML Use cases FSC_UC4 .....	20
Table 8: UML Use cases FSC_UC5 .....	20
Table 9: UML Use cases FSC_UC6 .....	21
Table 10: UML Use cases FSC_UC7 .....	21
Table 11: UML Use cases FSC_UC8 .....	22
Table 12: Flows of components depicted in Figure 6 .....	24
Table 13: WPTV - Scenario 1 .....	25
Table 14: UML Use cases SON_UC1 .....	27
Table 15: UML Use cases SON_UC2 .....	27
Table 16: UML Use cases SON_UC3 .....	28
Table 17: UML Use cases SON_UC4 .....	28
Table 18: UML Use cases SON_UC5 .....	29
Table 19: UML Use cases SON_UC6 .....	29
Table 20: Securing Autonomous Driving Function at the Edge - Scenario 1 .....	30
Table 21: Securing Autonomous Driving Function at the Edge - Scenario 2 .....	31
Table 22: UML Use cases SADE_UC1 .....	32
Table 23: UML Use cases SADE_UC2 .....	32
Table 24: UML Use cases SADE_UC3 .....	33
Table 25: UML Use cases SADE_UC4 .....	33
Table 26: UML Use cases SADE_UC5 .....	34
Table 27: Template of validation metric description .....	35
Table 28: Farm-to-Fork Supply Chain; Metric description SC1_B1 .....	35
Table 29: Farm-to-Fork Supply Chain; Metric description SC1_T1 .....	36
Table 30: Wood-based Panels Trusted Value-Chain; Metric description SC1_B1 .....	36
Table 31: Wood-based Panels Trusted Value-Chain; Metric description SC1_B2 .....	37
Table 32: Wood-based Panels Trusted Value-Chain; Metric description SC1_B3 .....	38
Table 33: SADE; Metric description SC1_T1 .....	38
Table 34: SADE; Metric description SC1_T2 .....	39
Table 35: SADE; Metric description SC1_T3 .....	39
Table 36: SADE; Metric description SC1_B1 .....	40
Table 37: Mapping of FISHY functionalities/offerings to supply chain cases .....	41
Table 38. Equipment used in F2F PoC prototype .....	49

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	6 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

*Table 39. Equipment and services (Wood-based Panels Trusted Value-Chain)..... 51*

*Table 40. Some of the Equipment embedded in the vehicle ..... 53*

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	7 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## List of Figures

<i>Figure 1: the evaluation methodology that will be executed in WP6 based on inputs from WP2 – WP5.....</i>	<i>13</i>
<i>Figure 2: The lifecycle of the products in the “Farm to Fork” supply chain.....</i>	<i>16</i>
<i>Figure 3: UML diagram for the Farm to Form supply chain case .....</i>	<i>18</i>
<i>Figure 4: End-to-End Melamine Supply Chain process and flows at Sonae Arauco.....</i>	<i>23</i>
<i>Figure 5: Sketch of the Connected Factory architecture at Sonae Arauco.....</i>	<i>23</i>
<i>Figure 6: Data Flows in IoT Platform .....</i>	<i>24</i>
<i>Figure 7: UML diagram for the WPTV supply chain case .....</i>	<i>26</i>
<i>Figure 8: UML diagram of SADE use cases.....</i>	<i>31</i>
<i>Figure 9: The F2F platform and its interconnection with the FISHY platform.....</i>	<i>41</i>
<i>Figure 10: The Connected Factory architecture and its interconnection with the FISHY platform.....</i>	<i>43</i>
<i>Figure 11: Sonae Arauco use case 1 flow .....</i>	<i>44</i>
<i>Figure 12: Sonae Arauco use case 2 flow .....</i>	<i>44</i>
<i>Figure 13: Sonae Arauco use case 3 flow .....</i>	<i>45</i>
<i>Figure 14 – SADE Use Case 3 (flow).....</i>	<i>46</i>

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	8 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final



## List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
B2B	Business to Business
D6.1	Deliverable number 1 belonging to WP6
DLT	Distributed Ledger Technologies
DoA	Description of Action
EC	European Commission
EIM	Exploitation and Innovation Manager
ER	Exploitable Result
EPO	European Patent Office
F2F	Farm to Fork
GA	Grant Agreement
HPC	High Performance Computing
IGT	Impact Generation Team
IoT	Internet of Things
IT	Information Technology
KPIs	Key Performance Indicators
OEM	Original Equipment Manufacturer
PoC	Proof of Concept
SACM	Security Audit and Certification Manager
SADE	Securing Autonomous Driving Function at the Edge
SPI	Secure Data and Privacy Infrastructure
TIM	Trust and Intent Manager
UC	Use case
UI	User Interface
UML	Unified Modeling Language
WPTV	Wood-based Panels Trusted Value-Chain

## Executive Summary

---

This deliverable presents the evaluation methodology of the FISHY project and describes in detail the scenarios and tests that will be run, using the first iteration of the FISHY platform (which will be delivered in M15). It is the first deliverable of WP6 reporting the work of tasks 6.1 and 6.2 in the first year of the project lifetime.

This deliverable starts with the evaluation methodology that is adopted throughout the FISHY project lifetime and then proceeds to the details of the test scenarios to be run with the IT-1 version of FISHY platform. These scenarios are used to extract Unified Modeling Language (UML)-compliant use cases which will also help in the testing of the various functionalities of the FISHY platform. Then, we also detail the metrics, which will be measured during the pilot tests. In the description of the scenarios, FISHY platform has been considered as a “black-box”, i.e. as a solution offering specific functionalities, which are to be evaluated. However, as WP6 scope is to evaluate FISHY, the FISHY functionalities that are assessed in each scenario are identified to ensure. This allows better synchronisation with WP2 regarding the interfaces and specifications of the FISHY platform and components. Furthermore, the setup of the infrastructure in each of the three FISHY pilot cases is outlined paving the way for integration with the FISHY platform IT-1.

It is worth stressing that the scenarios and metrics defined in this deliverable refer to the first phase of testing. Additional scenarios will be defined and tested in the second piloting round and will be reported in subsequent deliverables.

This deliverable is a roadmap which provides the information for the first pilot round of the FISHY IT-1 platform. It can be considered as the liaison between WP2 (that defines the functionality and interfaces) and WP5 (which provides the integrated FISHY platform).

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	10 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

# 1 Introduction

---

## 1.1 Purpose of the document

---

This deliverable provides a description of the scenario context and infrastructure set-up for the three use cases, as well as the strategy and plan for the validation of the FISHY platform IT-1. This document is an outcome of task 6.1 and task 6.2. The task 6.1 is titled “Use Cases Requirements and Holistic Demonstration Concept” and for each use case it elicits detailed requirements and respective scenarios. It consequently produces the demonstration concept and a clear validation plan, considering the expected outcomes from the technical WPs. The use cases are described in detail, and we show how the validation will be conducted in the respective pilot testbeds. Task 6.2 focuses on the setup of the pilot use case environment along with required applications, by bringing together the technical implementations and the deployment configurations carried out in the technical WPs.

An update of this deliverable will be prepared and submitted in M24 after the IT-1 version of the FISHY platform has been released.

## 1.2 Relation to other project work packages

---

This deliverable highly interrelates with D2.2 [1] as D2.2 describes the architectural framework of the FISHY platform and presents the requirements of the FISHY exemplar use cases. It also relates to and provides input to WP5, which will integrate the FISHY platform and to the subsequent tasks of WP6 where the FISHY platform validation activities take place.

## 1.3 Structure of the document

---

This document is organised in the following major chapters:

- **Chapter 2:** Evaluation Methodology: this chapter describes the methodology we follow in this work package towards the evaluation of the FISHY platform in pilot use cases.
- **Chapter 3:** Use case scenario context and description. This chapter describes the scenarios that will be tested and analyses them to produce UML diagrams.
- **Chapter 4:** Technical and Business Validation Metrics. This chapter describes the metrics that are targeted by IT-1 of the FISHY platform in each pilot site/case and their relevance to the FISHY project Key Performance Indicators (KPIs) indicated on the DoA.
- **Chapter 5:** Mapping of piloting activities to FISHY offerings. This chapter describes the FISHY offerings/functionalities tested per FISHY use case and additionally, it describes the information that is exchanged between the FISHY platform and each (of the three) supply chain IT system/solution. In other words, it describes the security probes for each use case.
- **Chapter 6:** Infrastructure set up. In this chapter, we describe the infrastructure set up at each of the three pilot sites.
- **Chapter 7** Conclusions. This chapter provides the conclusions of this deliverable.

## 1.4 Glossary adopted in this document and clarification of terms

---

In this section we clarify that:

- **FISHY use case:** FISHY has selected and described in its DoA three different supply chains (F2F, WPTV and SADE) which can use/exploit the FISHY platform. FISHY includes in its consortium

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)				Page:	11 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

appropriate partners to pilot and test the FISHY platform in one instance of each considered supply chain. Namely, Optimum and Synelixis for the piloting of the F2F use case, SONAE for the piloting of the WPTV use case and Capgemini Engineering (ex. ALTRAN) for the piloting of the SADE use case.

- **UC-Use Case.** In this deliverable, the acronym UC refers to the formally described “use cases” as they are defined using the Unified modelling language (UML). We studied the use of the FISHY and came up with UML diagrams for each FISHY use case in order to capture detailed requirements and rigorously define elaborate (UML-compliant) use cases that would drive the testing of the FISHY platform and its components. For this purpose, we try to differentiate it from the FISHY use cases which are in essence supply chain instances using FISHY platform. In many cases, to stress the difference we refer to FISHY use case vs. UML-compliant use cases.

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)				Page:	12 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status: Final

## 2 FISHY platform evaluation methodology

FISHY consortium has decided to follow an iterative development and validation strategy. Namely,

**Step 1:** Thorough investigation of the requirements of the three FISHY use cases (Farm to Fork, Wood-based Panels Trusted Value-Chain and Securing Autonomous Driving Function at the Edge) to capture use case relevant requirements, (which are listed in D2.2 [1]).

**Step 2:** Detailed definition of scenarios that enable the assessment of the level at which the FISHY platform developed in the technical WPs (WP2-WP5) meet the requirements listed in D2.2 and the ambitions described in the DoA. It should be mentioned at this point that the scenarios described in this document focus on the functionality that will be included and supported by IT-1 release. It is in this step that we also include the definition of the validation metrics which allow the assessment of the level at which the FISHY use case requirements are met by IT-1 release.

**Step 3:** Pilot activities in each FISHY pilot site. This includes the deployment of the necessary infrastructure, of the FISHY platform and the execution of the scenarios defined in step 2.

**Step 4:** Feedback is collected from the piloting activities. It is analysed and the comments/bugs/suggestion for improvements are fed back to a) the architecture and implementation focusing work-packages and b) to the evaluation scenario definition for their revision to define and support the 2<sup>nd</sup> version of piloting activities which will focus on IT-2 release.

**Step 5:** 2<sup>nd</sup> round- evaluation scenario definition (It is the 2<sup>nd</sup> execution of step 2 taking into consideration the feedback of the 1<sup>st</sup> piloting round).

**Step 6:** Pilot activities using the IT-2 release of the FISHY platform which will include the final set of components and functionality and execute the scenarios defined in step 5.

**Step 7:** final feedback collection so as to a) formulate the value proposition of the FISHY platform and b) define the development needs towards the commercialisation of the platform.

The steps are indicated in the following figure where those carried out solely in WP6 are marked in dark blue. In each box, two numbers are shown corresponding to the 1<sup>st</sup> and 2<sup>nd</sup> piloting phase. It should be stressed that the first two steps have been implemented by the delivery date of this deliverables and the pilot activities will take place in the time span M15-M18. The 2<sup>nd</sup> pilot round we take place from M19 till the project end.

