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

D6.3 Use cases settings and demonstration strategy (IT-2)

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

Related WP	WP6	**Document Reference**	D6.3
Related Deliverable(s)	D6.1, D6.4	**Dissemination Level (*)**	PU
Lead Participant	OPT	**Lead Author**	Antonis Gonos
Contributors	SYN, TID, UPC, OPT, Sonae, Altran/CAPGEMINI, UMinho.	**Reviewers**	Marlos Silva (SONAE) André Oliveira (UMINHO)

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 FHISY 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.

(*) 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
Jan Antić.	XLAB
Jasenka Dizdarevic	TUBS
Xavi Masip Bruin	UPC
Panagiotis Athanasoulis, Panagiotis Karkazis	SYN
Eva Marin Tordera	UPC
Antony Gonos, E. Kanakis	OPT
Jose Soriano Diaz	CAPGEMINI ENGINEERING
Guillermo Jimenez Prieto	CAPGEMINI ENGINEERING
Henrique Santos	UMINHO
André Oliveira	UMINHO
Ana Machado Silva	SONAE
Rui Guilherme Gonçalves	SONAE
Marlos Silva	SONAE
João Marques	SONAE ARAUCO
Daniele Canavese	POLITO
Ignazio Pedone	POLITO
Cataldo Basile	POLITO
Leonardo Regano	POLITO

Document History			
Version	Date	Change editors	Changes
0.1	2022-06-01	Antonis Gonos	ToC and initial structure
0.2	2022-06-20	Antonis Gonos	First round of contributions in chapter 1, 2 and 3 integrated.
0.3	2022-07-20	Antonis Gonos	2nd round of contributions (from UPC, SONAE, CAGENG, SYN) in chapter 1, 2, 3 and 4 integrated.
0.4	2022-07-22	SONAE	Improvements in chapters 3, 4 and 5 for WBPTV use case
0.5	2022-07-26	OPT (Antonis Gonos)	Complete version available for internal review
0.6	2022-08-10	OPT	Version revised based on first comments
0.7	2022-08-19	OPT	Version revised based on all comments from the first round of internal review
0.8	2022-08-29	OPT	Editted formatted version of 0.7 with comments from internal review addressed
1.0	2022-0831		FINAL VERSION TO BE SUBMITTED

Quality Control

Role	Who (Partner short name)	Approval Date
Deliverable leader	Antonis Gonos (OPT)	31/08/2022
Quality manager	Antonio Álvarez (ATOS)	31/08/2022
Project Coordinator	Antonio Álvarez (ATOS)	31/08/2022

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
B2B	Business to Business
D	Deliverable
DLT	Distributed Ledger Technologies
DoA	Description of Action
EC	European Commission
EDI	Electronic Data Interchange
EIM	Exploitation and Innovation Manager
EPO	European Patent Office
ER	Exploitable Result
ERP	Enterprise resource planning
F2F	Farm to Fork
GA	Grant Agreement
HPC	High Performance Computing
IGT	Impact Generation Team
IT	Information Technology
IoT	Internet of Things
Jwt	JSON (JavaScript Object Notation) web tokens
KPIs	Key Performance Indicators
OEM	Original Equipment Manufacturer
SACM	Security Assurance and Certification Manager
SADE	Securing Autonomous Driving Function at the Edge
SPI	Secure and Privacy Data Space Infrastructure
TIM	Trust and Incident 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 that will be adopted for the evaluation of 2nd iteration of the FISHY platform, referred by IT-2, which includes a) additional functionalities and b) improved versions of the components that existed in IT-1. It describes the scenarios and tests that will be running during IT-2 (which will be delivered in M32). It is the 3rd deliverable of WP6 reporting the work of tasks 6.1 and 6.2 in the second year of the project. As the FISHY architecture is developing along with technical details of the implementation, modifications in the technical details of the tests might occur (and will be detailed and justified in D6.4). It is stressed that the FISHY architecture is under finalisation according to the project plan and the rationale behind this choice was to meet additional requirements (like multi-tenancy) that have been captured from the first round of pilots as well as from the evolution of the research in the field. is still on-going in WP2-WP5,

This deliverable starts with a brief outline of the evaluation methodology that is adopted throughout the FISHY project lifetime (elaborated in D6.1) and then proceeds to the details of the test scenarios to be run with the IT-2 version of FISHY platform.

The test scenarios are used to extract Unified Modelling Language (UML)-compliant use cases which also aid the testing of the various functionalities of the FISHY platform. Then, the metrics that will be measured during the pilot tests are detailed. In the description of the scenarios, FISHY platform has been considered as a "black-box", i.e., as a solution offering specific functionalities, whose effects are to be evaluated. However, as WP6 scope is to evaluate the FISHY platform, the functionalities that are assessed in each scenario are identified. 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-2.

It is worth stressing that the scenarios and metrics defined in this deliverable refer to the final phase of testing. Thus, all the mentioned scenarios focus on the evaluation and confirmation of achievement of the project KPIs.

This deliverable is a roadmap that provides the information for the next piloting activities/rounds of the FISHY platform. It can be considered as the liaison between WP2 (which defines the functionality and interfaces) and WP5 (which provides the integrated FISHY platform).

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-2. This document is an outcome of task 6.1 and task 6.2. It produces the demonstration concept (i.e., what and how to demonstrate FISHY innovations and benefits) and a clear validation plan, considering the expected outcomes from the technical WPs. The use cases are described in detail, and it is shown 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. This deliverable is the update of D6.1 (which was focusing on IT-1 version of the FISHY platform).

1.2 Relation to other project work packages

This deliverable highly interrelates with D2.2 [1] as it describes the architectural framework of the FISHY platform and Milestone M2.4 which reports the updated requirements of the FISHY exemplar use cases. It relates to WP5, which delivers to WP6 the integrated 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-2 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:** This chapter 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 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. In many cases, to stress the difference we refer to FISHY use cases vs. UML-compliant use cases.

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) meets 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-2 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, deployment 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/suggestions for improvements are fed back to a) the architecture and implementation focused work-packages and b) to the evaluation scenario definition for their revision to define and support the second version of piloting activities which will focus on IT-2 release. This has been accomplished and reported in D6.2. (An updated list of use case requirements has also been produced – based on the experience gained from the 1st pilot round- in the framework of WP2- task 2.2.)

Step 5: scenario definition for the 2nd (and final) evaluation period (It is the 2nd execution of step 2 taking into consideration the feedback of the 1st piloting round). **This deliverable focuses on this step.** It is worth mentioning that this 2nd evaluation period will internally be organised in sub-rounds and this is the reason we name it 2nd evaluation period, above. The different rounds during this period will focus on the different versions of FISHY platform that will come out from WP5.

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. This feedback will be reported in D6.4.

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 1st and 2nd piloting phase. It should be stressed that the first four steps have been implemented by the delivery date of this deliverable and the 2nd pilot round will take place from M30 till the end of the project.

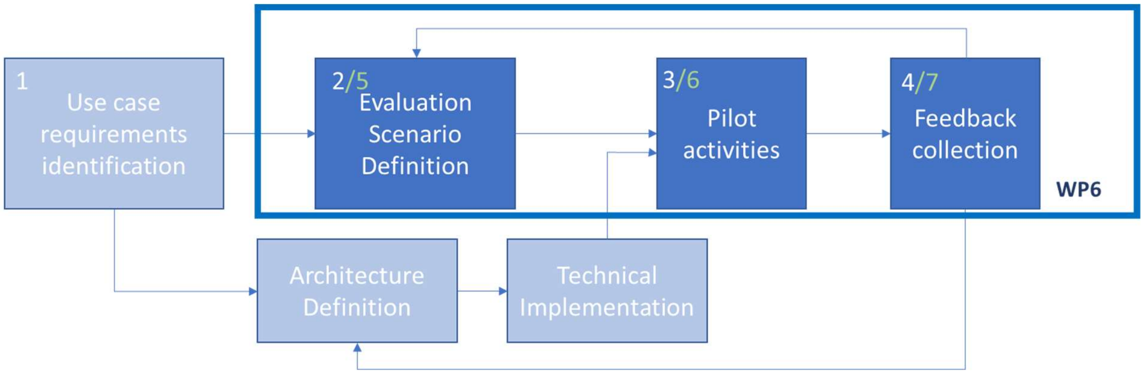

Figure 1: the evaluation methodology that will be executed in WP6 based on inputs from WP2 – WP5.

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 use-case.
2. The (updated) 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).

Next, 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 cases 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 components 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. ● All business companies have registered in FISHY platform. ● IoT platforms are installed and running)
Objective(s)	<List of the objectives of the scenario> (e.g. • Respect the privacy requirements of the involved actors and organizations and guarantee the integrity of the exchanged data. • Collect, filter and manage data and metadata from various IoT environments and other data entry points (i.e. web application).
Description	Description of the scenario in steps so that each one can be verified during piloting. For example, Step 1) The producer owns a field, … Step 2) When the producer’s goods are ready to be transported,…. Step 3) Transporter A drives the vehicle to the Warehouse (WH). Step 4) When one or more boxes should be transferred from y. Step 5) A customer scans.

