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

D2.4 Final Architectural design and technology radar

Document Identification			
Status	Final	**Due Date**	28/02/2023
Version	1.0	**Submission Date**	06/03/2023

Related WP	WP2	**Document Reference**	D2.4
Related Deliverable(s)	D2.1, D2.2, D2.3, D2.5, D2.6, D3.3, D3.4, D4.3, D4.4, D5.1 and D6.3	**Dissemination Level (*)**	PU
Lead Participant	TUBS	**Lead Author**	Admela Jukan, Jasenka Dizdarević, Francisco Carpio
Contributors	ATOS, SYN, XLAB, TID, UPC, POLITO, OPT, Sonae, STS, Uminho, Capgemini	**Reviewers**	Jan Antič, Hrvoje Ratkajec, XLAB
			Nelly Leligou, SYN

Keywords:
Architectural design, technology radar, cyber resilience constraints and 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.

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
Admela Jukan, Jasenka Dizdarević, Francisco Carpio, Mounir Bensalem	TUBS
Alexandra Lakka, Aggelos Orfanoudakis	SYN
Chrysanthos Chrysanthou, Tzortzia Koutsouri, Sofia Spanoudaki	STS
Joao Pita da Costa, Jan Antič, Hrvoje Ratkajec	XLAB
Eva Marin Tordera	UPC
Iván Vidal Fernández	UC3M
André Oliveira, Henrique Santos	UMinho
Daniele Canavese, Cataldo Basile	POLITO
Jorge Martinez Olmo	ATOS
Rui Guilherme Gonçalves	SONAE
Jose Soriano Diaz, Miguel Juaniz Lopez	CAPGEMINI

Document History			
Version	Date	Change editors	Changes
0.1	19/10/2022	Jasenka Dizdarević, Francisco Carpio (TUBS)	Table of content
0.2	02/12/2022	All partners	Added first versions of sections 2, 3 and 4
0.3	09/12/2022	All partners	Extended sections 2, 3 and 4
0.4	27/12/2022	Joao Pita da Costa (XLAB)	Added first version of section 5
0.5	28/12/2022	Francisco Carpio (TUBS)	Added first versions of section 6
0.6	6/2/2023	Alexandra Lakka (SYN), Rui Guilherme Gonçalves (SONAE), Miguel Juaniz Lopez(Capgemini)	Extended section 3.3
0.7	08/2/2023	Jorge Martinez Olmo (ATOS)	Added contents to section 5.1
0.8	14/2/2023	Hrvoje Ratkajec (XLAB)	Added contents to sections 4.3.1 and 4.3.6
0.9	15/2/2023	Jasenka Dizdarević, Francisco Carpio (TUBS)	Internal review
0.91	22/2/2023	Hrvoje Ratkajec (XLAB)	Revision from XLAB

0.92	23/2/2023	Nelly Leligou (SYN)	Revision from SYN
0.93	24/2/2023	Francisco Carpio (TUBS)	Version for QA
0.95	27/2/2023	Antonio Álvarez Romero (ATOS)	QA
0.96	28/2/2023	Jan Antič, Hrvoje Ratkajec (XLAB)	QA addressed
0.97	1/3/2023	Jasenka Dizdarević (TUBS)	FINAL VERSION TO BE SUBMITTED
1.0	03/03/2023	Antonio Álvarez, Juan Alonso (Atos)	Quality assessment and final version to be submitted.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Admela Jukan, Jasenka Dizdarević, Francisco Carpio (TUBS)	02/03/2023
Quality manager	Juan Andrés Alonso (ATOS)	03/03/2023
Project Coordinator	Antonio Álvarez (ATOS)	03/03/2023