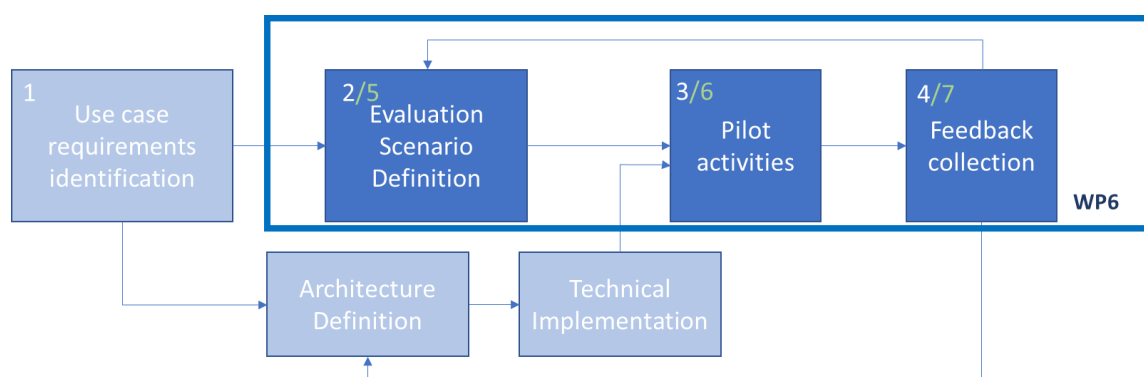


Figure 1: the evaluation methodology that will be executed in WP6 based on inputs from WP2 – WP5.

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)				Page:	13 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

## 3 Use case scenario context and description

### 3.1 Introduction

In this chapter, for each of the three FiSHY use cases, we define:

1. The scenario(s) of interest which demonstrates the value of the FiSHY for the specific supply chain case
2. The UML diagram which shows the involved actors, the UML-defined use cases and the interactions between them; while the “actors” in UML diagrams can be either humans or systems, in this chapter the “actors” refer to (human) users.
3. The description of the elements of the UML diagram (i.e. the UML-compliant use cases describing how the actors interact with the FiSHY platform and components).

In the sequel we present the template designed for the description of each scenario (see Table 1) and for the description of each UML-compliant use case. We should also mention that information about the three FiSHY use case and how they operate can also be found in D2.2, in the chapter devoted to the requirement extraction and more precisely, in the description of the storyline. Additionally, in the Services/Functionalities entry of the table describing the scenario, the component named and specified in D2.2 are referenced.

**Table 1: Scenario description template**

SCENARIO	<scenario name> (ex. Food Quality Monitoring)
History	Version of the documented scenario (e.g., v0.1)
Key Actors	< List of actors involved in the scenario> (e.g., Producer, transporter A, warehouse employee)
Assumptions / Dependencies	List of dependencies (e.g. <ul style="list-style-type: none"> <li>• All business companies have registered in FiSHY platform.</li> <li>• IoT platforms are installed and running)</li> </ul>
Objective(s)	<List of the objectives of the scenario> (e.g. <ul style="list-style-type: none"> <li>• Respect the privacy requirements of the involved actors and organizations and guarantee the integrity of the exchanged data.</li> <li>• Collect, filter and manage data and metadata from various IoT environments and other data entry points (i.e. web application).)</li> </ul>
Description	Description of the scenario in steps so that each one can be verified during piloting. For example, <p>Step 1) The producer owns a field, ...</p> <p>Step 2) When the producer’s goods are ready to be transported....</p> <p>Step 3) Transporter A drives the vehicle to the Warehouse (WH).</p> <p>Step 4) When one or more boxes should be transferred from y.</p> <p>Step 5) A customer scans.</p>
Services/Functionalities	FiSHY functionalities enacted.
Metrics	List of metrics to be measured during the testing of the scenario starting from DoA

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	14 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

**Table 2: UML-Use case description template**

USE CASE Description	
<b>ID</b>	Identifier of type A_UCB where A is indicating the FISHY supply chain acronym and B is an ascending number. Example FSC_UC1
<b>Name</b>	Descriptive name (e.g. Register farm system_
<b>Actors</b>	(Human) user involved in the this UML use case e.g. Producer
<b>Storyline</b>	text
<b>Trigger events</b>	The event that triggers the execution of this use case (e.g. A new item has been registered in the platform)
<b>Preconditions</b>	A required precondition so that the use case is appropriately executed (e.g. The registration components is deployed)
<b>Postconditions</b>	The condition -outcome of the use case (e.g. The item table is updated.)
<b>Related scenarios</b>	List of scenarios where this use case is enacted (e.g. scenario 1, scenario 2)

## 3.2 Farm-to-Fork (F2F) Supply Chain

### 3.2.1 Introduction

In this section, we describe the scenarios that will be carried out in the first round of piloting with IT-1 (i.e. M15-M18) relevant to the Farm-to-Fork supply chain. In this particular agricultural supply chain scenario, all interested stakeholders will be able to receive information about the conditions under which the products have been cultivated, stored and transported during their entire lifetime. For the purposes of FISHY and in line with their expertise and interest, the involved partners will offer: SynField IoT system collecting information from the farm, IoT system from the transportation company and IoT systems from the warehouse (e.g., Aberon).

The following figure (Figure 2) illustrates the lifecycle of agri-food products, from their production to consumption point. Such lifecycle is quite complex and involves a large number of actors and services and may generate a vast amount of data. For example, inside the farm, a perishable product could generate large volumes of related data (e.g., environmental conditions, utilization of fertilizers, date of plantation and harvest, water resources spent). During transportation, data related to the preservation conditions (refrigerator temperature and humidity), shipment details and truck route (GPS data) until final destination can be traced and stored in a distributed ledger, excluding the possibility of non-repudiation. Additionally, data can be created in other intermediary places, such as distribution centers, keeping data with respect to warehouse conditions, final destination, responsible employee, etc. Finally, all the data can be processed, and made available to consumers in the supermarkets.

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	15 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

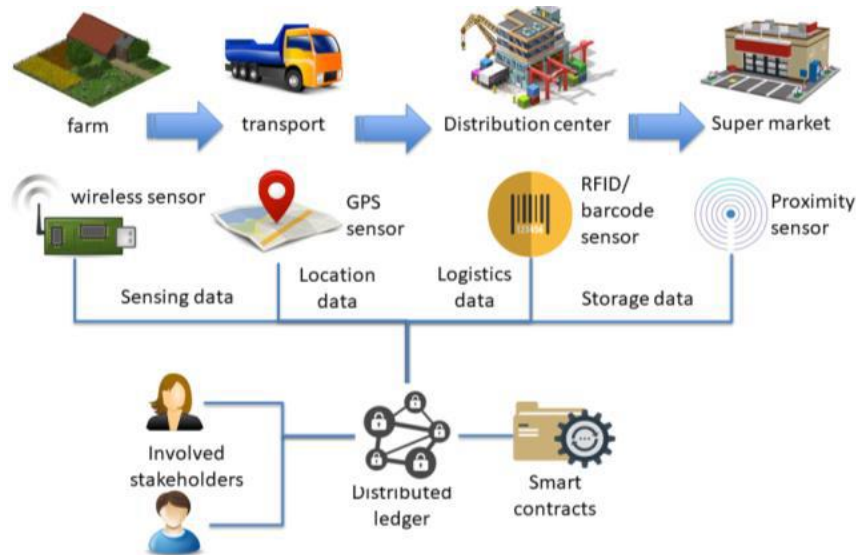


Figure 2: The lifecycle of the products in the “Farm to Fork” supply chain

### 3.2.2 Scenarios to be tested/piloted using the FISHY IT-1

The scenario that will be tested using the IT-1 FISHY platform is described in the following table. It is worth clarifying that:

- In the F2F supply chain that Optimum and Synelixis currently operate, the data from the various IoT islands are stored in different Distributed ledgers (Blockchain based ledgers) which mandates exchange of data between them. For this purpose, the FISHY platform needs to support “interledger” technologies, i.e. to support the monitoring and protection of systems involving more than one blockchain ledger.
- In the F2F supply chain, an F2F web app that supports the farmer, the transporter, the warehouse keeper and the consumer to insert and/or inspect different pieces of information relevant to a specific product (e.g. table grapes) already exists. This is the interface between the user and the IT solution the Optimum and Synelixis operate. Further information on this can be found in D2.2, in the requirement extraction chapter, in the description of the storyline.

Table 3: Farm to Form Supply Chain Scenario 1

SCENARIO	Data sharing in Farm to Fork involving interledger technologies
History	v0.1
Key Actors	Producer, transporter, warehouse employee, consumer
Assumptions / Dependencies	<ul style="list-style-type: none"> <li>• The farmer, the transporter, the warehouse keeper and the consumer are registered in the F2F web app.</li> <li>• The administrators of the three IoT platforms (described below) have installed, run and have registered in the FISHY platform the: <ul style="list-style-type: none"> <li>○ SynField field nodes and Cloud platform</li> <li>○ Transportation platform with boxes equipped with RFID tags, and vehicles equipped with RFID readers and temperature sensors</li> <li>○ IoT platform that monitors temperature in storage rooms</li> </ul> </li> </ul>

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)	Page:	16 of 55
Reference:	D6.1	Dissemination:	PU
		Version:	1.0
		Status:	Final



	<ul style="list-style-type: none"> <li>FISHY platform components have been installed and are running.</li> <li>FISHY IRO and dashboard are operational, and actors have been registered.</li> </ul>
<b>Objective(s)</b>	To validate FISHY threat detection mechanisms for evidence-based data sharing implementing interledger components supporting at least two interledger technologies
<b>Description</b>	<p>Steps 1-4 refer to the appropriate set up and use of the F2F web application which uses data from three IT systems.</p> <p>Step 1) SynField IoT island (through a gateway) is connected to a blockchain network of a certain technology (e.g. Ethereum) in the so-called “consortium ledger” and stores information about the temperature and soil humidity in Nemea vineyards.</p> <p>Step 2) the grapes are packed and an RFID tag is attached to the box. The employee uses a F2F web application to associate the RFID tag with the information of the specific vineyard.</p> <p>Step 3) the transportation company employee scans the RFID and associates it with the truck that is used. The information relevant to the truck (e.g. temperature throughout the travel to the warehouse) is also stored in the consortium ledger.</p> <p>Step 4) the transportation company employee delivers the box of grapes to the warehouse employee who inserts the box in the warehouse. Using an RFID reader, he associates the box to the warehouse location and conditions. All the information relevant to the box is now transferred to the public DLT (which is a different blockchain ledger). In this step, the interledger component (shown in chapter 4) is enacted.</p> <p>Step 5) The consumer wants to access all the history of the product. He scans the RFID and now the information generated by the IT systems of different organisations has to be accessed. At the same time, the FISHY platform notifies him of the security level of the gathered information.</p> <p>Step 6) a security threat/attack is issued/detected. Such an attack can be an (adverse) device trying to authenticate in the solution or a compromised hash attack. (For further details see chapter 4).</p> <p>Step 7) the FISHY detects the threat/attack and notifies the appropriate user (IoT platform administrator).</p>
<b>Services/Functionalities</b>	SACM, TIM, SPI functionalities enacted
<b>Metrics</b>	≥2 interledger technologies

### 3.2.3 UML diagram

The UML diagram shown in figure 3 depicts the use cases involved in the F2F supply chain scenarios described above. We mark in blue the use cases relevant to the FISHY platform and in black the use cases involved in the F2F web app that enables the monitoring of information across the supply chain. The latter are also included for completeness reasons mainly. Before any scenario is executed the three

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	17 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final