Services/Functionalities	FISHY functionalities enacted.
Metrics	List of metrics to be measured during the testing of the scenario starting from DoA

Table 2: UML-Use case description template

USE CASE Description	
ID	Identifier of type ASC_UCB where A is the first letter of the FISHY supply chain acronym and B is an ascending number. Example FSC_UC1
Name	Descriptive name (e.g., Register farm system)
Actors	(Human) user involved in this UML use case e.g., Producer
Storyline	Text
Trigger events	The event that triggers the execution of this use case (e.g. A new item has been registered in the platform)
Preconditions	A required precondition so that the use case is appropriately executed (e.g. The registration component is deployed)
Postconditions	The condition -outcome of the use case (e.g., the item table is updated.)
Related scenarios	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 relevant to the Farm-to-Fork supply chain. In this 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 share: 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 concerning warehouse conditions, final destination, responsible employee, etc. Finally, all the data can be processed, and made available to consumers in the supermarkets.

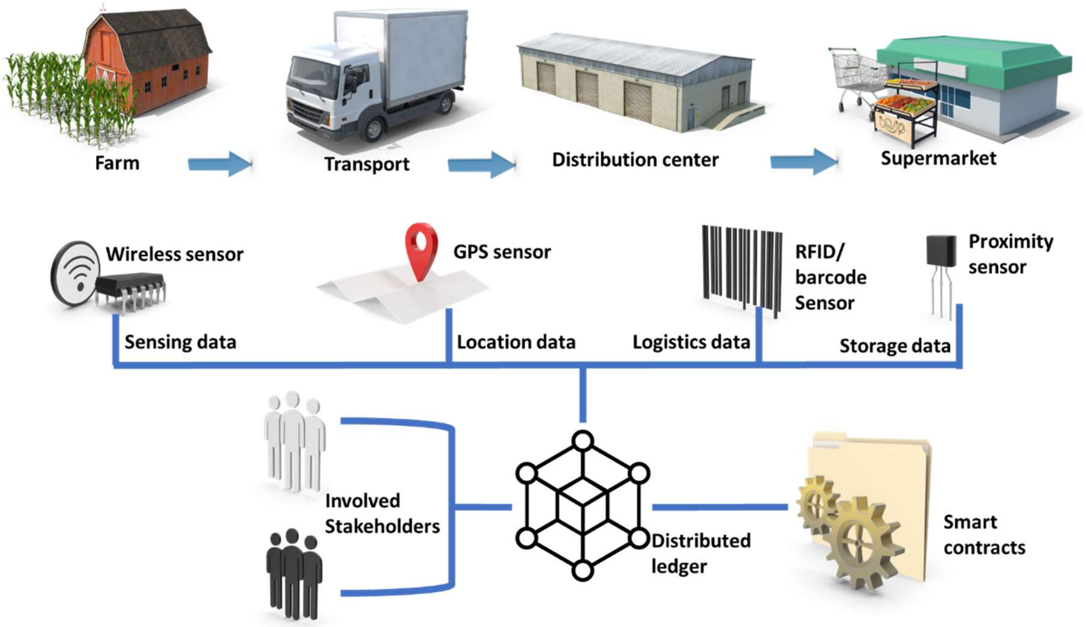

Figure 2: The lifecycle of the products in the "Farm to Fork" supply chain

3.2.2 Scenario to be tested/piloted using the FISHY IT-2

The scenario that will be tested using the IT-2 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 that 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	v0.2 – changes in steps 5-8
Key Actors	Operator of integrated F2F IT platform
Assumptions / Dependencies	• The farmer, the transporter, the warehouse keeper and the consumer are registered in the F2F web app. • The administrators of the three IoT platforms (described below) have installed, operated, and registered in the FISHY platform the assets of the IT platform to be protected which include SynField field nodes, blockchain networks, Aberon and IoT devices and federation agents. • FISHY platform components have been installed and are running. • FISHY IRO and dashboard are operational, and the F2F platform operator has been registered.
Objective(s)	To validate FISHY threat detection mechanisms for evidence-based data sharing implementing interledger components supporting at least two interledger technologies.
Description	Steps 1-5 refer to the appropriate set up and use of the F2F web application which uses data from three IT systems. 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. 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. Step 3) the transportation company employee scans the RFID and associates it with the truck that is used. The information relevant to the truck is also stored in the consortium ledger. 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). 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 organizations must be accessed. Step 6) a security threat/attack is issued/detected. Such an attack can be an unauthorized user attack (at login level), an unauthorized user attack at wallet ID level, an (adverse) device trying to authenticate in the solution or a compromised hash attack. (For further details see chapter 4). Step 7) the FISHY detects the threat/attack. Step 8) FISHY platform defines a mitigation measure expressed as a configuration policy (triggered and defined by IRO and EDC) and finally, Step 9) it notifies the appropriate user (F2F platform administrator).

Services/Functionalities	The main functionalities enacted include: SACM, TIM, EDC, IRO and the dashboard
Metrics	≥2 interledger technologies (e.g. public Ethereum, Hyperledger Fabric, KS) demonstrating the flexibility of FISHY to support the protection of complex IT systems of different supply chains

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 mainly for completeness reasons. Before any scenario is executed the three blue arrows are enacted. During the FISHY piloting, the role of the administrators of the different islands will be played by the F2F platform administrator as he/she has authorization to register the relevant information entry points and devices in the platform for the pilot purposes. For this purpose, in the sequel we define a unique use case titled "Register the F2F platform in FISHY". Considering an extension of FISHY to support multi-tenancy, this use case will be instantiated multiple times with each actor/tenant registering in the FISHY platform the island (part of the platform) he/she operates/administers.

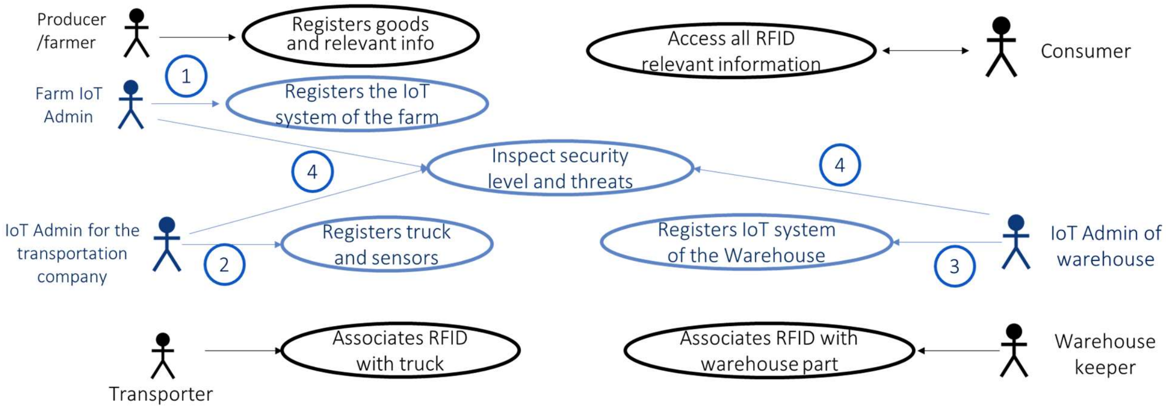
Producer /farmer
Registers goods and relevant info
Access all RFID relevant information
Consumer
1
Farm IoT Admin
Registers the IoT system of the farm
4
Inspect security level and threats
4
IoT Admin for the transportation company
2
Registers truck and sensors
Registers IoT system of the Warehouse
3
IoT Admin of warehouse
Associates RFID with truck
Associates RFID with warehouse part
Transporter
Warehouse keeper

Figure 3: UML diagram for the Farm to Form supply chain case

3.2.4 UML Use cases

We focus on the description of the FISHY (blue) use cases relevant to the FISHY platform which are updated/modified while the rest are described in D6.1 and refer to the operation of the F2F platform.

USE CASE Description	
ID	FSC_UC1

Name	Register the F2F platform in FISHY
Actors	F2F platform admin
Storyline	The administrator of the integrated F2F solution including Synfield based IoT system and Aberon-based warehouse system is registered in FISHY platform and defines the assets to be protected.
Trigger events	New F2F-platform registration in FISHY platform
Preconditions	The F2F-platform is available and an F2F administrator account (FISHY user) has been created.
Postconditions	The FISHY platform is now aware of the system under monitoring/supervision.
Related scenarios	scenario 1

USE CASE Description	
ID	FSC_UC4
Name	Inspect security level and threats
Actors	Administrator of F2F platform
Storyline	The administrator of the F2F platform enters the FISHY platform. He intends to inspect the security conditions/level of the F2F platform he is responsible for. After a successful login in the FISHY platform and he gets information about the security level of all the systems involved in the farm-to-fork journey of the specific good. If an attack or a threat has been detected, a notification appears in the dashboard providing the details of the event. Additionally, he/she is prompted to enforce a policy defined by FISHY intelligent components.
Trigger events	The actor enters the FISHY platform and selects security inspection or notifications tab.
Preconditions	The F2F platform is registered, the rules for attack detection and mitigation have been set.
Postconditions	Attack mitigation, Report about the security status in this chain generated, security audit certificate received.
Related scenarios	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 2 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.