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AD	Advanced Driving
ADAS	Advanced Driving Assistance Systems
AI	Artificial Intelligence
API	Application Programming Interface
CEF	Common Event Format
CLIPS	C Language Integrated Production System
CON	Constraint
CPC	Cooperative Patent Classification
CSP	Communications Service Provider
D2.4	Deliverable number 4 belonging to WP2
EC	European Commission
EDC	Enforcement and Dynamic Configuration
EDI	Electronic data interchange
ETSI	European Telecommunications Standards Institute
F2F	Farm to Fork use case
GUI	Graphical User Interface
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IPO	Intellectual Property Office
IRO	Intent-based Resilience Orchestrator and Dashboard
JSON	JavaScript Object Notation
JWT	JSON Web Token
KER	Key Exploitable Results
KPI	Key-Performance Indicators
MEC	Multi Access Edge Computing
NBI	Northbound Interface
NED	The Network Edge Device
NFV	Network Function Virtualisation
NSF	Network Security Function

Abbreviation / acronym	Description
OF	Orchestration Function
OIDC	OpenID Connect
PoC	Proof of Concept
RAE	Risk Assessment Engine
REQ	Requirement
SACM	Security Assurance & Certification Manager
SADE	Secure Autonomous Driving function at the Edge
SBI	Southbound Interface
SEN	Secured Edge Node
SIA	Secure infrastructure Abstraction
SLA	Service Level Agreement
SPI	Secure and Privacy Data Space Infrastructure
TIM	Trust and Incident Manager
TM	Trust Manager
TPM	Trusted Platform Module
UC	Use case
VNF	Virtual Network Function
WBP	Wood-based Panels use case
WP	Work Package
WPTV	WPTV Wood-based Panels Trusted Value-Chain
XACML	Extensible Access Control Markup Language
XL-SIEM	Cross-Layer Security Information and Event Management

Executive Summary

This document, developed by the FISHY project, represents the final version (iteration IT-2) of the FISHY architectural solution for cyber resilience provisioning in ICT-based supply chains, and is the main outcome of the work done in WP2 tasks "T2.1 - Research and technology radar, and business models", "T2.2 - Cyber resilience related constraints and requirements" and "T2.3 - Architectural design". This deliverable offers an overview of the updated FISHY architectural design, related constraints and requirements and of technology radar after adopting the necessary modifications from the previous versions documented in deliverables D2.2 [1] and D2.3 [2]. The identified and described modifications are necessary for a successful development of the architectural design in IT-2.

The high-level conceptual specification of the FISHY architecture is described in detail in Section 2 of the deliverable, along with the evolution of the architecture from its first proposed version until its final modifications required for the successful deployment of the FISHY Platform. Section 3 provides the updated description of the individual architectural modules, and the description of newly introduced ones, as well as the description of the high-level communication between modules is explained. Then, in Section 4, the focus is on the updated requirements and constraints which need to be satisfied and met by the final architectural solution, as a result of the task "T2.2 - Cyber resilience related constraints and requirements". This section also includes an updated mapping of the use cases to the final reference architecture. It is followed by Section 5, which gives an overview of the final stage of the FISHY Radar, providing an update on the technology market, as well as the extensions of the research, legal and regulatory landscapes.

The outcome of this document is an updated detailed final architectural design of the FISHY solution, and an updated FISHY radar that is the compass for FISHY exploitation.

1 Introduction

1.1 Purpose of the document

This document describes the final architectural design of the FISHY solution. It identifies and describes necessary modifications in architectural design and components of the FISHY system, as well as in its related constraints and requirements for IT-2, based on the knowledge gained during the practical implementation and integration with pilots in IT-1. It proposes updated solutions for the individual components, including the updates in the communication and interfaces design. In addition, it reports on the last updates of the FISHY technology radar.

1.2 Relation to other project work

This deliverable builds on the work done in all of the tasks of WP2. It updates the technology radar and cyber resilience related requirements and constraints, described and analyzed in tasks T2.1 (inc. D2.1 [5]) and T2.2, respectively. The focus of the task T2.3, has been on the update of the FISHY architectural design. To this end, we took into consideration updated designs and implementation insights of WP3 and WP4 system components Trust Manager (TM) and Security and Certification Manager described in D3.4 [13] and D4.4 [41], respectively, to ensure coherent alignment. In addition to considering WP3, WP4 and WP5 development efforts, the overall FISHY Platform implementation and integration with pilots, as reported in D6.3 [6] have influenced the updates in the architectural design for IT-2.