Table 5: UML Use cases FSC\_UC2

USE CASE Description	
<b>ID</b>	FSC_UC2
<b>Name</b>	Register truck and sensors
<b>Actors</b>	Administrator of the IoT system of the transportation company
<b>Storyline</b>	The administrator of the IoT system of the transportation company registers the IoT system including the truck (e.g. plate number), the sensors (GPS, temperature) the vehicle carries and the cloud server /blockchain ledger where the information is kept.
<b>Trigger events</b>	New IoT system in the supply chain
<b>Preconditions</b>	The transportation company has pursued a web application that associated vehicle plates with sensors for the monitoring of the conditions and routes of the fleet.
<b>Postconditions</b>	The truck and relevant sensors are registered and associated in the application.
<b>Related scenarios</b>	scenario 1

Table 6: UML Use cases FSC\_UC3

USE CASE Description	
<b>ID</b>	FSC_UC3
<b>Name</b>	Register IoT system of the warehouse
<b>Actors</b>	Administrator of the Warehouse IoT system
<b>Storyline</b>	The warehouse IoT administrator registers in the FISHY platform the IoT system (e.g. Aberon) that is in place in the warehouse. This includes the sensors (RFID reader, temperature sensors) and the backend (cloud and blockchain network) where the information collected from the sensors is stored.
<b>Trigger events</b>	New IoT system installed in the warehouse and becomes part of the supply chain.
<b>Preconditions</b>	The warehouse IoT system is installed.
<b>Postconditions</b>	The warehouse IoT system are registered in the FISHY platform.
<b>Related scenarios</b>	scenario 1

Table 7: UML Use cases FSC\_UC4

USE CASE Description	
<b>ID</b>	FSC_UC4
<b>Name</b>	Inspect security level and threats
<b>Actors</b>	Administrator of IoT system (of farm or of transportation company or of warehouse)
<b>Storyline</b>	The actor (any of the above types) enters the platform with an RFID tag at hand. He is interested in inspecting the security conditions/level of the involved IoT systems. He enters FISHY platform and he can get information about the security level of all the systems involved in the farm-to-fork journey of the specific good. If no violation of the IoT system has happened and the relevant system is highly secure, then the replacement should be done immediately. Otherwise, the situation is arguable.
<b>Trigger events</b>	The actor enters the FISHY platform with an RFID tag at hand.
<b>Preconditions</b>	All IoT solutions of the supply chain are connected with FISHY platform The use has an RFID tag at hand FISHY platform operates from the time the good with the specific RFID tag was first inserted in the platform
<b>Postconditions</b>	Report about the security status in this chain is compromised or not
<b>Related scenarios</b>	Scenario 1

Table 8: UML Use cases FSC\_UC5

USE CASE Description	
<b>ID</b>	FSC_UC5
<b>Name</b>	Associate goods and relevant info
<b>Actors</b>	Producer/farmer
<b>Storyline</b>	The producer inserts grapes in boxes which carry in RFID. Through a web application the RFID is associated with the farm part where this set of grapes has been cultivated.
<b>Trigger events</b>	RFID attached to box containing grapes (specific goods).
<b>Preconditions</b>	Farm IoT system and part have been registered and relevant information exists in the data base.
<b>Postconditions</b>	The RFID tag has been associated with information relevant to farm part.
<b>Related scenarios</b>	Scenario 1

Table 9: UML Use cases FSC\_UC6

USE CASE Description	
<b>ID</b>	FSC_UC6
<b>Name</b>	Associate RFID with truck
<b>Actors</b>	Transportation company employee
<b>Storyline</b>	The employee receives the boxes from the producer. Each box has the RFID the producer attached to it. The transportation company employee uses a web application and an RFID reader to scan the RFID and associate it with the specific truck that will be used for its transportation.
<b>Trigger events</b>	RFID reading during the exchange between producer and transportation employee.
<b>Preconditions</b>	The transportation employee has access to the web application and the RFID reader. The truck ID (plate) and the relevant sensors have been registered.
<b>Postconditions</b>	The RFID of the box is associated with the truck identifier.
<b>Related scenarios</b>	scenario 1

Table 10: UML Use cases FSC\_UC7

USE CASE Description	
<b>ID</b>	FSC_UC7
<b>Name</b>	Associate RFID with warehouse parts
<b>Actors</b>	Warehouse keeper
<b>Storyline</b>	The employee of the warehouse, upon reception of new boxes containing goods, scans the RFID of the boxes and associates them with the part of the warehouse where these will be kept so that the conditions of storage can be appropriately associated.
<b>Trigger events</b>	New boxes arrive in the warehouse and the RFID reader scans them.
<b>Preconditions</b>	RFID tags are attached to the boxes and Warehouse parts are registered in the platform.
<b>Postconditions</b>	RFID tags and warehouse parts are associated.
<b>Related scenarios</b>	scenario 1

Table 11: UML Use cases FSC\_UC8

USE CASE Description	
<b>ID</b>	FSC_UC8
<b>Name</b>	Access all info about a specific RFID
<b>Actors</b>	Consumer
<b>Storyline</b>	The consumer inspects the product found on a shelf and scans the RFID. The information about the grapes he is about to purchase from the farm, the truck and the warehouse appears on this screen.
<b>Trigger events</b>	Scan RFID with mobile phone.
<b>Preconditions</b>	<p>The consumer is registered in the application.</p> <p>The IT solution of the farmer delivers information to the F2F scan application.</p> <p>The IT solution of the transportation company delivers information to the F2F scan application.</p> <p>The IT solution of the warehouse company delivers information to the F2F scan application.</p> <p>The RFID is used as the identified so as to retrieve the information.</p>
<b>Postconditions</b>	<p>The F2F application shows all the information to the consumer.</p> <p>The consumer can check if the conditions were appropriate or not, thus performing a kind of auditing of the overall process. The application provides a pdf copy of the results.</p>
<b>Related scenarios</b>	scenario 1

### 3.3 Wood-based Panels Trusted Value-Chain (SONAE)

#### 3.3.1 Introduction

This section details the scenario and use-cases considered for the Wood-based Panels Trusted Value-Chain testing during iteration 1 of the FiSHY validation.

This validation will focus on an End-to-End Supply Chain process at Sonae Arauco, specifically the one that considers the melamine surfaced panels production, as detailed below.

The key relevant business processes identified by Sonae Arauco for FiSHY are presented in Figure 4 and consist of:

- Sales Order Management (Melamine surfaced boards) - (Downstream)
- Manufacturing of decorative paper impregnation - (Working in progress)
- Manufacturing of melamine surfaced boards - (Working in progress)
- Raw materials purchase (namely for resins) - (Upstream)

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	22 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

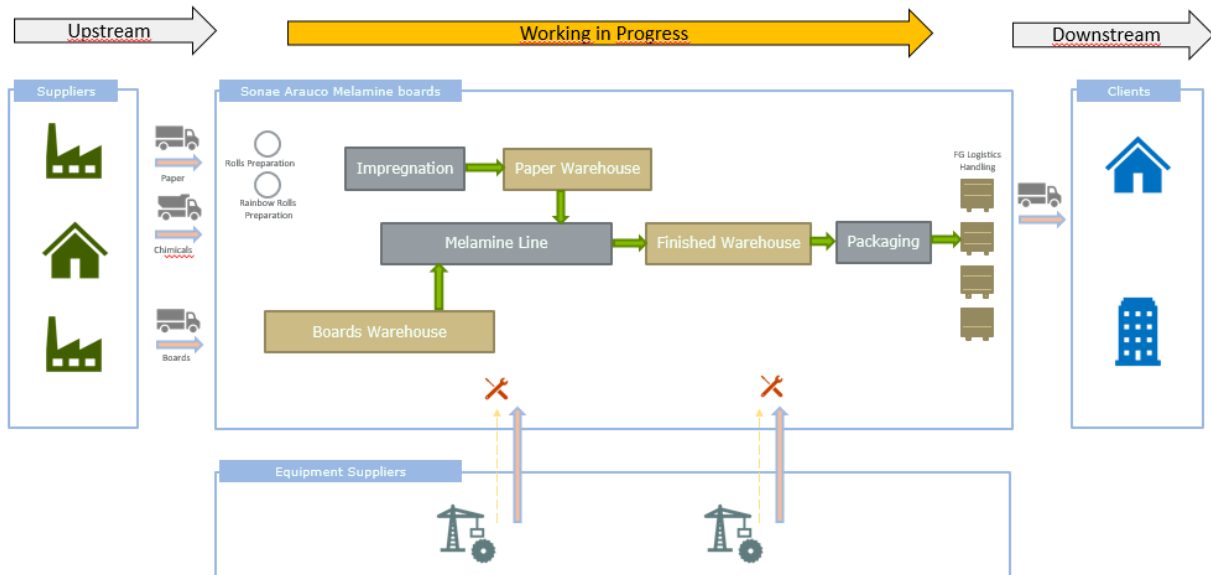


Figure 4: End-to-End Melamine Supply Chain process and flows at Sonae Arauco

For the 1<sup>st</sup> interaction, the use cases defined for FiSHY is based on the existing IOT architecture of the Connected Factory, (shown in Figure 5 and Figure 6), with focus in “working in progress” process.

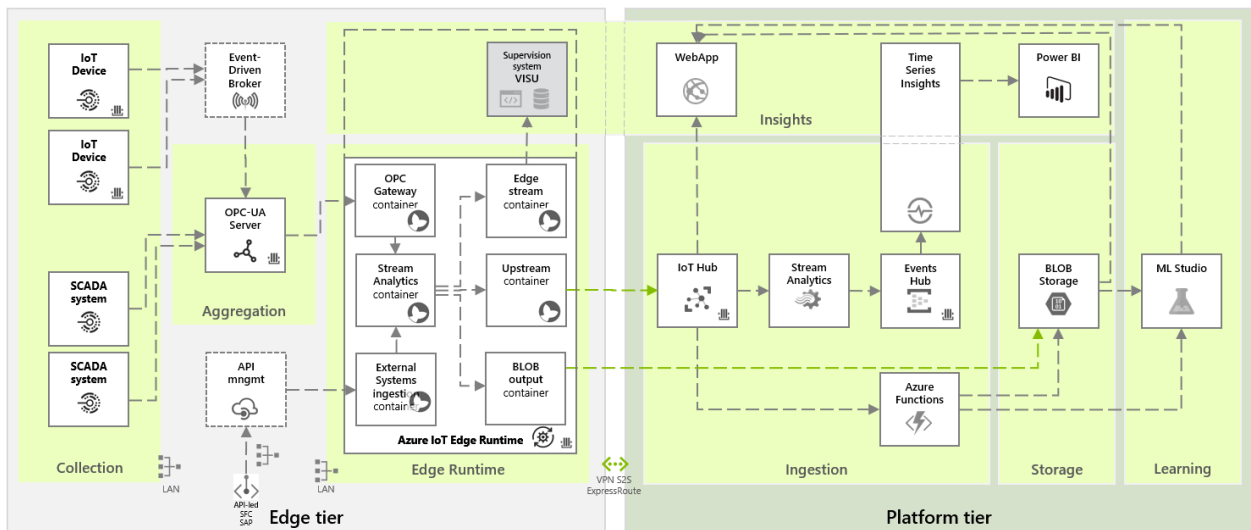
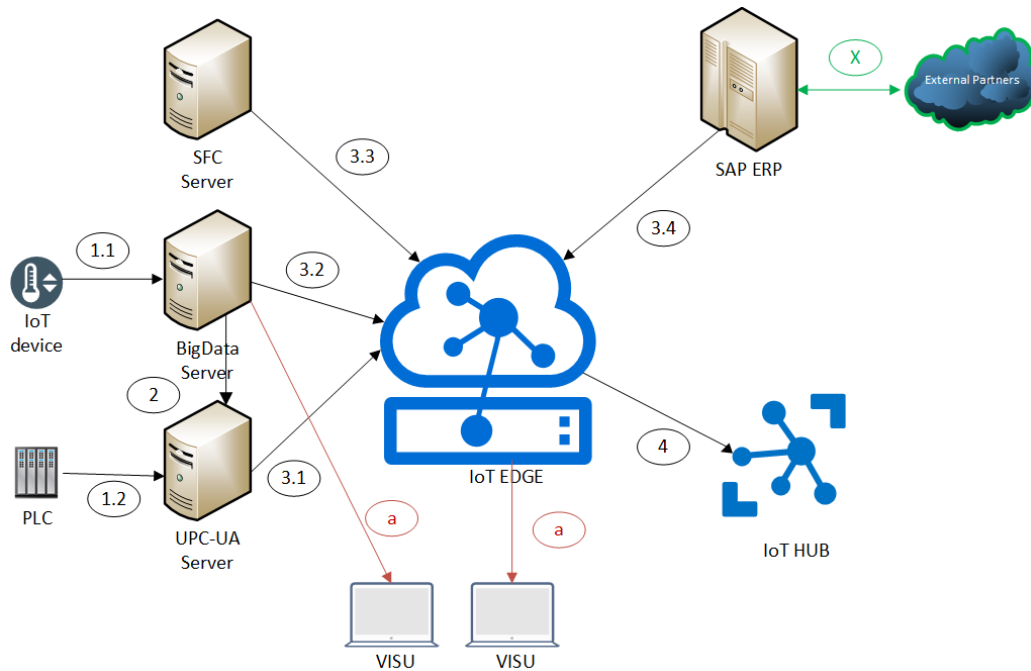