Some of the key intertwined 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 - (Upstream)

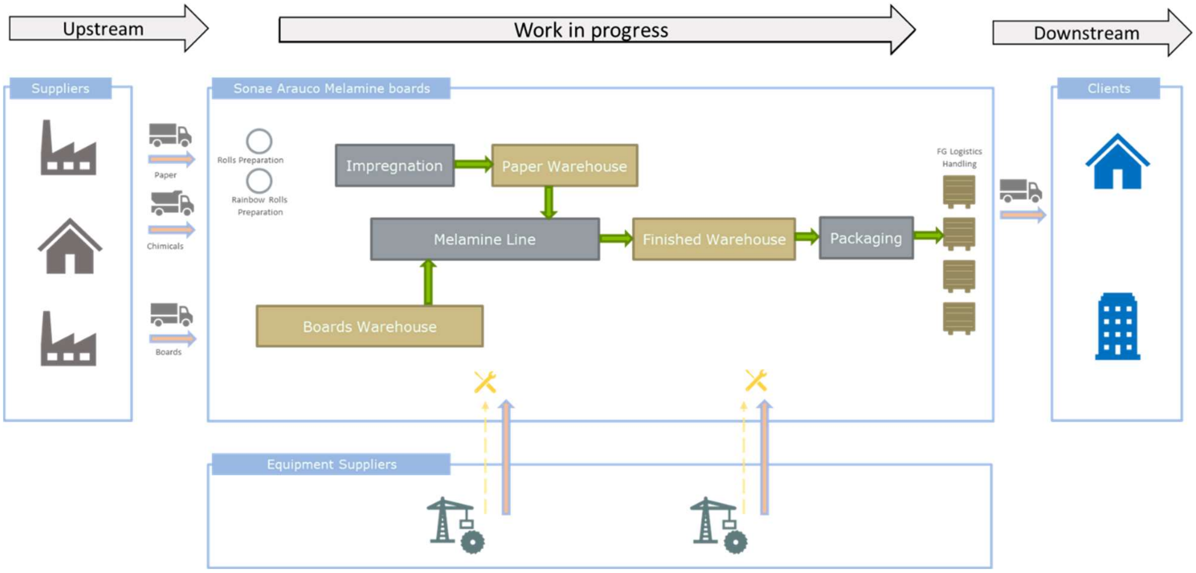

Figure 4: End-to-End Melamine Supply Chain process and flows at Sonae Arauco

For the 2nd iteration, the processes defined in D6.1 for FISHY 1st iteration based on the Connected Factory and with focus on the “work in progress”, are now complemented by the inclusion of downstream and upstream processes that are triggered via http communications with the existing ERP system (S AP) through EDI – Electronic Data Interchange.

FISHY 1st iteration – Connected factory

Ensuring the connectivity of the equipment, Sonae Arauco has sensors and IoT devices in place to enable data flows at the plant level (manufacturing floor) and at the company level (between different plants) as described in D2.2 as well. The existing IoT architecture of the Connected Factory is shown in Figure 5, and the relevant data flows and components are presented in Figure 6 and Table 4.

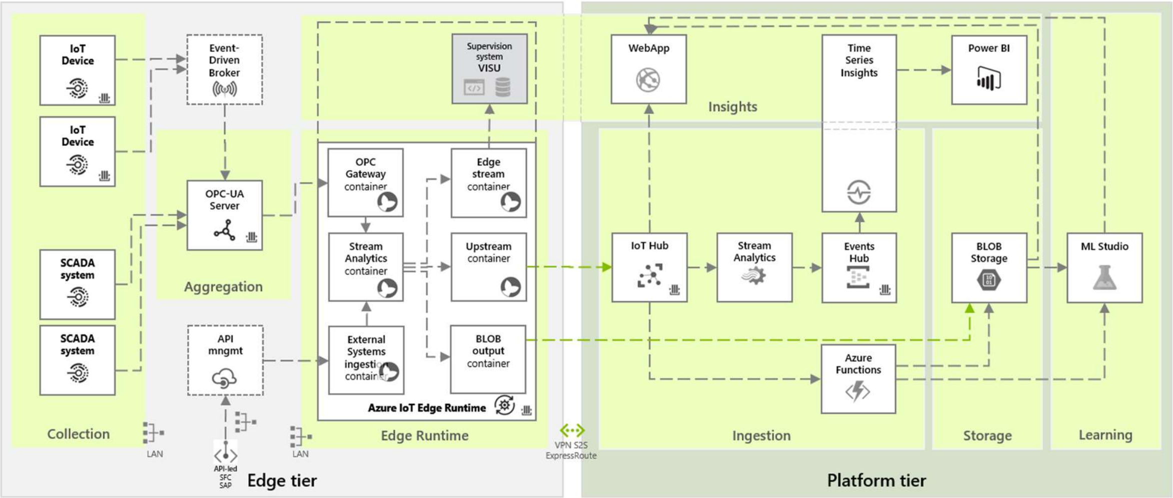

Figure 5: Sketch of the Connected Factory architecture at Sonae Arauco

From the general architecture of the connected factory, the most relevant components for FISHY platform are represented in the next figure:

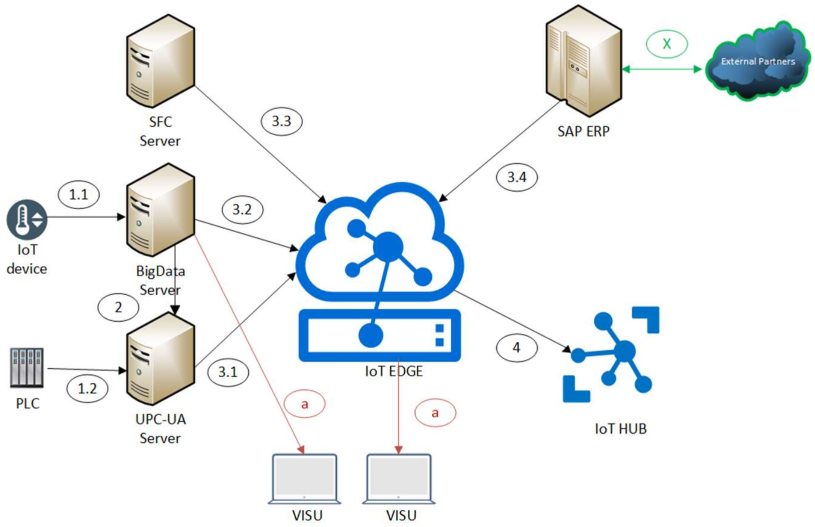

Figure 6: Data Flows in IoT Platform

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 (tracks and documents the transformation of raw materials to finished goods)

- IoT Edge Runtime Server: Collects IoT telemetry data and sends them to Cloud (to IoT Hub Server)
- IoT Hub Server: Collects IoT telemetry from all IoT Edge Servers

Table 4 represents the flows and protocols of the relevant components detailed in Figure 6:

Table 4: Flows of components depicted in Figure 6

NR	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

FISHY 2nd iteration – Electronic Data Interchange

The http communications made through Electronic Data Interchange (EDI) connect the internal Enterprise Resource Planning (ERP) upon request with both clients and suppliers.

EDI enables the exchange of business-critical information (purchase orders, invoices, booking requests, etc…), through a set of protocols, with the bulk of Sonae's Arauco trading partners by electronic process, information that could, if for any reason isn't shared in real time, cause considerable constraints. As a practical example, a communications outage could prevent Sonae Arauco from informing a logistics center partner of details about one or more customer orders, resulting in the inability to route supplies to customers on time, highly affecting the entire supply chain.

Both the sales order process (client order – downstream), and the raw materials order process (order to supplier – upstream) communications are exchanged through an AS2 protocol and intercepted by a reverse proxy (SAP Web Dispatcher) before they are ready to be processed in the ERP system, as shown in Figure 7.

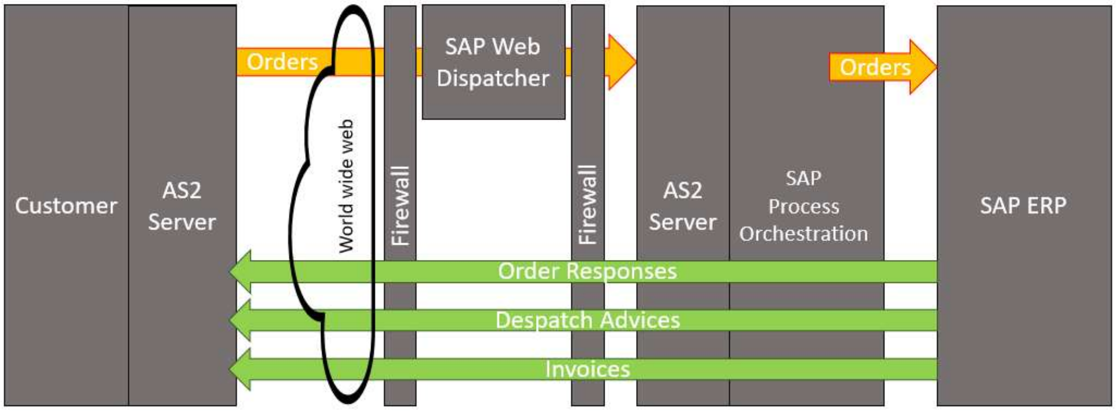

Figure 7: Data flow for business-to-business communication through AS2 for EDI

3.3.2 Scenarios to be tested/piloted using the FISHY IT-2

For iteration 2 of the FISHY validation, the complete set of scenarios are described in both Table 5 and Table 6.