1.3 Structure of the document

This document is structured in the following way:

Section 2 gives the high-level conceptual specification of the FISHY architecture for IT-2, describing the evolution from the version released in IT-1.

Section 3 describes the FISHY platform building components, highlighting the modifications adopted for IT-2, as well as the inter-component communication aspects of the FISHY Platform.

Section 4 details a modified list of functional and non-functional requirements as imposed on the FISHY Platform by pilots.

Section 5 describes the final stage of the FISHY Technology Radar.

2 FISHY system description

This section describes the high-level conceptual specification of the FISHY architecture. We start by describing the evolution of the architecture from the first version described in the proposal, its refinement in D2.2 until the final version in IT-2, including the limitations from the version released in IT-1. Then, we follow up describing the final reference architecture and revisiting the action areas of concern already introduced in IT-1.

2.1 Evolution of architecture design in IT-1

The preliminary version of the FISHY architecture presented in the FISHY proposal is shown in Figure 1. It consisted of a set of building modules which included: 1) Intent-based Resilience Orchestrator & Dashboard (IRO), 2) Security Assurance & Certification Manager (SACM), 3) Trust and Incident Manager (TIM), 4) Enforcement and Dynamic Configuration (EDC), 5) Security and Privacy Data Space Infrastructure (SPI), and 6) Secure Infrastructure Abstraction (SIA).