Figure 5: Sketch of the Connected Factory architecture at Sonae Arauco

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)			Page:	23 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status: Final



**Figure 6: Data Flows in IoT Platform**

#### Description of the relevant components in Figure 6:

- SAP ERP Server: Enterprise resource planning (integrated management software of main business processes)
- BigData/VISU Server: On-time Analytics of production figures
- OPC-UA Server: Collects IoT and Industrial automation data (OPC-UA is machine to machine communication protocol for industrial automation)
- SFC Server: Manufacturing Execution System (track and document the transformation of raw materials to finished goods)
- IoT Edge Runtime Server: Collects IoT telemetry and send to Cloud (to IoT Hub Server)
- IoT Hub Server: Collects IoT telemetry from all IoT Edge Servers

Table 12 represents the flows and protocols of the relevant components detailed in Figure 6:

**Table 12: Flows of components depicted in Figure 6**

#	Source	Destination	Protocol/ service	Authentication
1.1	IoT Devices (Devices in dedicated VLAN only reachable by BigData server)	Bigdata Server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	HTTP	No authentication
1.2	PLCs (Devices in industrial VLAN)	OPC-UA Server (Server in dedicated VLAN (Level 3.5 in Purdue Model))		No authentication
2	BigData Server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	OPC-UA server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	Port 1433	Local Database User
3.1	OPC-UA server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	IoT Edge (Server in dedicated VLAN (Level 3.5 in Purdue Model))	OPC	
3.2	Bigdata Server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	IoT Edge (Server in dedicated VLAN (Level 3.5 in Purdue Model))	Port 1433	Local Database User
3.3	SFC Server (Server in dedicated VLAN (Level 3.5 in Purdue Model))	IoT Edge (Server in dedicated VLAN (Level 3.5 in Purdue Model))	Port 152x	Local Database User
3.4	SAP ERP (Server in Main datacenter)	IoT Edge (Server in dedicated VLAN (Level 3.5 in Purdue Model))	Port 152x	Local Database User
4	IoT Edge (Server in dedicated VLAN (Level 3.5 in Purdue Model))	Azure IoT Hub (Public server)	HTTPS	Authentication based in "connection string" (each Hub has dedicated string and ID on Azure)
a	IoT Edge + BigData server	VISU (information dashboards)	HTTPS	
X	External partners	SAP ERP (Server in Main datacenter)	FTP; EDIFACT; IDOC	SAP Users; Operating System users



### 3.3.2 Scenarios to be tested/piloted using the FISHY IT-1

For iteration 1 of the FISHY validation, the chosen scenario is described in Table 13: WPTV - Scenario 1.

**Table 13: WPTV - Scenario 1**

SCENARIO	Security of IoT Platform
History	V0.1
Key Actors	IT, plant IT, plant operators, Plant Maintenance
Assumptions/Dependencies	<ul style="list-style-type: none"> <li>IoT Platform implemented and IoT devices available for testing including:</li> <li>UPC-UA system</li> <li>BigData system</li> <li>Shopfloor Control system</li> <li>FISHY platform components have been installed and are running</li> </ul>
Constraints	<ul style="list-style-type: none"> <li>Existing scenario did not address security in the design</li> </ul>
Objective(s)	<p>To validate FISHY mechanisms for ensuring the security and cyber resilience in the Connected Factory architecture in all chain since IoT devices to end using, with the purpose of:</p> <ol style="list-style-type: none"> <li>ensuring accurate in-time exchange of information;</li> <li>ensuring continuous delivery of service monitoring and identifying key vulnerabilities and threads;</li> <li>recommending preventive and corrective measures;</li> <li>enforcing security</li> </ol>
Description	<p>The IoT platform address all aspects of getting information of the manufacturing of decorative paper impregnation and melamine surface boards related to approximately 600 process variables, including: temperature, humidity, speed, etc., process data and provides information in real-time on a visual web portal. It provides predictive information about two main process variables (RC-Resins Content and VC-Viscosity Content), in case the values are outside the recommended interval it allows the operators to adjust some of the process parameters. It makes also a prediction of which of types of defects can occurs on the on-going production of decorative paper impregnation. It uses, among other sources, the data collected by IoT devices and using the platform Microsoft Azure Machine Learning module.</p> <p>Step 1) IoT devices reading information from the process (Temperature, moisture, ...)</p> <p>Step 2) Readings are stored in a local SQL Database</p> <p>Step 3) Data is read into an OPC-UA Server</p> <p>Step 4) Data is received by an OPC client in the Edge Runtime and published into the Edge Hub</p> <p>Step 5) The information is enriched with metadata, thresholds and alarms</p> <p>Step 6) The enriched data is sent to the IoTHub (Cloud)</p> <p>Step 7) A web application reads the data from the IoTHub and displays it in real-time</p>
Services/Functionalities	IRO; TIM; SCM; SPI

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	25 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

Metrics	Described on chapter 4
---------	------------------------

### 3.3.3 UML diagram

The following UML diagram depicts the use cases involved in the WBP scenarios described above. The use cases directly related to FISHY are marked in black bold.

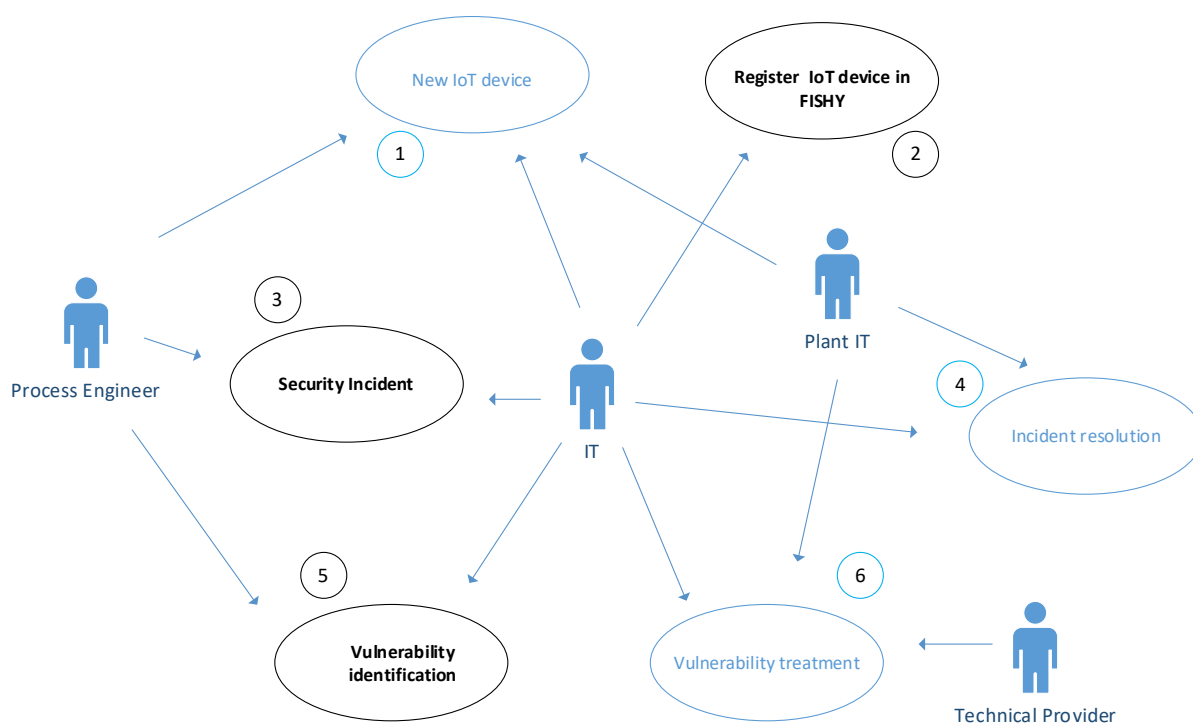


Figure 7: UML diagram for the WPTV supply chain case

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)			Page:	26 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status: Final

### 3.3.4 UML Use cases

Table 14: UML Use cases SON\_UC1

USE CASE Description	
ID	SON_UC1
Name	New IoT Device
Actors	Process Engineer, Plant IT, IT
Storyline	<ul style="list-style-type: none"> <li>- Process engineer identifies that it is necessary to collect additional data from the production line for better efficiency or to improve the ML module. The data collected will have two purposes, to provide real-time values to the plant operators and to be used by Azure Machine Learning module to obtain predictive insights.</li> <li>- Plant Maintenance technician installs the new IoT device locally.</li> <li>- Plant IT configures the IoT device.</li> <li>- IT handles all actions in Connected Factory so that the data captured is then used in the pre-defined purpose.</li> </ul>
Trigger events	New data collection need
Preconditions	IT and Plant IT have all information to configure IoT device. IT has all process variables identified by Process Engineers
Postconditions	Information is available in real time and accurate to the plant operators.
Related scenarios	scenario 1

Table 15: UML Use cases SON\_UC2

USE CASE Description	
ID	SON_UC2
Name	Register IoT device in FISHY
Actors	IT
Storyline	IT registers the new IoT device in FISHY platform. If for any reason the new IoT device is used by IoT platform before being registered, it will be opened an incident.
Trigger events	New IoT device installed and configured in the IoT Platform.
Preconditions	New IoT device installed and configured.
Postconditions	New IoT is ready to be used by IoT platform.
Related scenarios	scenario 1

Table 16: UML Use cases SON\_UC3

USE CASE Description	
<b>ID</b>	SON_UC3
<b>Name</b>	Security incident
<b>Actors</b>	IT, Process Engineer
<b>Storyline</b>	A security incident is detected in one of the components of the IoT platform. TIM module of the FiSHY platform performs the analysis of the impact that the incident may have on the organization and will give instructions (Action plan) to IT on what actions are necessary to resolve or mitigate the incident effectively. IT and Process Engineer validates the plan and take the correspondent actions to solve the incident.
<b>Trigger events</b>	Security incident in IoT platform
<b>Preconditions</b>	Incident management process known by FiSHY Business and Technical Metrics defined
<b>Postconditions</b>	Proceed with the resolution of the incident
<b>Related scenarios</b>	scenario 1