Table 5: WPTV - Scenario 1

SCENARIO	Security of IoT Platform
History	V0.2
Key Actors	IT, plant IT, plant operators, Plant Maintenance
Assumptions/ Dependencies	• IoT Platform implemented and IoT devices available for testing including: • OPC-UA system • BigData system • Shopfloor Control system

	• FISHY platform components have been installed and are running
Objective(s)	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: a) ensuring accurate in-time exchange of information; b) ensuring continuous delivery of service monitoring and identifying risks, threats and incidents; c) Raising alarms when risk levels rise.
Description	The IoT platform addresses 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 also makes a prediction of which types of defects can occur 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. Step 1) IoT devices reading information from the process (Temperature, moisture, …) FISHY inspects IoT device connectivity logging (Wi-Fi controller) to detect rogue devices Step 2) Readings are stored in a local SQL Database FISHY inspects OS logging to detect brute force attacks to the SQL Database host Step 3) Data is read into an OPC-UA Server FISHY inspects OS logging to detect brute force attacks to the OPC-UA server Step 4) Data is received by an OPC client in the Edge Runtime and published into the Edge Hub FISHY inspects OS logging to brute force attacks to the Edge Runtime Server Step 5) The information is enriched with metadata, thresholds and alarms Step 6) The enriched data is sent to the IoTHub (Cloud) FISHY inspects the traffic metrics to detect Denial of Service attacks Step 7) A web application reads the data from the IoTHub and displays it in real-time”
Services/Functionalities	IRO, TIM, SCM, SPI, SIA

Metrics	Described on chapter 4 of this document

Table 6: WPTV - Scenario 2

SCENARIO	**Security of EDI Communications**
History	V0.1
Key Actors	IT, SAP Applicational Administrator
Assumptions/ Dependencies	• FISHY platform components have been installed and are running • Using http communication with trading partners through electronic data interchange in a Red Hat Linux System
Objective(s)	To validate FISHY mechanisms for ensuring the security and cyber resilience in the communications with trading partners (suppliers and clients) through EDI, with the purpose of: a) ensuring accurate in-time exchange of information; b) ensuring continuous delivery of service monitoring and identifying threats (i.e. denial of service attack); c) ensuring on-time communication with strategic partners when system malfunction occurs; d) ensuring actuation to stop an attack once it is identified
Description	EDI allows to manage all invoices, orders, expeditions and other related messages within customers and suppliers in the most efficient way. Electronically sends and receives documents in a structured format according to a defined set of standards established between Sonae Arauco and their trading partners. In turn, this creates a secure and paperless way to directly connect to each of your partners. EDI uses AS2 (Applicability Statement 2) a http-based protocol to transmit messages safely, cheaply and quickly. EDI process flow encompasses the transmission, message flow, document format and the software that is able to interpret the documents received. Being an essential tool to connect business partners (business-to-business integration) this is a critical infrastructure for the company and if a security issue causes the malfunction or stoppage of this communication window it could consequently harm or even freeze any transactions with such partners until the problem is solved, fully disrupting the flow on the entire supply chain. Basic process flow: Step 1) Customer sends order through AS2 server (public internet) Step 2) The entry point to this external request is the (SAP) web dispatcher – a reverse proxy. Step 3) Connection is established to the SAP Process Orchestration subsystems using HTTP request Step 4) FISHY secures that these requests are valid and legit Step 5) SAP Orchestration communicates the order with SAP ERP Step 6) Order response, dispatch advice and invoices are communicated back as a response from SAP ERP.

Services/Functionalities	IRO; TIM; FISHY Dashboard; EDC
Metrics	Described on chapter 4 of this document.

3.3.3 UML diagram

The following UML diagram (Figure 8) depicts the use cases involved in the WPTV scenario described above.

The use cases directly related to FISHY are marked in black bold. The ones numbered in green are exclusive from iteration 2.

Regarding scenario 1, the first use case needed to deploy all others is the introduction of a new IoT device in the network, which will then be tested for legitimacy and registration encompassed in both use cases 2 and 3. The 4th scenario is about analysing network traffic patterns and possible suspicious fluctuations. Then, both use cases 5 and 6 are exclusive from scenario 2, they introduce the communications between external partners and our ERP system, SAP, which implies the need of a new actor, the "SAP application administrator" who should have visibility of both existing attacks and all the expected consequences for the overall system from the attack itself and from the incident resolution actuation by FISHY (for instance, the ceasing of all communication via EDI for a certain period to block the attack) in order to be alerted to work on mitigation actions.

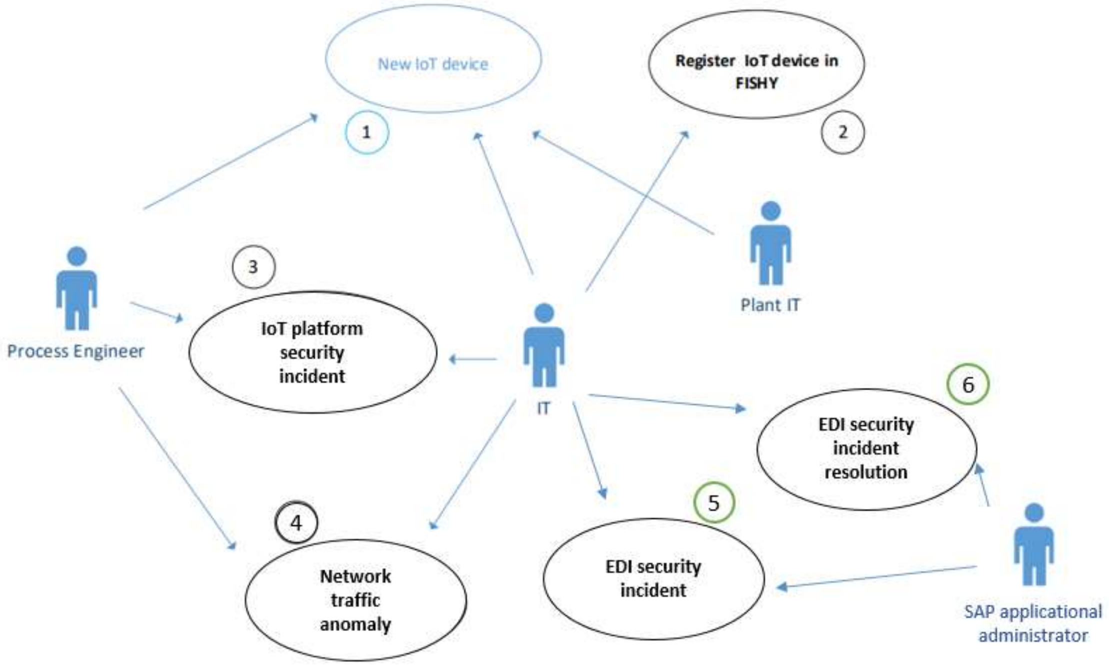
New IoT device
1
Register IoT device in FISHY
2
Plant IT
3
IoT platform security incident
Process Engineer
IT
6
EDI security incident resolution
5
4
Network traffic anomaly
EDI security incident
SAP applicational administrator

Figure 8: UML diagram for the WPTV supply chain case

3.3.4 UML Use cases

Table 7: UML Use cases SON_UC1

USE CASE Description	
ID	**SON_UC1**
Name	New IoT Device
Actors	Process Engineer, Plant IT, IT
Storyline	- 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. - Plant Maintenance technician installs the new IoT device locally. - Plant IT configures the IoT device. - IT handles all actions in Connected Factory so that the data captured is then used in the pre-defined purpose.
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 8: UML Use cases SON_UC2

USE CASE Description	
ID	**SON_UC2**
Name	Register IoT device in FISHY
Actors	IT administrator
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 9: UML Use cases SON_UC3

USE CASE Description	
ID	**SON_UC3**
Name	IoT platform Security incident
Actors	IT, Process Engineer
Storyline	A security incident is detected in one of the components of the IoT platform. TIM module of the FISHY platform will issue an alert and perform the analysis of the impact that the incident may have on the organization.
Trigger events	Security incident in IoT platform
Preconditions	Incident management process known by FISHY Business and Technical Metrics defined
Postconditions	Proceed with the resolution of the incident
Related scenarios	scenario 1

Table 10: UML Use cases SON_UC4

USE CASE Description	
ID	**SON_UC4**
Name	Network traffic control anomaly
Actors	IT, Process Engineer
Storyline	A traffic anomaly (unusual network behaviour) is detected in the network by the controller. FISHY platform will issue an alert on the anomaly and perform the analysis of the impact that the incident may have on the organization, also raising the level of cyber-risk
Trigger events	Abnormal network traffic
Preconditions	Network traffic patterns analysed
Postconditions	Information is accurate and available in real time to the FISHY administrator.
Related scenarios	scenario 1

Table 11: UML Use cases SON_UC5

USE CASE Description	
ID	**SON_UC5**
Name	EDI security incident
Actors	IT; SAP application administrator

Storyline	A security incident is detected in the SAP web dispatcher. FISHY platform will issue an alert and perform the analysis of risk and impact that the incident may have on the organization
Trigger events	Request flooding via fake URLs, multiple failed login attempts, malicious functions or URLS
Preconditions	Web dispatcher normal activity known by FISHY platform Known malicious URLs pre-identified Business and Technical Metrics defined
Postconditions	Inform strategic trading partners of the malfunctions in the system
Related scenarios	scenario 2

Table 12: UML Use cases SON_UC6

USE CASE Description	
ID	**SON_UC6**
Name	EDI Incident resolution
Actors	IT, SAP Application administrator
Storyline	Following the identification of the incident FISHY platform will proceed with an action to stop the incoming attack
Trigger events	Security incident in web dispatcher
Preconditions	Incident management process known by FISHY Business and Technical Metrics defined
Postconditions	Incoming malicious requests are stopped
Related scenarios	scenario 2

3.4 Securing Autonomous Driving Function at the Edge (SADE)

3.4.1 Introduction (SADE)

This section details the scenario and use-cases considered for the SADE supply chain during iteration 2 of the FISHY validation. Given **REMOTIS**, an autonomous vehicle, the aim of this FISHY use case is to apply a security layer to secure information about sensors (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. In figure 9 we show a small diagram of how, adding the SIA to the different functional modules of the infrastructure, this enables communication between them, regardless of their location at the network/domain level.