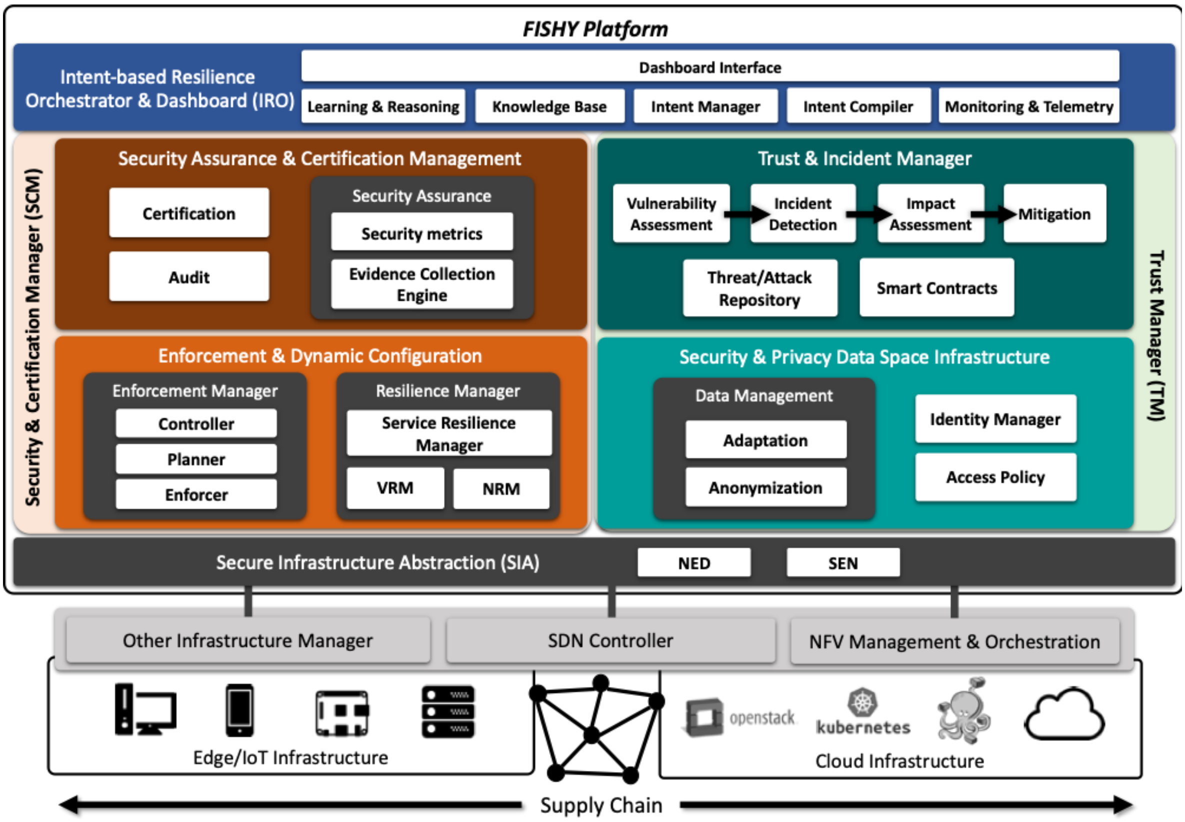

Figure 1: FISHY original proposal architecture

Next, we give an overview of each one of the different modules:

IRO: is in charge of translating security requirements within the FISHY Platform into intents and in turn corresponding security workflows and policies. IRO also includes a dashboard interface for system security, control and performance monitoring facilitation.

SACM: coordinates the monitoring process, the automated evidence-based security reporting and the certification towards ensuring that the required security policies are correctly implemented.

TIM: includes tools, such as vulnerability and risk estimation, along with incident detection and management, with a goal of developing mechanisms, which would ensure security assessment of the stakeholder’s supply chains.

EDC: is in charge of security policies enforcement and configuring the specific infrastructure and network security functions (NSF) to ensure resilience.

SPI: is in charge of identity management, access policy and data management procedures including several activities, such as access control, anonymization of the data and the tools for assessing the security of the stakeholder’s device.

SIA: module enables connectivity among different infrastructures (IoT, edge, cloud) and the FISHY Platform, controlling connectivity and providing telemetry of the network, in order to adapt it to other modules.

During the first revision of the architecture in IT-1, some initial changes were made from the original proposal, resulting in the following architecture shown in Figure 2.