Table 17: UML Use cases SON\_UC4

USE CASE Description	
<b>ID</b>	SON_UC4
<b>Name</b>	Incident resolution
<b>Actors</b>	IT, plant IT
<b>Storyline</b>	Following the validation of the plan for the resolution of an incident, IT and plant IT will proceed the planned actions to solve the incident.
<b>Trigger events</b>	Security incident in IoT platform
<b>Preconditions</b>	Incident management process known by FiSHY Business and Technical Metrics defined
<b>Postconditions</b>	Address lessons learned, including the remediation/improvements action plan if applicable
<b>Related scenarios</b>	scenario 1

Table 18: UML Use cases SON\_UC5

USE CASE Description	
<b>ID</b>	SON_UC5
<b>Name</b>	Vulnerability identification
<b>Actors</b>	IT, Process Engineer
<b>Storyline</b>	<p>A security vulnerability has been identified in one of the components of the IoT platform. FISHY platform will classify the risk of the vulnerability and suggest a mitigation plan, which may be:</p> <ul style="list-style-type: none"> <li>- Install a security patch if it is available or request the provider to develop one.</li> <li>- Other measures that will reduce the risk such as reduce exposition.</li> </ul>
<b>Trigger events</b>	A vulnerability has been identified in IoT platform
<b>Preconditions</b>	<p>Patch management process and known by FISHY</p> <p>Risk management process known by FISHY</p>
<b>Postconditions</b>	Check if the risk has been reduced to an acceptable level
<b>Related scenarios</b>	scenario 1

Table 19: UML Use cases SON\_UC6

USE CASE Description	
<b>ID</b>	SON_UC6
<b>Name</b>	Vulnerability treatment
<b>Actors</b>	IT, plant IT, technical provider
<b>Storyline</b>	Following the identification of a vulnerability, treatment plan validated and scheduled, Plant IT and/or IT proceed with the planned actions. Case required, the Technical Provider will be involved in the resolution.
<b>Trigger events</b>	A vulnerability has been identified in IoT platform
<b>Preconditions</b>	<p>Vulnerability treatment plan have been validated</p> <p>Treatment scheduled</p>
<b>Postconditions</b>	Check if the risk has been reduced to an acceptable level
<b>Related scenarios</b>	scenario 1

## 3.4 Securing Autonomous Driving Function at the Edge (SADE) ALTRAN

### 3.4.1 Introduction (SADE)

Given **REMOTIS**, an autonomous vehicle, the aim of this FISHY use case is to secure all sensor (LIDAR, video cameras, driving parameters, ...), actuators (brakes, acceleration, steering) and the car itself using FISHY technologies and communication protocols.

From a network perspective, the aim is to develop a highly robust and secure telecom interface between the vehicle and the server (Cloud / Edge Computing), that must be able to provide real-time data transfer and the management of all the actors. For that, the FISHY SIA (Secure Infrastructure Abstraction) functional block will provide the means to define an Abstraction of Network Edge Device of the REMOTIS car.

Implementation will allow to Offload the Security Applications into the EDGE Network.

For that purpose and as representative of the current trends in Automotive Industry, REMOTIS /AD concept car will be expanded with the following services:

- **Biometric Facial Key:** The car will be activated with the face of the car user, being able to track and record when each user was driving it as well as information about his/her driving style.
- **Sensors Secure Environment:** Currently, REMOTIS relies in the many of the sensors own security policies to control crypto resources such as passwords, certificates, capabilities (codecs), etc. A single entity will be created with the responsibility to manage north bound those sensors capabilities.

### 3.4.2 Scenarios to be tested/piloted using the FISHY IT-1

Table 20: Securing Autonomous Driving Function at the Edge - Scenario 1

SCENARIO	Securing information when owner has not the car yet
History	v0.1
Key Actors	Local Operator, Dealer
Assumptions / Dependencies	<ul style="list-style-type: none"> <li>• The local operator and dealer are registered in FISHY platform.</li> <li>• FISHY platform components have been installed and are running.</li> <li>• FISHY IRO and dashboard is operational, and actors have been registered.</li> <li>• Car is built and ready at car dealership.</li> </ul>
Objective(s)	FISHY will provide manage access to private and sensitive Data Data will be anonymized and protected
Description	Step 1) Local Operator have information about the car (VIN) and must register the car information in FISHY platform  Step 2) Dealer sells the car  Step 3) Dealer must create a training of face recognition model to allow the owner to power on the car.
Services/Functionalities	IRO, TIM, SPI
Metrics	The metric is detailed in chapter 4.

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	30 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

Table 21: Securing Autonomous Driving Function at the Edge - Scenario 2

SCENARIO	Securing car assets after owner receives the car
History	v0.1
Key Actors	Local Operator, Dealer and Owner
Assumptions / Dependencies	<ul style="list-style-type: none"> <li>The local operator, dealer and owner are registered in FISHY platform.</li> <li>The car was registered at FISHY platform by local operator.</li> <li>Dealer added owner's information at FISHY platform (personal data and Face model).</li> <li>FISHY platform components have been installed and are running.</li> <li>FISHY IRO and dashboard is operational.</li> <li>The owner has the car.</li> </ul>
Objective(s)	<p>Manage access to Private Data</p> <p>Sensitive data will be anonymized and protected</p> <p>Apply a homogenous and consistent continuous secure software development life cycle.</p> <p>Identify security assets of the cars.</p> <p>Provide a secure way to power on the car connected to the Edge verifying that a user is known by the system through face recognition.</p>
Description	Step 1)
Services/Functionalities	IRO, TIM, SPI
Metrics	The metric is detailed in chapter 4.

### 3.4.3 UML Diagrams (SADE)

The UML diagram depicts the use cases involved in the SADE pilot.

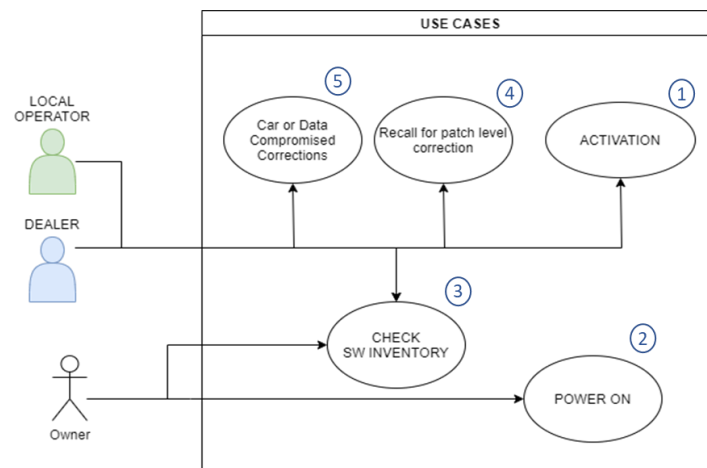


Figure 8: UML diagram of SADE use cases

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)	Page:	31 of 55
Reference:	D6.1	Dissemination:	PU
Version:	1.0	Status:	Final

### 3.4.4 UML Use cases (SADE)

Table 22: UML Use cases SADE\_UC1

USE CASE Description	
<b>ID</b>	SADE_UC1
<b>Name</b>	Activation
<b>Actors</b>	Local Operator, Dealer
<b>Storyline</b>	<p>Local operator introduces information about the car once it is available in the market. This information should be at least VIN (Vehicle identification number), plate and all car information needed.</p> <p>Once the car is sold, Dealer must introduce all information about the owner in FISHY Platform. The most important information should be the training model for owner's face recognition.</p> <p>The data will be securely stored in SPI.</p>
<b>Trigger events</b>	New car is sold
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>The car has a VIN known by Local Operator.</li> <li>The car is sold.</li> </ul>
<b>Postconditions</b>	Private data information about car and owner is securely stored in SPI
<b>Related scenarios</b>	Scenario 1

Table 23: UML Use cases SADE\_UC2

USE CASE Description	
<b>ID</b>	SADE_UC2
<b>Name</b>	Power On
<b>Actors</b>	Owner
<b>Storyline</b>	<ol style="list-style-type: none"> <li>Owner opens the car and inserts the first key which powers on the system.</li> <li>Car will ask to the ENSCONCE which is the closest Edge and starts to interact with it.</li> <li>Car start checking at the registry if the VIN of the vehicle is valid, and if it is registered into FISHY platform. If it is not valid will be rejected.</li> <li>A ROS ID will be created, and Car will publish camera info to be checked in a biometric authorization module.</li> <li>System will sync data about the vehicle and biometric information, system will check if Owner is allowed to start the car. If is not allowed, request will be rejected, otherwise, one instance of APP ID ROS ID will be created with sync data from vehicle and High voltage battery will be powered on, allowing to owner to drive the connected car.</li> <li>Camera will capture user face and send it to the ENSCONCE to check</li> </ol>
<b>Trigger events</b>	Owner tries to start the car
<b>Preconditions</b>	Car was activated
<b>Postconditions</b>	Car's battery is powered on and car is ready to start driving.

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	32 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final



<b>Related scenarios</b>	Scenario 2
--------------------------	------------

**Table 24: UML Use cases SADE\_UC3**

USE CASE Description	
<b>ID</b>	SADE_UC3
<b>Name</b>	Software patch certification
<b>Actors</b>	Local operator, dealer, owner
<b>Storyline</b>	Any actor could access to IRO in order to check firmware versions of assets in a car. After check that user is allowed, SIA will ask to AD application in ENSCONCE to list available software information about a car.  This module will ask to request inventory in a module inside the car and the information returns to be displayed in IRO after saved into SPI.
<b>Trigger events</b>	One actor access to IRO and requests software information about a vehicle
<b>Preconditions</b>	Car was activated and powered on.
<b>Postconditions</b>	Information about firmware versions of car assets is listed.
<b>Related scenarios</b>	Scenario 2

**Table 25: UML Use cases SADE\_UC4**

USE CASE Description	
<b>ID</b>	SADE_UC4
<b>Name</b>	Patch Level Correction
<b>Actors</b>	Local operator, dealer
<b>Storyline</b>	Any actor could access to IRO to check firmware versions and inform owners to recall a car.  The dealer will upgrade any firmware compromised by a vulnerability.
<b>Trigger events</b>	The firmware of an asset has a vulnerability and car the dealer informs to the owner
<b>Preconditions</b>	Car was activated and powered on.
<b>Postconditions</b>	Owner is informed with an email that car must be checked at car's dealership.
<b>Related scenarios</b>	Scenario 2

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	33 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

Table 26: UML Use cases SADE\_UC5

USE CASE Description	
<b>ID</b>	SADE_UC5
<b>Name</b>	Car compromised
<b>Actors</b>	Local operator, dealer
<b>Storyline</b>	<p>When an actor detects that private data or application at the Edge is compromised, they could start an operation to remove Instances and data about the compromised car.</p> <p>SIA will send this operation to the ENSCONCE and the registry will send a notification to the car to inform the car will be offline.</p> <p>Information about ROS ID will be deleted from SPI.</p> <p>Car is offline from this point</p>
<b>Trigger events</b>	Application at the Edge or private data was compromised
<b>Preconditions</b>	Car was activated and powered on.
<b>Postconditions</b>	APP ID ROS ID instances are deleted from the Edge. Car is offline from this point.
<b>Related scenarios</b>	Scenario 2

## 4 Business and Technical Validation Metrics

### 4.1 Introduction

Already from the DoA, FISHY consortium has defined a set of concrete metrics to measure the success of the project in each of the three supply chain cases. As in the current deliverable we focus in the pilot activities using iteration-1 of the FISHY platform, we present the metrics we aim to evaluate and the methodology we will pursue, adopting the following table (Table 27) as a template. Additional metrics to cover all the targeted scenarios described in the DoA will be presented in D6.3. Furthermore, in almost all pilot sites and systems, additional points of assessment (e.g. performance in technical terms) will be assessed such as the CPU and storage needs for the execution of FISHY components. In the next sections, we present the metrics for each of the three FISHY pilots. It is worth stressing that in the row titled “Involved components” the most relevant components are included as in all cases more than one component interact. The reason for including this row is to establish a common understanding between the pilot partners and the FISHY technical partners developing the FISHY platform.