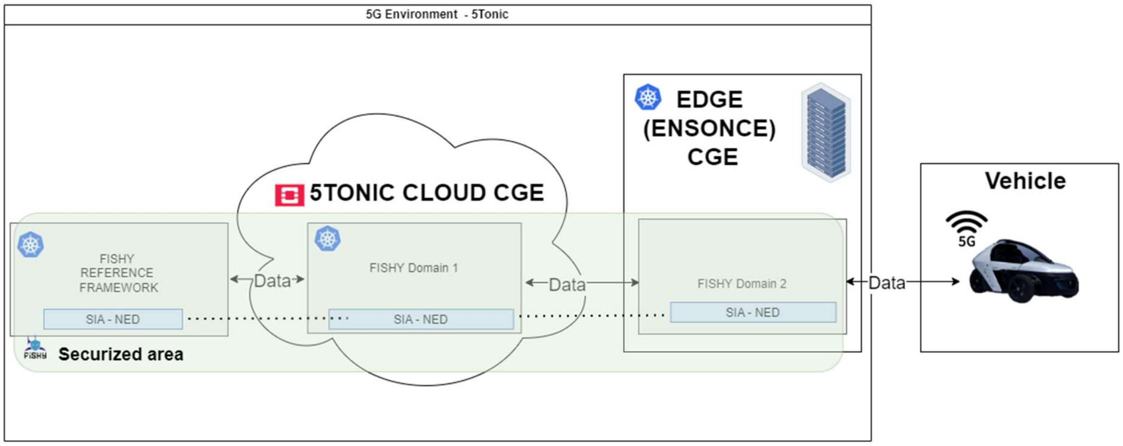

Figure 9: SADE Use case global environment image

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

For that purpose and as representative of the current trends in the 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-2

At this section, the two main use cases are described. At first, the securization of the car and its future owner information to establish that connection between car and owner, and to allow him to be identified by the face recognition system. And secondly, when the owner has the car, the monitoring of the whole private data exchange between the car and the FISHY platform.

Table 13: 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	• The local operator and dealer are registered in FISHY platform. • FISHY platform components have been installed and are running. • FISHY IRO and dashboard are operational, and actors have been registered. • Car is built and ready at car dealership.
Objective(s)	FISHY will provide/manage access to private and sensitive Data. Data will be anonymized and protected.
Description	Step 1) Local Operator has 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	Dashboard, IRO, SPI
Metrics	The metric is detailed in chapter 4 in this document.

Table 14: 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	• The local operator, dealer and owner are registered in FISHY platform. • The car was registered at FISHY platform by local operator. • Dealer added owner's information at FISHY platform (personal data and Face model). • FISHY platform components have been installed and are running. • FISHY IRO and dashboard are operational. • The owner has the car.
Objective(s)	Manage access to Private Data Sensitive data will be anonymized and protected Apply a homogenous and consistent continuous secure software development life cycle. Identify security assets of the cars. 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. Detect potential risk raising alerts when some specific threats were detected.

Description	This scenario tries to demonstrate the capabilities of the FISHY platform to secure an automotive industry environment, related to the connected car. This scenario addresses the management of the IoT devices embedded in the different vehicles. Each vehicle will send information about current software versions to be monitored. Also, FISHY platform will provide the means to manage sensitive data between the EDGE and the Cloud, like this software information or face images to allow the driver to power on the vehicle. Finally, it is expected to detect critical data compromised and perform mitigation actions over the vehicle infrastructure.
Services/Functionalities	DASHBOARD, IRO, SCM, TIM, EDC, SPI, SIA
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.

In the diagram we can see the three actors involved in the interaction with the system. The first two actors, Local Operator and Dealer, are responsible for registering the vehicle in the system and initializing the vehicle with the owner's data. In addition, they should be able to make fixes on compromised cars, order checks and claim vehicles for patch level fixes.

Finally, the Owner, to use the vehicle, will have to turn it on, thus interacting directly with the system. In addition, indirectly, it will work as a passive responsible in the different checks that the vehicle sends to the system, which can produce an alarm that the owner will receive.

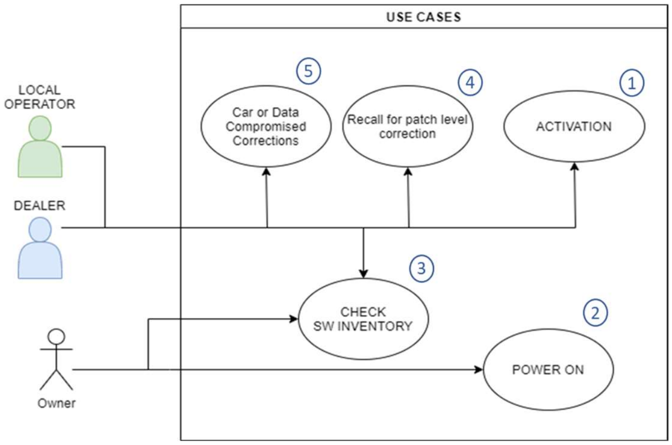

Figure 10: UML diagram of SADE use cases

3.4.4 UML Use Cases (SADE)

Table 15: UML Use cases SADE_UC1

USE CASE Description	
ID	SADE_UC1
Name	Activation
Actors	Local Operator, Dealer
Storyline	Local operator introduces information about the car once it is available in the market. This information should be at least VIN (Vehicle identification number), manufacturer, model and country of activation. 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, so dealer must upload a set of photos of the owner's face. (Already, this functionality is provided using the dashboard.) The data will be securely stored in the database.
Trigger events	New car is sold
Preconditions	• The car has a VIN known by Local Operator. • The car is sold.
Postconditions	Private data information about car and owner is securely stored in the database
Related scenarios	Scenario 1

Table 16: UML Use cases SADE_UC2

USE CASE Description	
ID	SADE_UC2
Name	Power On
Actors	Owner
Storyline	1. Owner opens the car and inserts the first key which powers on the system. 2. Car will ask to the ENSCONCE which is the closest Edge and starts to interact with it. 3. Car start checking at the registry if the VIN of the vehicle is valid, and if it is registered into the FISHY platform. If it is not valid will be rejected. 4. A ROS ID will be created, and Car will publish camera info to be checked in a biometric authorization module. 5. Camera information is a photo of the driver's face and is sent to the Edge (ENSCONCE) using ROS2 communications. 6. One service of the SADE Use case will sync data about the vehicle and biometric information, checking if the driver is allowed to start the car. If he is not allowed (eligible), 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.
Trigger events	Owner tries to start the car
Preconditions	Car was activated
Postconditions	Car's battery is powered on and car is ready to start driving.
Related scenarios	Scenario 2

Table 17: UML Use cases SADE_UC3

USE CASE Description	
ID	SADE_UC3
Name	Software patch level certification
Actors	Local operator, dealer, owner
Storyline	Any actor could access to the dashboard in order to check firmware versions of assets in a car. After checking that user is allowed, FISHY platform will request the list of all available software information about the car. This information will be published periodically in a RabbitMQ deployed in the cloud as a service . There is a service deployed in the Edge (ENSCONCE) named "Request Inventory", which is in charge of feeding that software information into the RabbitMQ. SACM will compare the software information from RabbitMQ with the software certifications provided by OEMs. This software certificated as safe will be recovered through a REST API.
Trigger events	One actor accesses the dashboard and requests software information about a vehicle
Preconditions	Car was activated and powered on.
Postconditions	Listed information about firmware versions of car assets.
Related scenarios	Scenario 2

Table 18: UML Use cases SADE_UC4

USE CASE Description	
ID	SADE_UC4
Name	Patch Level Correction
Actors	Local operator, dealer
Storyline	Any actor could access to dashboard to check if there is any alert about firmware versions and inform owners to recall a car. The dealer will upgrade any firmware compromised by a vulnerability.
Trigger events	A device's firmware has a vulnerability. An actor or FISHY platform informs the owner because an alert has been raised.

Preconditions	Car was activated and powered on.
Postconditions	Owner is informed with an email that car must be checked at car's dealership.
Related scenarios	Scenario 2

Table 19: UML Use cases SADE_UC5

USE CASE Description	
ID	SADE_UC5
Name	Car compromised
Actors	Local operator, dealer
Storyline	When FISHY platform 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. The platform will send an order to stop the autonomous driving. This order is sent to the vehicle server deployed in the EDGE (ENSCONCE) and it will send a notification to the car to inform the car will be offline. Information about ROS ID will be removed from the database. Car should be offline from that moment.
Trigger events	Application at the Edge or private data in the Cloud was compromised
Preconditions	Car was activated and powered on.
Postconditions	APP ID ROS ID instances are deleted from the Edge. Car is offline from this point.
Related scenarios	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 on the pilot activities using iteration-2 of the FISHY platform, we present the metrics we aim to evaluate and the methodology we will pursue, adopting the following table (Table 20) as a template. 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 maintain a common understanding between the pilot partners and the FISHY technical partners developing the FISHY platform.