**Table 27: Template of validation metric description**

Metric description	
<b>ID</b>	SCx_ty where x is 1 for F2F, 2 for WPTV and 3 for SADE pilots; t is T for technical metrics and B for business metrics; y is an ascending order number.
<b>Name</b>	Descriptive name
<b>Type</b>	Business and/or technical
<b>Target value</b>	The value aimed to be achieved in the first pilot round.
<b>Methodology</b>	What steps will be followed to evaluate it
<b>Involved components</b>	Components of the FISHY platform
<b>Comments</b>	Any relevant comment

### 4.2 Farm-to-Fork Supply Chain

**Table 28: Farm-to-Fork Supply Chain; Metric description SC1\_B1**

Metric description	
<b>ID</b>	SC1_B1
<b>Name</b>	Number of interledger technologies supported
<b>Type</b>	Business and technical
<b>Target value</b>	2

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	35 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

<b>Methodology</b>	In the scenario 1, a set of 2 ledgers are involved. These two ledgers communicate thanks to interledger components: To validate and demonstrate this, we will <ul style="list-style-type: none"> <li>A) Show through the IRO that three different systems are connected and monitored by the FiSHY platform and these are of different technologies</li> <li>B) provide evidence based on wallet printscreens, UI interface to the user (end consumer) showing the wallet ID, the transaction number, and the blockchain technologies of each system</li> </ul>
<b>Involved components</b>	SACM (for the registration and the auditing of the three blockchains), TIM, SPI, IRO

**Table 29: Farm-to-Fork Supply Chain; Metric description SC1\_T1**

Metric description	
<b>ID</b>	SC1_T1
<b>Name</b>	Number/Types of threats that can be detected
<b>Type</b>	Technical
<b>Target value</b>	3
<b>Methodology</b>	The F2F supply consists of a number of traditional web-based apps and of blockchain solutions. The detection of the threats described in section 5.2 will be based on the demonstration of the execution of the rules defined in the same section.
<b>Involved components</b>	TIM

### 4.3 Wood-based Panels Trusted Value-Chain

**Table 30: Wood-based Panels Trusted Value-Chain; Metric description SC1\_B1**

Metric description	
<b>ID</b>	SC1_B1
<b>Name</b>	Unregistered IoT devices in the network
<b>Type</b>	Business and technical
<b>Target value</b>	1
<b>Methodology</b>	The WLAN controller of Sonae Arauco monitors in real-time the VLAN of the IoT devices and send the collected information to FiSHY. If a new unregistered IoT device is identified in the network we are facing an incident which can be a rogue device on the network or the installation procedure has not been followed by the administrator (previously register the IoT device on FiSHY).

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	36 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

	<p>To validate Sonae Arauco will:</p> <ul style="list-style-type: none"> <li>- Register all existing IoT devices on FISHY</li> <li>- Add a “temporary” not registered IoT device in the network</li> </ul> <p>FISHY will:</p> <ul style="list-style-type: none"> <li>- Identify the new IoT device and verify if it is registered</li> <li>- If not registered open an incident to the administrator that will be opened until any action from the administrator.</li> </ul>
<b>Involved components</b>	<p>WLAN Controler (from Sonae Arauco)</p> <p>SPI; TIM; SIA; EDC; IRO</p>
<b>Comments</b>	<p>Identified target value is a reference for the pilot as if one rogue device is detected, any similar can also be detected.</p>

**Table 31: Wood-based Panels Trusted Value-Chain; Metric description SC1\_B2**

Metric description	
<b>ID</b>	SC1_B2
<b>Name</b>	Maximum time to address vulnerabilities
<b>Type</b>	Business and technical
<b>Target value</b>	1 week
<b>Methodology</b>	<p>FISHY will perform vulnerability assessments to IoT systems, whenever vulnerabilities are identified, FISHY will rating them based on risk and send a report to the administrator. In a maximum of one week the administrator will have to register in FISHY what will be the treatment, by who and when the vulnerability will be addressed.</p> <p>To validate Sonae Arauco will:</p> <ul style="list-style-type: none"> <li>- Register IoT systems in FISHY</li> <li>- Do not give any answer before 1 week + 1 day</li> </ul> <p>FISHY will:</p> <ul style="list-style-type: none"> <li>- After 1 week without answer, open an incident</li> <li>- If the vulnerability still exists after the treatment date, open an incident</li> </ul>
<b>Involved components</b>	<p>IoT systems (from Sonae Arauco)</p> <p>SIA; TIM; SCM; IRO</p>
<b>Comments</b>	<p>Identified target value is a reference for the pilot.</p>

**Table 32: Wood-based Panels Trusted Value-Chain; Metric description SC1\_B3**

Metric description	
<b>ID</b>	SC1_B3
<b>Name</b>	IoT Hub telemetry sent from Edge
<b>Type</b>	Business
<b>Target value</b>	volume of telemetry < as the minimum historic
<b>Methodology</b>	<p>OPC-UA server (EDGE component) collects in real time telemetry values that will be sent to IoT HUB. Whenever the volume of telemetry collected is lower as the historic minimum, we are facing with an incident that must be immediately addressed (critical). To validate Sonae Arauco will:</p> <ul style="list-style-type: none"> <li>- Identify a reference minimum historic</li> <li>- To be defined, how to simulate one incident or waiting for a real scenario</li> </ul> <p>FISHY will:</p> <ul style="list-style-type: none"> <li>- Send an email (and a SMS if possible) to the administrator whenever an incident append.</li> </ul>
<b>Involved components</b>	IoT HUB (From Sonae Arauco) SIA; SCM; TIM; IRO
<b>Comments</b>	Identified target value is a reference for the pilot. Due the criticality of this process, Sonae Arauco will have a redundant alarm system during the pilot.

#### 4.4 Securing Autonomous Driving Function at the Edge (SADE)

**Table 33: SADE; Metric description SC1\_T1**

Metric description	
<b>ID</b>	SC1_T1
<b>Name</b>	Detect unauthorized access to the vehicle
<b>Type</b>	Technical
<b>Target value</b>	1
<b>Methodology</b>	<p>Driver will power up the vehicle. Only the owner and allowed drivers can power on the vehicle. Biometric information must be checked before allowing the vehicle to start. If biometric data obtained from the vehicle by the inside camera matches with the data stored in FISHY platform, the vehicle will start, otherwise, vehicle will remain powered off.</p> <p>To validate, Capgemini Engineering administrator will:</p>

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	38 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

	<ul style="list-style-type: none"> <li>- Register a vehicle into the FISHY platform.</li> <li>- Register and upload biometric data allowed to power on the vehicle.</li> </ul> <p>FISHY will:</p> <ul style="list-style-type: none"> <li>- Allow access to the sensitive information when the vehicle tries to start.</li> <li>- Return biometric information about drivers allowed to drive the vehicle.</li> </ul>
<b>Involved components</b>	SPI; SIA

**Table 34: SADE; Metric description SC1\_T2**

Metric description	
<b>ID</b>	SC1_T2
<b>Name</b>	Integrate inside SIA – secure biometric function
<b>Type</b>	Technical
<b>Target value</b>	Integrated 1 function
<b>Methodology</b>	Integrate function within SIA in ENSCONCE platform
<b>Involved components</b>	SIA

**Table 35: SADE; Metric description SC1\_T3**

Metric description	
<b>ID</b>	SC1_T3
<b>Name</b>	Integrate inside SIA – Software update function
<b>Type</b>	Technical
<b>Target value</b>	Integrated 1 function
<b>Methodology</b>	Integrate function within SIA in ENSCONCE platform
<b>Involved components</b>	SIA

Table 36: SADE; Metric description SC1\_B1

Metric description	
<b>ID</b>	SC1_B1
<b>Name</b>	Reduce recall operation to the car's dealer
<b>Type</b>	Business
<b>Target value</b>	60% of the car recalls to dealer could be prevented. The target is to decrease this number.
<b>Methodology</b>	<p>Autonomous vehicles will send all information about software installed in its embedded components to SADE Platform. FISHY will collect this information. If a component is registered in FISHY Platform and version is not present as certified, FISHY will enforce a policy to fix it.</p> <p>To validate Capgemini Engineering will:</p> <ul style="list-style-type: none"> <li>- Provide a list of software versions verified as safe through FISHY Platform</li> <li>- The vehicle service will send current software versions installed in the car, including one specific component with a version is not certified.</li> </ul> <p>FISHY will:</p> <ul style="list-style-type: none"> <li>- Identify the vehicle</li> <li>- Enforce a policy to update the component.</li> </ul>
<b>Involved components</b>	SPI; SCM; SIA; EDC; IRO



## 5 Mapping of piloting activities to FiSHY offerings

### 5.1 Introduction and functionality-to-SC case map

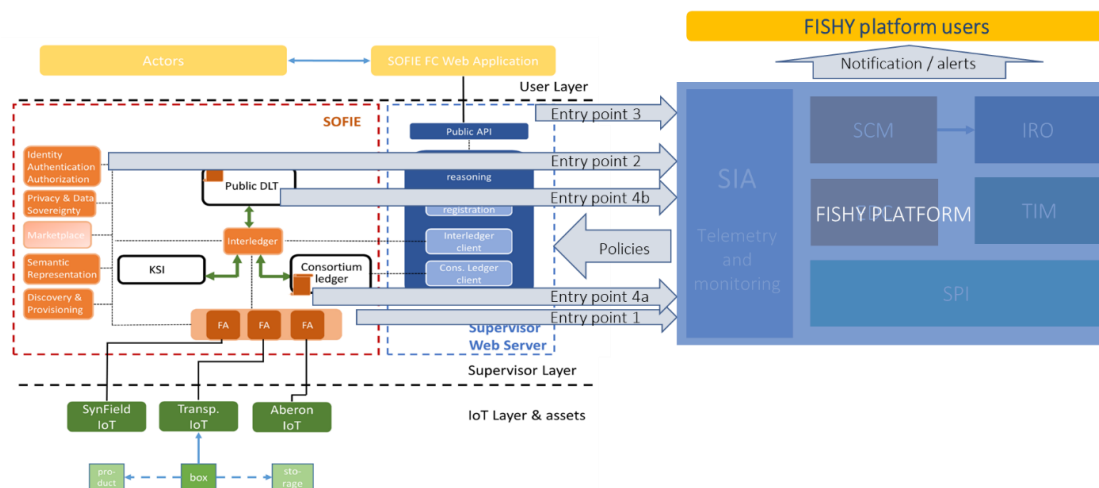
In this chapter, our aim is to ensure the list of FiSHY offerings that are validated/assessed in each of the three FiSHY use cases (corresponding to the three pilot sites). To do so, we first include a table where for each FiSHY high-level functionality, we define which FiSHY pilot will use it and test it. Then, we go on defining the exchange of information between the IT solutions deployed in each pilot site and the FiSHY platform. In other words, in section 5.2, 5.3, 5.4 we describe the security probes that will be deployed and used in each FiSHY pilot site.

**Table 37: Mapping of FiSHY functionalities/offerings to supply chain cases**

FiSHY functionality	F2F	WBP	SADE
Vulnerabilities and risk estimation (RAE, Vulnerability Assessment)		Y	Y
Incident management and mitigation (Advanced Mitigation Strategy)		Y	
Prediction and estimation of risks (RAE)			Y
Enforcement and Dynamic configuration (Attack Remediation Engine, Filter and L7 Filter, vIPSecless)	Y		Y
Security Assurance and Certification Manager	Y		Y
Monitoring and testing of supply chain - intrusion detection (XL-SIEM, Detection and Protection)	Y		Y
Auditing (including evidence collection)	Y	Y	

### 5.2 Farm-to-Fork Supply Chain

In the farm to fork supply chain, to protect the F2F platform, we have implemented the components that deliver to the FiSHY platform information from four distinct points of the deployed F2F platform. The “security probes” of the F2F platform are shown in the following Figure 9. These data are consumed by the FiSHY platform.



**Figure 9: The F2F platform and its interconnection with the FiSHY platform**

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)	<b>Page:</b>	41 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU
<b>Version:</b>	1.0	<b>Status:</b>	Final

They will be sent to FISHY in the form of a JSON object which will include the following fields: UUID (Unique Universal ID, Timestamp (UTC timestamp), Type, Metadata. Four types are distinguished and are meant to detect different types of attacks/threats.

- Type 1: Unauthorised device –wallet ID level
  - Metadata: {Attacker wallet ID, Expected Legitimate Wallet ID, Device name}
- Type 2: Unauthorised device – DID level
  - Metadata: {Attacker DID, Device name, Jwt}
- Type 3: Unauthorised User
  - Metadata: {username, IP}
- Type 4: Attack to Blockchain node
  - Metadata: {IP, port, incident type}

Although in the current chapter we consider FISHY as a black box offering functionalities to the F2F platform, it is worth mentioning at high level that once the data arrive at the SPI, it dispatches them to TIM, which is detecting the issue and EDC, which is in charge of enforcing appropriate rules. (Further details on how this is accomplished is out of scope of the current deliverable.)

For all the above rules/scenarios to be validated the following components are involved/assessed:

**TIM:** check whether the condition is satisfied

**IRO:** presents to the FISHY user the detected threats and notifications and allows the configuration of intents.

**EDC:** enforce a wallet ID ban

**SPI-SIA:** receives the logs and pass to the F2F platform the decisions.

For each type, the following security rules will be applied:

Type	RULE
1	If Attacker wallet ID appears more than <i>Threshold1.1</i> times in <i>Threshold 1.2</i> hours, then <ul style="list-style-type: none"> <li>• FISHY <b>notifies/alerts</b> F2F supply chain operator and/or</li> <li>• FISHY <b>notifies</b> IoT Island operator and/or</li> <li>• FISHY <b>enforces</b> Wallet ID ban (i.e. the F2F SOFIE platform will no longer consider keeping information coming from this wallet ID).</li> </ul>
2	If Attacker DID appears more than <i>Threshold2.1</i> times in <i>Threshold2.2</i> hours, then <ul style="list-style-type: none"> <li>• FISHY <b>notifies/alerts</b> F2F supply chain operator providing the relevant log info (Attacker DID, Device name) and/or</li> <li>• FISHY <b>notifies</b> IoT Island operator and/or</li> <li>• FISHY <b>enforces</b> DID ban (i.e. the F2F SOFIE platform will no longer consider keeping information coming from this DID).</li> </ul>
3	If IP appears more than <i>Threshold3.1</i> times in <i>Threshold3.2</i> hours, then <ul style="list-style-type: none"> <li>• FISHY <b>notifies</b> F2F supply chain operator providing the relevant log info (username, IP) and/or</li> <li>• FISHY <b>enforces</b> IP ban (i.e. the F2F SOFIE platform will no longer accept access request from this specific IP).</li> </ul>
4	If IP appears more than <i>Threshold4.1</i> times in <i>Threshold4.2</i> hours, then <ul style="list-style-type: none"> <li>• FISHY <b>notifies</b> F2F supply chain operator providing the IP and port number and/or</li> <li>• FISHY <b>enforces</b> IP ban (i.e. the F2F SOFIE platform will no longer accept access request from this specific IP).</li> </ul>

### 5.3 Wood-based Panels Trusted Value-Chain

In the Wood-based Panels Trusted Value-Chain, we implement the components that deliver to the FiSHY platform information from tree distinct points of the deployed Sonae Arauco's IoT platform. The "collecting points" are shown in the following figure and the data being consumed by the FiSHY platform:

- (1) – Collects information on Network Infrastructure (WLAN Controller).
- (2) – Collects information from the systems devices of the IoT Infrastructure that are located, some on-prem and others in Azure Cloud.
- (3) - Collects information on IoT Hub.

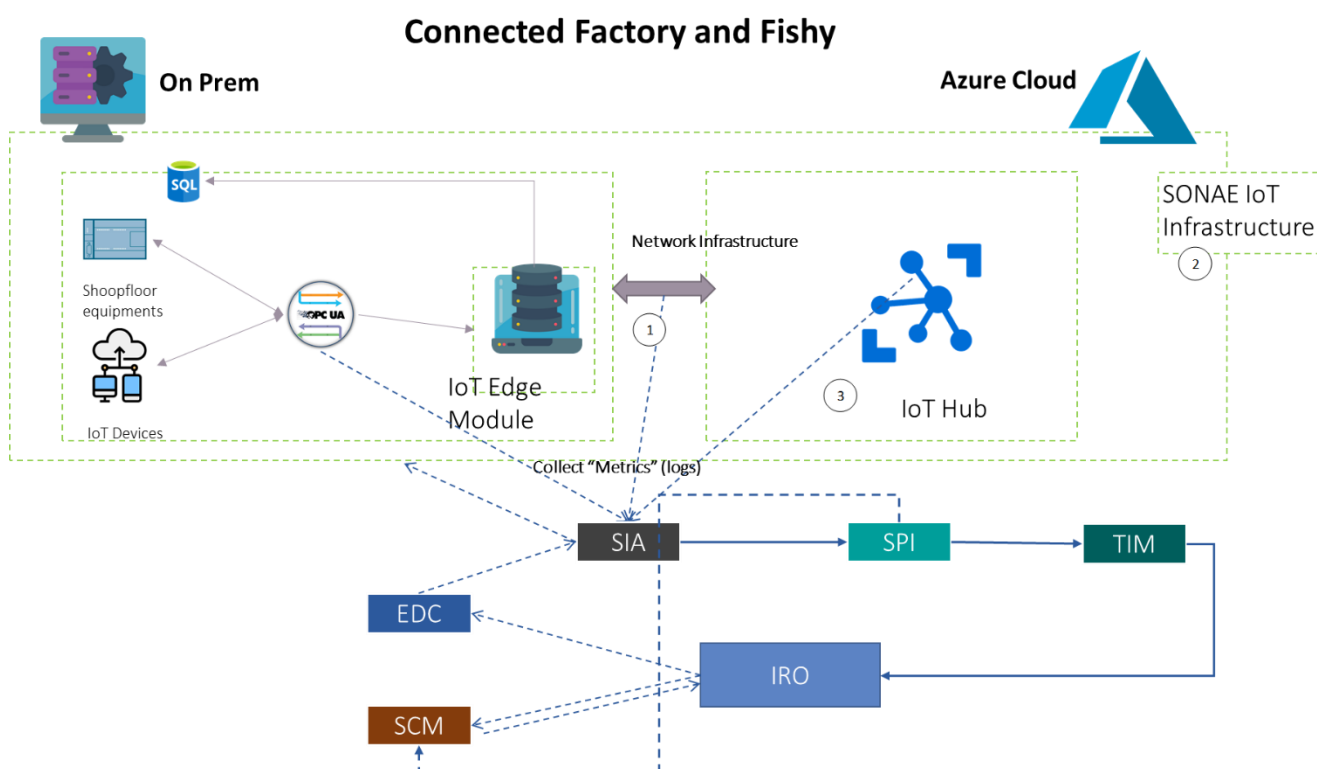


Figure 10: The Connected Factory architecture and its interconnection with the FiSHY platform

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	44 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final

- After 7 days without an answer from the administrator, FISHY will open an incident (TIM) (5)
- When treatment date has passed without corrective action FISHY will open a critical incident (TIM) (6)

Information collected by FISHY: IP addresses; System name; Time Stamp; Operating System; Vulnerability.

### 5.3.3 UC3 – Incident Management:

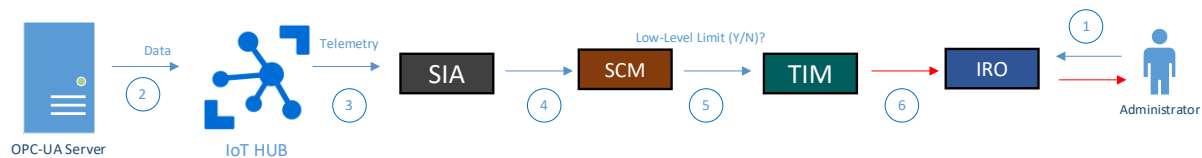


Figure 13: Sonae Arauco use case 3 flow

- Pre-condition: Sonae Arauco identify “minimum historic” (1)
- IoT Hub collects the volume of telemetry (metrics) sent from Edge (OPC-UA server) (2)
- SIA reads telemetry from IoT platform (3)

#### RULES

- SCM verify If the volume of telemetry is lower as the minimum historic (4) and,
  - if volume lower the minimum historic TIM analyzes the impact (5),
  - and opens an incident with a suggested mitigation plan (6)

Information collected by FISHY: Resource ID; Time Stamp; Metric Name; Time Grain; Count.

## 5.4 Securing Autonomous Driving Function at the Edge (SADE)

In the Securing Autonomous Driving Function at the Edge supply chain, to protect information about software and prevent software vulnerabilities detected along time, we have implemented the components that deliver information from the deployed SADE platform to the FISHY platform. An example is shown in the following Figure 13. Data are consumed by the FISHY platform asking via REST/RabbitMQ.

For all the following rules/scenarios to be validated the following components are involved:

**TIM:** detects and checks whether the condition is satisfied.

**IRO:** presents to the FISHY user the detected threats and notifications and allow dealers to register vehicles, personal data about owners and certifications included by OEMs.

**EDC:** enforces action policies against SADE API using REST when some condition is taken.

**SPI:** Has the information of the existing vehicles, and personal data information.

**SIA/NED:** Allows a secure connection between SADE Platform and FISHY Platform to perform operations

### 5.4.1 UC1 - ACTIVATION:

For the activation, FISHY platform does not need to collect data from SADE platform. All data about the vehicle and its owner is provided by the manufacturer and the dealer through FISHY platform.

Data must be stored in a secure way and SPI module will provide secure methods to store and recover this information.

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	45 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final



<b>Model</b>	TempMeterXXX
<b>SW Version</b>	1.1235
<b>Safe Update Link (optional)</b>	https://company.com/updates/TempMeterXXX/1.1235/firmware.bin
<b>Update checksum (optional)</b>	5a000ca5302b19ae8c7a66149f3e1e98

Data from vehicles will be sent to FISHY in the form of a JSON object which will include: UUID (Unique Universal ID, Timestamp (UTC timestamp) and Metadata

```
{
  "metadata": {
    "sw_data": [{
      "manufacturer": "Capgemini Engineering",
      "model": "TempMeterXXX",
      "sw_version": "1.1235",
      "serial_number": "sensor_ht:257d0001XXXX",
    },
    {
      "manufacturer": "Capgemini Engineering",
      "model": "CamSensorXXX",
      "sw_version": "0.1",
      "serial_number": "sensor_cam:1d101s",
    }
  ],
  "vin": "0000-0000-0000-0001",
  "timestamp": "1624003974",
},
"UUID": ""
}
```

SADE will send this information to a RabbitMQ service, deployed near to SIA/NED as a k8s POD.

- FISHY platform must get JSON messages and parses the received information.
- FISHY compares with SW certification versions provided by OEMs.

#### RULES

- There is one rule that checks if one version received is not certified:
  - FISHY **notifies/alerts** users related to the compromised vehicle.
  - FISHY **enforces** Update\* policy against SADE Service (REST API module)

\* If an updated version model is certified and contains a safe link for an update, that link must be provided, if not, our module will start a recall notification, FISHY just do not send any link in the POST request.