Table 20: Template of validation metric description

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

4.2 Farm-to-Fork Supply Chain

Table 21: Farm to Fork use case: Metric description SC1_B1

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

Methodology	In the scenario 1, a set of 2 ledgers are involved. These two ledgers communicate through the interledger components: To validate and demonstrate this, we will 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
Involved components	SACM (for the registration and the auditing), TIM, IRO

Table 22: Farm to Fork use case: Metric description SC1_T1

Metric description	
ID	SC1_T1
Name	Number/Types of threats that can be detected
Type	Technical
Target value	4
Methodology	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.
Involved components	TIM

4.3 Wood-based Panels Trusted Value-Chain

Table 23: Wood-based Panels Trusted Value-Chain; Metric description SC2_B1

Metric description	
ID	SC2_B1
Name	Unregistered IoT devices in the network
Type	Business and technical
Target value	1
Methodology	The WLAN controller of Sonae Arauco monitors in real-time the VLAN of the IoT devices and sends 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). To validate, Sonae Arauco will:

	- Register all existing IoT devices on FISHY - Add a "temporary" not registered IoT device in the network FISHY will: - Identify the new IoT device and verify if it is registered - If not registered, open an incident to the administrator that will be opened until any action from the administrator.
Involved components	WLAN Controller (from Sonae Arauco) SPI, TIM, IRO
Comments	Identified target value is a reference for the pilot as if one rogue device is detected, any similar can also be detected.

Table 24: Wood-based Panels Trusted Value-Chain; Metric description SC2_B2

Metric description	
ID	SC2_B2
Name	IoT Hub telemetry sent from Edge
Type	Business
Target value	volume of telemetry < as the minimum historic
Methodology	OPC-UA server (EDGE component) collects in real time telemetry values that will be sent to the IoT HUB. Whenever the volume of telemetry collected is lower than the historic minimum, we are facing with an incident that must be immediately addressed (critical). To validate, Sonae Arauco will: - Identify a reference historical minimum - Simulate one incident with telemetry below historical minimum FISHY will: - Notify/alert about anormal telemetry values - Raise specific risk model level of risk - Raise overall system level of cyber-risk
Involved components	IoT HUB (From Sonae Arauco) SIA, SCM, TIM, IRO
Comments	Identified target value is a reference for the pilot. Due to the criticality of this process, Sonae Arauco will have a redundant alarm system during the pilot.

Table 25: Wood-based Panels Trusted Value-Chain; Metric description SC2_T1

Metric description	
ID	SC2_T1
Name	Unauthorised access – Windows system
Type	Technical
Target value	Same user login or 5 failed logins' in less than 60 secs
Methodology	If suspicious unauthorized access appears in one Windows system, then FISHY notifies/alerts and "Administrator" starts the incident process. Suspicious access might happen through: - Login with the same user in different servers/IP's in less than 60 seconds - If a bypass login is detected - at least 5 failed logins in less than 60 seconds To validate Sonae Arauco will: - Simulate both defined scenarios for suspicious access FISHY will: - Notify/alert the existence of suspicious access - Raise specific risk model level of risk - Raise overall system level of cyber-risk
Involved components	OPC-UA Server and IoT Edge server (From Sonae Arauco) TIM, IRO, dashboard
Comments	

Table 26: Wood-based Panels Trusted Value-Chain; Metric description SC2_B3

Metric description	
ID	SC2_B3
Name	Network traffic anomaly
Type	Business
Target value	Network traffic is > (higher) or < (lower) than the expected by historic patterns
Methodology	Anomaly detection caused by unusual network behavior like heavy traffic flow during otherwise 'quiet' hours (based on historic data analysis). To validate Sonae Arauco will: - Simulate scenario of heavy traffic or reduce FISHY control value below what is expected by historic data FISHY will: - Notify/alert the network anomaly

	- Raise specific risk model level of risk - Raise overall system level of cyber-risk
Involved components	IRO, dashboard, TIM
Comments	

Table 27: Wood-based Panels Trusted Value-Chain; Metric description SC2_B4

Metric description	
ID	SC2_B4
Name	EDI types of attack that can be detected and actuated
Type	Technical
Target value	3
Methodology	EDI communication via HTTP always reaches the ERP through a reverse proxy that has some vulnerabilities. The detection of the potential threats/attacks described in section 5.3 will be based on the demonstration of the execution of the rules defined in the same section.
Involved components	TIM; IRO; EDC; SCM
Comments	

Table 28: Wood-based Panels Trusted Value-Chain; Metric description SC2_B5

Metric description	
ID	SC2_B5
Name	EDI transactions real time monitoring
Type	Business
Target value	Real time monitoring information available at 99% of time
Methodology	Getting the information in real time is critical for it influences productivity, efficiency of processes, costs, and customer satisfaction. Therefore, EDI communication will be continuously tested be FISHY regarding response availability. If response is unavailable FISHY will raise an alert FISHY will: - Continuously monitor SAP web dispatcher availability in real time - Notify/alert in case of unavailability - Raise specific risk model level of risk accordingly

	- Raise overall system level of cyber-risk accordingly
Involved components	TIM, IRO
Comments	

4.4 Securing Autonomous Driving Function at the Edge (SADE)

Table 29: Driving Function at the Edge supply chain; Metric Description: SC3_T1

Metric description	
ID	SC3_T1
Name	Detect unauthorized access to the vehicle
Type	Technical
Target value	1 unauthorized access code produced by failed access attempts after a short time
Methodology	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 and a notification will be sent to the owner. To validate, Capgemini Engineering administrator needs: - Register a vehicle into the FISHY platform. - Register and upload biometric data allowed to power on the vehicle. FISHY will: - Allow access to the sensitive information when the vehicle tries to start. - Return biometric information about drivers allowed to drive the vehicle.
Involved components	SPI, SIA, IRO, EDC, TIM

Table 30: Driving Function at the Edge supply chain; Metric Description: SC3_T2

Metric description	
ID	SC3_T2
Name	Integrate inside SIA – secure biometric function
Type	Technical

Target value	Biometric functionality from the car will use SIA in order to integrate to the FISHY framework
Methodology	Integrate function through SIA in ENSCONCE platform
Involved components	SIA

Table 31: Driving Function at the Edge supply chain; Metric Description: SC3_T3

Metric description	
ID	SC3_T3
Name	Integrate inside SIA – Software update function
Type	Technical
Target value	True. SADE functionality from the car will use SIA in order to integrate to the FISHY framework.
Methodology	Integrate SADE functions with FISHY framework through SIA
Involved components	SIA

Table 32: Driving Function at the Edge supply chain; Metric Description: SC3_B1

Metric description	
ID	SC3_B1
Name	Reduce recall operation to the car's dealer
Type	Business
Target value	Fishy will allow to enforce policies to fix software versions without having a recall.
Methodology	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. To validate Capgemini Engineering needs: - Provide a list of software versions verified as safe through FISHY Platform

	- The vehicle will send some information about multiple embedded IoT devices and components and its software versions. At least one version won't be certified. FISHY will: - Identify the vehicle - Enforce a policy to update the component or inform the owner about the issue.
Involved components	SPI; SCM; SIA; EDC; IRO

5 Supply-chain specific attacks to be detected by FISHY

5.1 Introduction and functionality-to-SC case map

In this chapter, we detail the exchange of information between the IT solutions deployed in each pilot site and the FISHY platform. In other words, we describe the security probes that will be deployed and used in each FISHY pilot site.

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 11. These data are consumed by the FISHY platform.

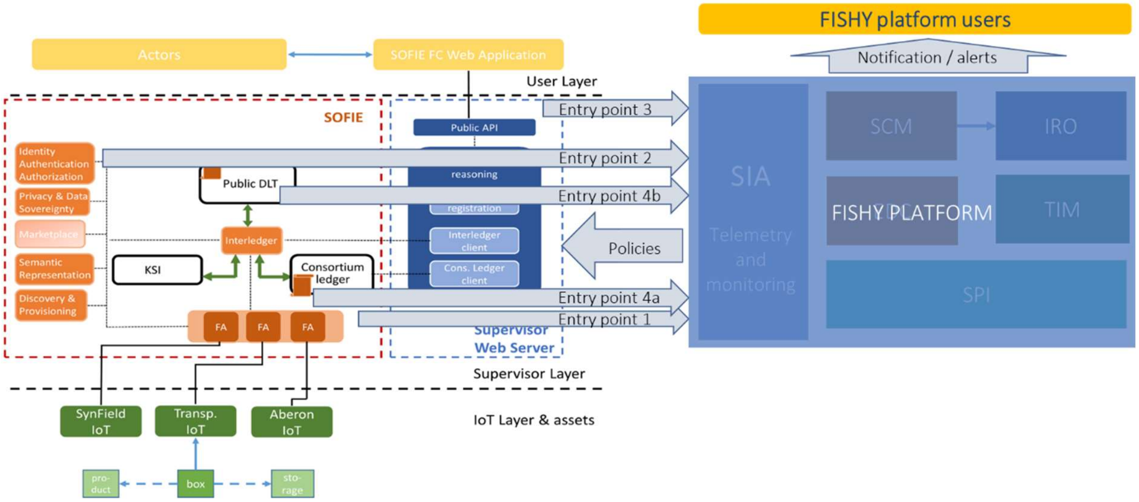

Figure 11: The F2F platform and its interconnection with the FISHY platform

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 each type, the following security rules will be applied:

Type	RULE
1	If Attacker wallet ID appears more than *Threshold1.1* times in *Threshold 1.2* hours, then • FISHY **notifies/alerts** F2F supply chain operator and/or • FISHY **notifies** IoT Island operator and/or • FISHY **enforces** Wallet ID ban (i.e., the F2F SOFIE platform will no longer consider keeping information coming from this wallet ID).
2	If Attacker DID appears more than *Threshold2.1* times in *Threshold2.2* hours, then • FISHY **notifies/alerts** F2F supply chain operator providing the relevant log info (Attacker DID, Device name) and/or • FISHY **notifies** IoT Island operator and/or • FISHY **enforces** DID ban (i.e., the F2F SOFIE platform will no longer consider keeping information coming from this DID).
3	If IP appears more than *Threshold3.1* times in *Threshold3.2* hours, then • FISHY **notifies** F2F supply chain operator providing the relevant log info (username, IP) and/or • FISHY **enforces** IP ban (i.e., the F2F SOFIE platform will no longer accept access request from this specific IP).
4	If IP appears more than *Threshold4.1* times in *Threshold4.2* hours, then • FISHY **notifies** F2F supply chain operator providing the IP and port number and/or • FISHY **enforces** IP ban (i.e., the F2F SOFIE platform will no longer accept access request from this specific IP).