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)				<b>Page:</b>	47 of 55
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

#### 5.4.4 UC4 – Software Patch Level correction

When a dealer detects that one vehicle has a high level of risk due to multiple IoT devices in the vehicle with software versions not certified, dealer could send a recall notification to update software inside the vehicle at the dealer's concessionaire.

##### RULES

- FISHY will notify to the administrator that the vehicle is in high level of risk.  
Administrator confirms the risk and allows to send notification to the user.  
FISHY will send a REST call to the SADE API which is in charge of send the notification to the owner via Email.
- Administrator knows that an specific software version is dangerous and submits a condition with this specific software version and the allowance to send notification to the users when their vehicles has this specific software version installed.  
FISHY will send a REST call to the SADE API which is in charge of send the notification to all owners via Email.

#### 5.4.5 UC5 – Car compromised

In this use case, the dealer or local operator will confirm a security threat and will perform an action in the FISHY platform to stop applications and disconnect the autopilot if a vehicle is compromised when a security vulnerability is detected.

The action is a REST call to the SADE API, which is in charge of stopping all instances in the EDGE that control the autonomous car.

##### RULES

- FISHY will notify to the administrator that the vehicle or data was compromised.  
Administrator confirms the risk and allows to send notification to the user.  
FISHY will send a REST call to the SADE API which is in charge of remove all services related to the compromised car.

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)					Page:	48 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final



## 6 Infrastructure set up

### 6.1 Introduction




In this chapter, we describe the platforms that will be set up in each pilot site and connected with the FISHY platform.




### 6.2 Farm-to-Fork Supply Chain

In the farm-to-fork case the infrastructure that will be set up comprises of the farm-to-fork platform connected to the FISHY platform.

The farm-to-fork platform that FISHY will protect uses the infrastructural components listed in the following table (Table 38). The used equipment relates mostly with the sensing devices and the hardware components which are used by the two IoT platforms, which are integrated in the PoC prototype, i.e. the SynField platform [2] and the Kaa-based [3] transportation IoT platform. The first is a production environment (uses operational data) that has been deployed in a vineyard field in the area of Kiato, Greece. The second is a lab environment that integrates all the devices which will be finally deployed on site for the transportation IoT platform. Note that both the IoT platforms, as well as the backend services and the used DLTs of the F2F web application are deployed in Synelaxis cloud infrastructure.

**Table 38. Equipment used in F2F PoC prototype**

Equipment	Role in pilot	View
SynField Head Node (HN)	It is installed in the field and acts as a gateway to collect and transfer farming data into the cloud SynField IoT platform. It is provided by Synelaxis Solutions.	
Weather Station	It is connected to the SynField HN to measure temperature, humidity and other climatic factors (wind speed/direction, rain collector etc.). It is provided by Davis (Vantage Pro 2 <a href="https://www.davisinstruments.com/pages/vantage-pro2">https://www.davisinstruments.com/pages/vantage-pro2</a> ) and it includes SynField adaptation kit.	
RFID tags (boxes IDs)	An RFID tag is attached over each box.	

IoT transportation GW	A raspberry which will be installed inside the truck cabin is used as a GW for the transportation IoT platform. A 4G router is used to guarantee that the GW is always connected to the internet.	
Long range RFID (CAEN ion – R4301P)	Long range RFID which is installed in the truck trolley and it is connected to the IoT transportation GW. It features embedded HW architecture (x86) and standard operating system (Linux) to enable the development of custom software that detects every onboarded box. It is provided by CAENRFID ( <a href="https://www.manualslib.com/products/CAEN-Rfid-Ion-R4301p-10288861.html">https://www.manualslib.com/products/CAEN-Rfid-Ion-R4301p-10288861.html</a> ).	
Temperature sensor (ds18b20)	Analogue temperature sensor which is deployed inside the transportation truck trolley. It is connected with the truck GW.	

The farm-to-fork platform is deployed within the OPENSTACK cluster of Synelixis.

Two virtual machines (Vms) are configured.

- VM1 with the following resources:
  - 2 vCPUs
  - 4 GB RAM
  - 160 GB disk
- VM2 with the following resources:
  - 4 vCPUs
  - 4 GB RAM
  - 120 GB disk

All the platform components and the consortium blockchain are deployed in a dockerized environment.

The transportation IoT KAA platform is deployed alongside with the Federation Adapters of the SOFIE platform.

Any extra components (e.g. RabbitMQ server) are planned to be deployed in VM1 (unless resources are depleted) in which case, a new VM will be deployed.

### 6.3 Wood-based Panels Trusted Value-Chain





In Wood-based Panels Trusted Value-Chain use cases described in previous sections, for the pilot will be used the IoT platform implemented in Oliveira do Hospital, which comprises components in Microsoft's Cloud Azure and components in the plant.





In this phase, the main focus of the PoC is on data acquisition from IoT sensors in the plant, and the flow of data to the Cloud components. For this purpose, will be used the equipment's and services

<b>Document name:</b>	D6.1 Use cases settings and demonstration strategy (IT-1)			<b>Page:</b>	50 of 55	
<b>Reference:</b>	D6.1	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b> Final

described in the table below that will be provided by Sonae Arauco and which will be integrated into the FiSHY platform.

**Table 39. Equipment and services (Wood-based Panels Trusted Value-Chain)**

Equipment	Role in pilot	View
WIFI-sensor	Digital IoT sensor installed in the Impregnation line that collects several production parameters such as temperature, humidity, speed, position, levels, etc. Brand: Advantech Model: WISE-4012 QTY: 15  <a href="https://www.advantech.com/products/4260f153-57cd-4102-81ea-7a0f36d9b216/wise-4012/mod_0dd63bf5-6516-4488-a6f6-9293b5b17eff">https://www.advantech.com/products/4260f153-57cd-4102-81ea-7a0f36d9b216/wise-4012/mod_0dd63bf5-6516-4488-a6f6-9293b5b17eff</a>	
WIFI-sensor	Digital IoT sensor that collects several parameters such as temperature, humidity, speed, position, levels, etc. Brand: Advantech Model: WISE-4220 QTY: 7  <a href="https://www.advantech.com/products/229f9f5b-d073-4cc2-ac54-d90147e04c12/wise-4220/mod_c4851078-f819-4e6d-b597-4ba15b7e1266">https://www.advantech.com/products/229f9f5b-d073-4cc2-ac54-d90147e04c12/wise-4220/mod_c4851078-f819-4e6d-b597-4ba15b7e1266</a>	
WIFI antenna	WIFI antennas located in the impregnation production area that connect the IoT devices with Sonae Arauco's network Brand: CISCO Model: air-ap1542i-E-K9 QTY: 7  <a href="https://www.cisco.com/c/en/us/support/wireless/aironet-1542i-outdoor-access-point/model.html">https://www.cisco.com/c/en/us/support/wireless/aironet-1542i-outdoor-access-point/model.html</a>	
Switchs	Equipment located in the production area where the WIFI antennas are connected Brand: CISCO Model: ws-c2960X-24PS-L QTY: 3  <a href="https://www.cisco.com/c/en/us/support/switches/catalyst-2960x-24ps-l-switch/model.html">https://www.cisco.com/c/en/us/support/switches/catalyst-2960x-24ps-l-switch/model.html</a>	

WLAN Controller	Equipment that manages all aspects of the WIFI network among them the segregation (logical isolation) of the network and collect in real time all information of the equipment connected to the WIFI network. Brand: CISCO Model: WLC 2504 QTY: 1  <a href="https://www.cisco.com/c/en/us/support/wireless/2504-wireless-controller/model.html">https://www.cisco.com/c/en/us/support/wireless/2504-wireless-controller/model.html</a>	
IoT HUB	Central message Hub located in the Cloud (Azure) that provide communication between IoT applications and IoT devices. Brand: Microsoft QTY: 1	
UPC-UA Server	Server located in the plant that have the UPC-UA installed. UPC-UA is used to exchange industrial data and applications. Type: VM Hyper-V OS: Windows Server 2019 std QTY: 1	
PRTG	Monitoring solution that monitors the local network in real-time all equipment's except WIFI. <a href="https://www.paessler.com/prtg">https://www.paessler.com/prtg</a>	

All other components related to FISHY platform that will be needed in the plant will be deployed in a new dedicated server.

## 6.4 Securing Autonomous Driving Function at the Edge (SADE)

SADE use case needs at least one vehicle with sensors.



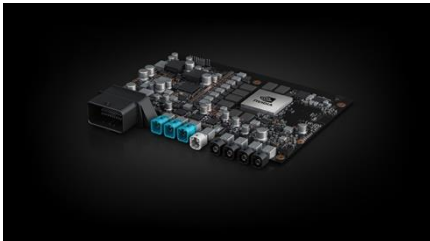

The embedded hardware will serve in the first phase to demonstrate the effectiveness of use case three.

In order to deploy the necessary services, the [5TONIC](#) research environment (deployed in Madrid) will be used.

Here are some of the embedded components within the vehicle.



Table 40. Some of the Equipment embedded in the vehicle

Equipment	Role in pilot	View
Modem 5G	5G modem used for prototyping. Brand: Quectel Model: RM500Q Web reference: <a href="http://sekolab.com/products/camera/">http://sekolab.com/products/camera/</a>	
Other network components	To be provided by the 5TONIC among the pools of providers available there supporting from NSA to SA Web reference: <a href="https://www.5tonic.org/">https://www.5tonic.org/</a>	
AD Enabled vehicle	AD Enabled vehicle including NVIDIA compute module. Brand: Nvidia Model: Drive AGX Xavier Web reference: <a href="https://developer.nvidia.com/drive/drive-agx">https://developer.nvidia.com/drive/drive-agx</a>	
Cameras	Brand: Sekonix Model: SF3325 QTY: 4 Web reference: <a href="http://sekolab.com/products/camera/">http://sekolab.com/products/camera/</a>	

Related to the network, the vehicle will be connected to 5TONIC using 5G Network.

In the 5TONIC.

- **gNode**: Already present at the 5TONIC
- **vEPC (NSA Core)**: Already present at the 5TONIC.
- **5GC (SA Core)**: Already present at the 5TONIC.
- **MEC (Multi-Access EDGE Computing)** – Complete Capgemini engineering ENSCONCE solution deployed in our LAB (Central and Prototyping EDGE POP) and in the 5TONIC (Remote EDGE PoP)

All services developed will be deployed using ENSCONCE solution (based on kubernetes) or in the ENSCONCE cloud (based on Openstack). These are the nodes available to deploy SADE services.

- **Central PoP and Prototyping:**
  - Central Node - DELL PowerEdge R330 + ENSCONCE SW
- **Edge PoP for prototyping**
  - HPE DL360 Gen10 + ENSCONCE SW with a NVIDIA TESLA P4 GPU
- **5TONIC Edge PoP**
  - HPE DL360 Gen10 + ENSCONCE SW x2 (2 compute nodes) and only 1 of them with a NVIDIA TESLA P4 GPU

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)			Page:	53 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status: Final

## 7 Conclusions

---

This deliverable has presented the methodology of the first round of the FISHY IT-1 platform and has presented in detail the scenarios to be executed and metrics to be measured. It has also presented the infrastructure that the pilot providers will set up and will be connected with the IT-1 platform. This deliverable will be the roadmap for the first round of evaluations that will take start in M15. It is stressed that a wider set of scenarios and more detailed evaluation will follow in the 2<sup>nd</sup> round of piloting activities.

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)				Page:	54 of 55
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status: Final

## 8 References

---

- [1] FISHY project, D2.2 “IT-1 architectural requirements and design”, 2021
- [2] <https://www.synfield.gr/>
- [3] <https://www.kaaiot.com/>

Document name:	D6.1 Use cases settings and demonstration strategy (IT-1)				Page:	55 of 55	
Reference:	D6.1	Dissemination:	PU	Version:	1.0	Status:	Final