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 three distinct points of the deployed Sonae Arauco’s IoT platform (Figure 12) and one last point from the SAP web dispatcher from EDI connections (Figure 13) . Therefore, FISHY platform:

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

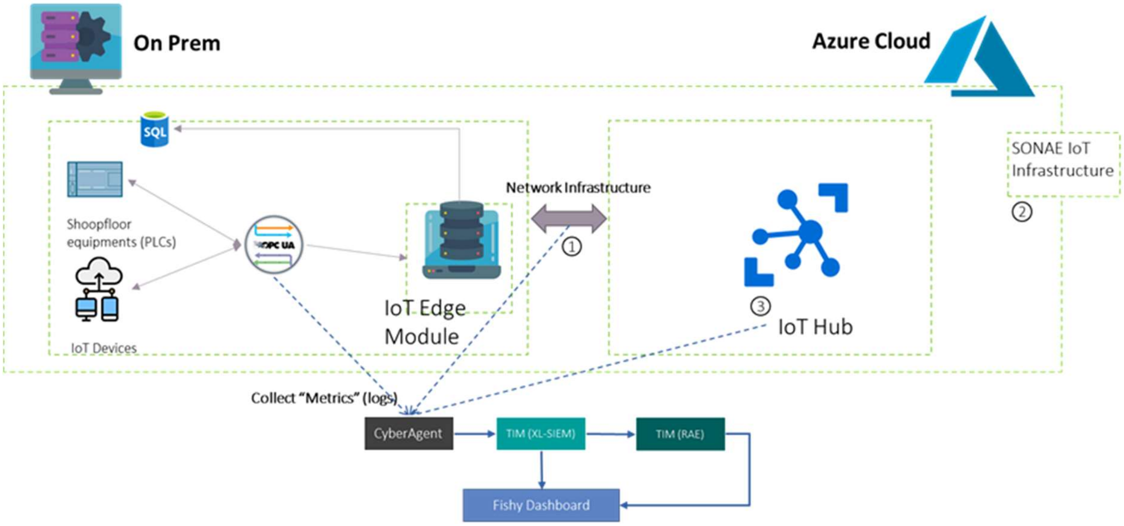

Figure 12: The Connected Factory architecture and its interconnection with the FISHY platform

- Collects information on the SAP web dispatcher (4)

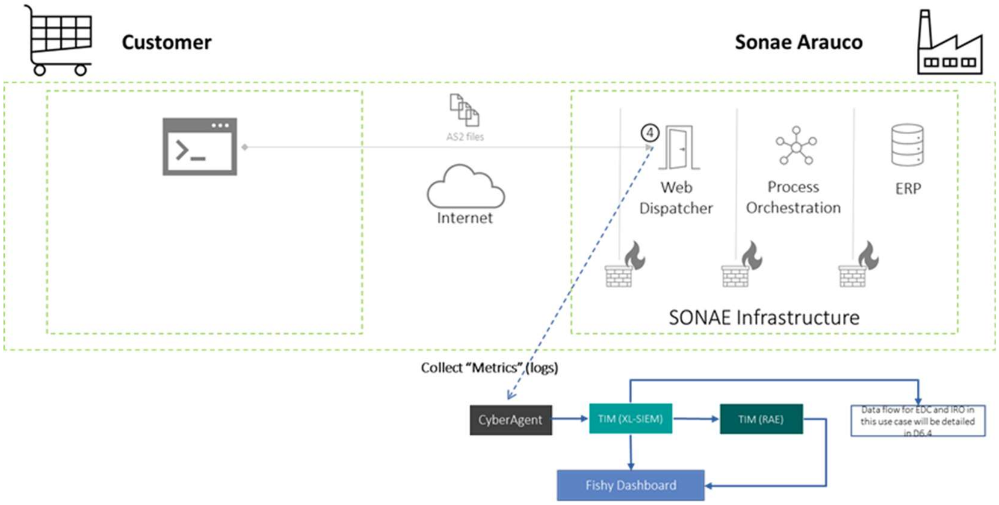

Figure 13: EDI communications architecture and its interconnection with the FISHY platform

For the iteration 2, and as described in chapter 3, the following use cases were considered:

UC1 and UC2– IoT devices management:

PRE-CONDITIONS:

- existing IoT devices on the Company are already registered on FISHY.
- Sonae Arauco's "WLAN Controller" monitors WLAN of IoT devices in real-time and sends information (LOGs) to SIA.

RULES:

- If a new device is identified in the WLAN, TIM asks to SPI if the device is registered in FISHY
    - If not, TIM open an incident to administrator
    - Administrator validates if is an authorized device
        - If authorized, Administrator registers new device and closes the incident
        - If not authorized, Administrator asks to identify existing connections from/to this device and identify potential impacts

Information collected by FISHY: IP addresses; Mac Addresses; Time Stamp

UC3 – Incident Management:

PRE-CONDITIONS:

- Pre-condition: Sonae Arauco identify "minimum historic" volume of telemetry
- IoT Hub collects the volume of telemetry (metrics) sent from Edge (OPC-UA server)
- TIM reads telemetry from IoT platform

RULES:

- TIM verifies If the volume of telemetry is lower than the minimum historic and,
    - if volume lower than the minimum historic TIM analyzes the impact,
    - and opens an incident

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

UC4 – Network traffic control anomaly:

PRE-CONDITIONS:

- Pre-condition: Sonae Arauco identifies, by pattern analysis, normal network traffic
- Zeek will continuously read network traffic

RULES:

- Zeek verifies If the network traffic volume is higher than the expected value
    - if volume is higher than expected TIM analyzes the impact,
    - and opens an incident

Information collected by FISHY: will be detailed in D6.4

UC5 and UC6 – EDI incident management

PRE-CONDITIONS:

Pre-condition: Sonae Arauco identifies normal requests activity and has the web dispatcher issuing logs with characterization of requests in real time through Suricata's sensor to XL-SIEM (TIM)

RULES:

- If abnormal activity happens with flood of requests:
    - TIM analyses the impact and opens an incident

  - EDC will enforce action by stopping incoming network requests

- If an invalid/unauthorized user tries, and fails, multiple password attempts for the same URL request
  - TIM analyses the impact and opens an incident
  - EDC will enforce action by stopping incoming requests from attacking IP adresses

- If a valid/authorized user uses a known unauthorized function or URL
  - TIM analyses the impact and opens an incident
  - EDC will enforce action by stopping incoming requests from attacking IP adresses

Information collected by FISHY: will be detailed in D6.4

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 throughout 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 14. 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, (attacks, failures in the infrastructure or data, unauthorized power on in the vehicle, etc).

DASHBOARD: presents to the FISHY user the detected security events and allow dealers to register vehicles, personal data about owners and certifications included by OEMs.

IRO: Create intents to match what is happening in the environment infrastructure with policies to be enforced to mitigate attacks, threats, etc.

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

SPI: Allows access to the information about existing vehicles, and personal data. It also controls who can access, and the type of access by using Role based model.

SIA/NED: Allows a secure communication between different domains: EDGE, Cloud, and control services. SADE Platform will be allocated into the Cloud but some specific services of the vehicle are deployed into the EDGE. Interconnection of services in the cloud with the FISHY control services will be needed perform mitigation and operations.

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 (Dashboard).
Data must be stored in a secure way using SPI module, providing secure methods to store and recover this information.

RULES

During registration:

- If vehicle is not registered the vehicle will be registered in the database.

Adding owner data:

- If a vehicle is valid, personal information about owner and drivers will be updated in the database.

UC2 – POWER ON:

In this use case, SADE will ask FISHY platform about personal information of the drivers allowed to drive the vehicle. FISHY must provide biometric information stored through the platform and SADE will check if the biometric info has the same patterns as the driver trying to start the connected car.

RULES

The car service module will ask FISHY for the biometric information allowed to power ON:

- If vehicle identification number and the request are valid, FISHY will return all biometric information related to the vehicle.
- If a vehicle is not valid or a request is coming from an untrusted source, FISHY will notify to the owner, raising an alert.

UC3 – Software Patch Level Certification

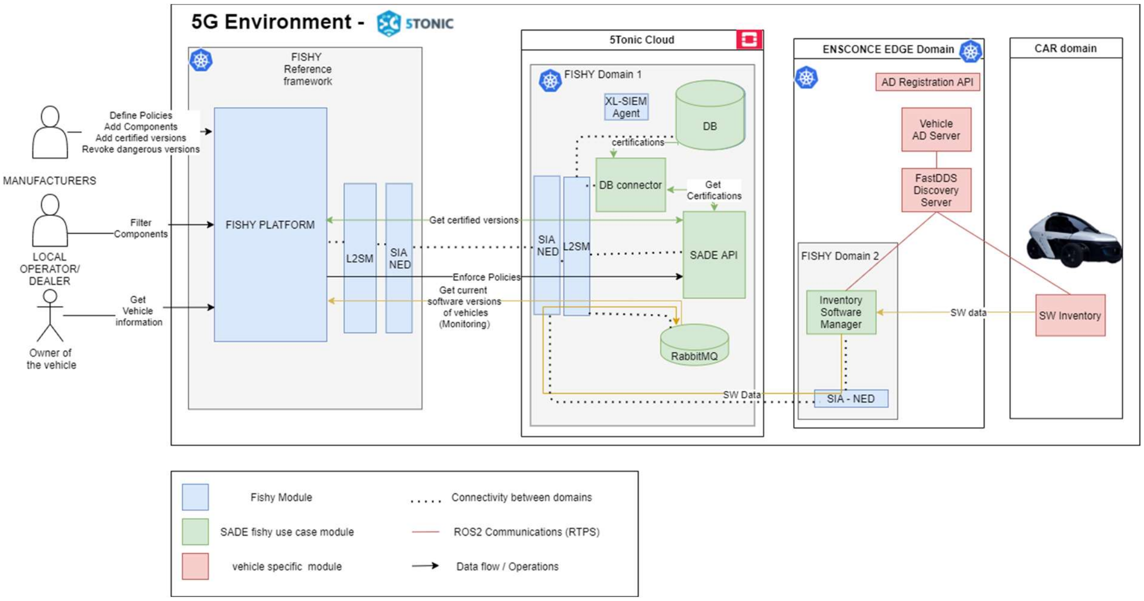

Figure 14 : SADE Use Case 3 (flow)

The following table shows an example of information that OEMs add using FISHY dashboard to certify its software versions. This information is stored in the FISHY platform.

FIELD	VALUE
Manufacturer	Capgemini Engineering
Model	TempMeterXXX

SW Version	1.1235
Safe Update Link (optional)	https://company.com/updates/TempMeterXXX/1.1235/firmware.bin
Update checksum (optional)	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 (SACM).
- FISHY compares with SW certification versions provided by OEMs (SACM).

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.

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 the administrator that the vehicle is in high level of risk.

  Administrator checks and 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 sending the notification to the owner via email.

- Administrator knows that a specific software version is dangerous and can revoke that version using the DASHBOARD. FISHY will detect that this version is no longer certified so if one vehicle has this version, one update or recall policy will be sent to the SADE platform.

UC5 – Car compromised

In this use case, the dealer or local operator will confirm a security threat and will perform an action on 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 the administrator that the vehicle or data was compromised raising an alert.
- FISHY will enforce a mitigation policy through a REST call to the SADE API which is in charge of removing all services related to the compromised car.

6 Infrastructure set up

6.1 Introduction

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

6.2 Farm-to-Fork Supply Chain

The setup is the same as for IT-1 and has been described in D6.1. The logs are passed to the FISHY platform through a RabbitMQ deployed in Synelixis own cloud infrastructure. The F2F platform administrator will be able to check the status and obtain audit certificate through the FISHY dashboard.

The main difference from the situation reported in D6.1 is the integration of the Farm to Fork IT platform with **PMEM**. PMEM is a machine learning based Intrusion Detection System (IDS) which consists of different modules installed in a distributed way. Certain modules are installed in the UPC premises while others are installed in Synelixis cloud where the F2F IT platform is also deployed.

As shown in Figure 15, the PMEM data capturing module is based on the real time data collector. This module is using the TCP-dump tool to extract the real time traffic from a specific port of the F2F router. This port contains all the incoming and outgoing traffic in the network. The raw traffic patterns are dumped in the PCAP format and are forwarded to a Virtual Machine (VM) locally deployed in the use case. The Feature extraction and Data Forwarding Module are installed in this VM. The feature extraction module is responsible for extracting the useful machine learning features needed by PMEM for the detections/predictions. These features are stored in CSV format on the local VM. The data forwarding module is a NodeJS based application which is connected to the public port for forwarding the data outside the organization. The API will wait for the client to make a request of data and the data is forwarded in JSON format after authenticating a client using a specific authentication token. Only the features needed for the detection/prediction are forwarded and no organizational information is forwarded outside the network of F2F. The Classification module which is responsible for making the prediction of the Cyber attacks on the real time traffic resided in the UPC premises. The same deployment approach will be followed in the 3rd year of the project and the emphasis will be on the detection of unknown attacks.

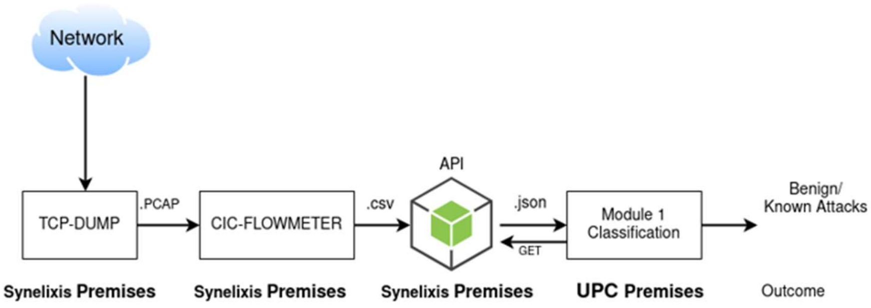

Figure 15: PMEM deployment in the Farm to Fork use case

6.3 Wood-based Panels Trusted Value-Chain

In Wood-based Panels Trusted Value-Chain use cases described in previous sections, for the pilot the IoT platform implemented in Oliveira do Hospital will be used, which comprises components in Microsoft's Cloud Azure and components in the plant (Figure 11: The F2F platform and its interconnection with the FISHY platform and the EDI communications (Figure 13).

For this purpose, the equipment's and services described in the table below will be used that will be provided by Sonae Arauco and which will be integrated into the FISHY platform.

Table 33: 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 https://www.advantech.com/products/4260f153-57cd-4102-81ea-7a0f36d9b216/wise-4012/mod_0dd63bf5-6516-4488-a6f6-9293b5b17eff	
WIFI-sensor	Digital IoT sensor that collects several parameters such as temperature, humidity, speed, position, levels, etc. Brand: Advantech Model: WISE-4220 QTY: 7 https://www.advantech.com/products/229f9f5b-d073-4cc2-ac54-d90147e04c12/wise-4220/mod_c4851078-f819-4e6d-b597-4ba15b7e1266	
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 https://www.cisco.com/c/en/us/support/wireless/aironet-1542i-outdoor-access-point/model.html	

Switches	Equipment located in the production area where the WIFI antennas are connected Brand: CISCO Model: ws-c2960X-24PS-L QTY: 3 https://www.cisco.com/c/en/us/support/switches/catalyst-2960x-24ps-l-switch/model.html	
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 https://www.cisco.com/c/en/us/support/wireless/2504-wireless-controller/model.html	
IoT HUB	Central message Hub located in the Cloud (Azure) that provide communication between IoT applications and IoT devices. Brand: Microsoft QTY: 1	
OPC-UA Server	Server located in the plant that have the OPC-UA installed. OPC-UA is used to exchange industrial data and applications. Type: VM Hyper-V OS: Windows Server 2019 std QTY: 1	OPC UA
PRTG	Monitoring solution that monitors the local network in real-time all equipment's except WIFI. https://www.paessler.com/prtg	PRTG NETWORK MONITOR
SAP Web Dispatcher	Entry point for HTTP(s) requests from trading partners into SAP ERP system, that can either reject or accept connections. https://help.sap.com/docs/ABAP_PLATFORM/683d6a1797a34730a6e005d1e8de6f22/488fe37933114e6fe10000000a421937.html	SAP

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. A general view of the platform deployed to validate de SADE use case could be seen in Figure 9.

Here are some of the embedded components within the vehicle.

Table 34: Some of the Equipment embedded in the vehicle

Equipment	Role in pilot	View
Modem 5G	5G modem used for prototyping. Brand: Quelctel Model: RM500Q Web reference: http://sekolab.com/products/camera/	
Other network components	To be provided by the 5TONIC among the pools of providers available there supporting from NSA to SA Web reference: https://www.5tonic.org/	5TONIC
AD Enabled vehicle	AD Enabled vehicle including NVIDIA compute module. Brand: Nvidia Model: Drive AGX Xavier Web reference: https://developer.nvidia.com/drive/drive-agx	
Camera	Brand: Logitech Model: C920 PRO HD Web reference: https://www.logitech.com/en-gb/products/webcams/c920-pro-hd-webcam.960-001055.html	

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 Openstck). 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

7 Concluding remarks

This deliverable has presented the methodology of evaluation of the 2nd version of the FISHY 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-2 platform. This deliverable will be the roadmap for the 2nd and final round of evaluations that will take start in M33. To ensure high-quality of assessment results, FISHY consortium pays attention to the following set of points:

- The deployment information provided in the previous chapters is the result of a) experience from the 1st round of evaluation and b) discussions between technical and use-case partners. However, we consider that there may be a need for modifications as the FISHY platform development proceeds so as to shed light, evaluate and demonstrate as many aspects and functionalities of FISHY as possible.
- In this document, FISHY use case partners have defined a set of attacks of interest to them. These are fully in line with the attacks on the supply chain presented in [4], where it is mentioned that the number of attacks in the supply chain proliferates. Of high interest to all the use case is the PMEM module of FISHY which detects anomalies (i.e., is capable of detecting unknown attacks). FISHY use case partners will map the addressed attacks to the categories defined in [4] in D6.4 where the overall and final evaluation of FISHY will be included.

8 References

[1] FISHY, D2.2 “IT-1 architectural requirements and design”, 2021

[2] https://www.synfield.gr/

[3] https://www.kaaiot.com/

[4] ENISA, THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS, 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021