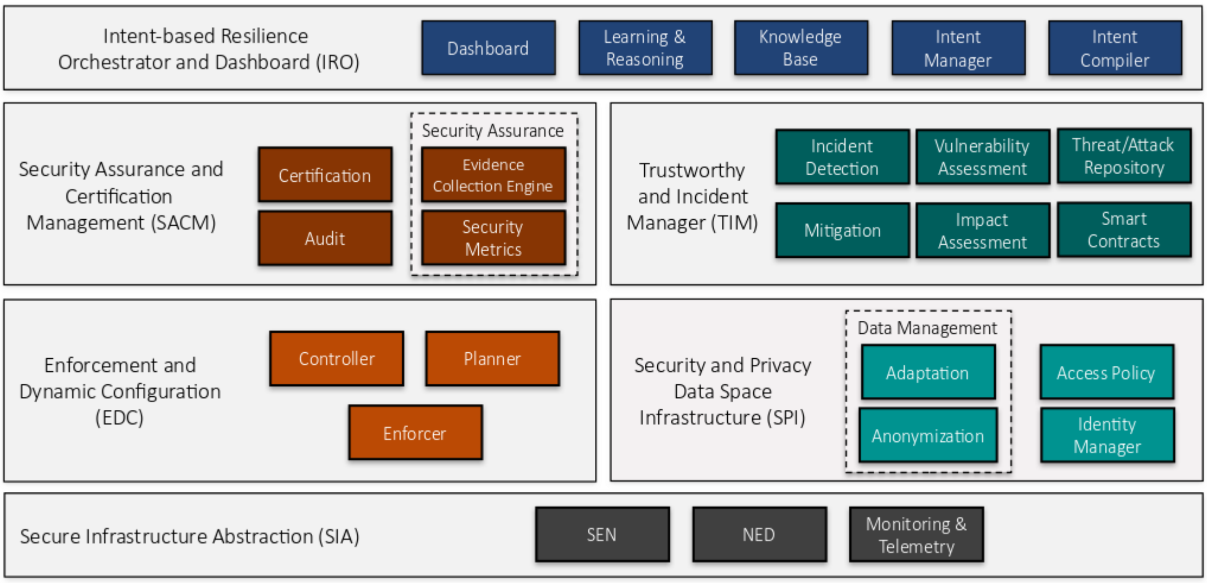

Figure 2: FISHY architecture IT-1 version 1

The first change is related to the “Monitoring & Telemetry“ component, which was originally placed within IRO, and now it is moved to SIA. This change was made due to this component being related to the telemetry data coming from network, connectivity, and infrastructure (cloud, disk, network topology, etc.), which is very related to SIA functionalities. The second change involves the EDC, where the Resilience Manager is removed, and its features were integrated into the EDC’s Controller module.

The activities that took place in WP6 using the IT-1 of the platform gave the opportunity to the use case partners to define in more detail and clarity the requirements and constraints. These, together with the experience from the development phase of IT-1 led to the update of the architecture. The next updated version of the architecture is shown in Figure 3.

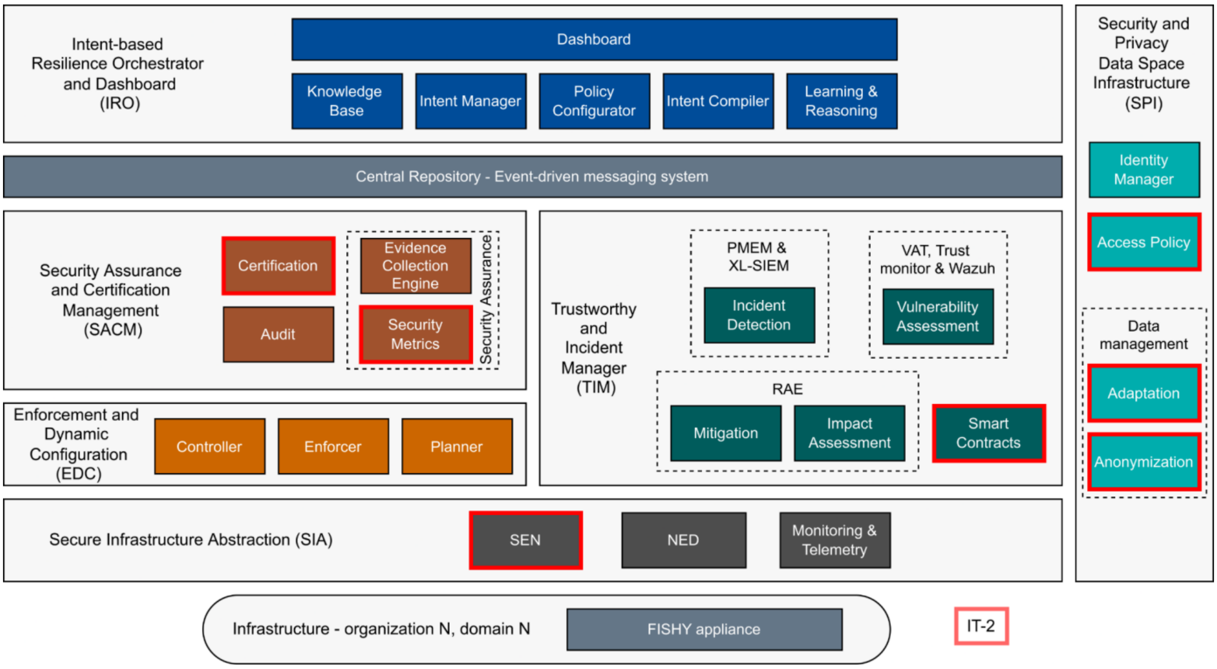
Intent-based Resilience Orchestrator and Dashboard (IRO)
Dashboard
Knowledge Base
Intent Manager
Policy Configurator
Intent Compiler
Learning & Reasoning
Security and Privacy Data Space Infrastructure (SPI)
Identity Manager
Access Policy
Central Repository - Event-driven messaging system
Security Assurance and Certification Management (SACM)
Certification
Audit
Evidence Collection Engine
Security Metrics
Security Assurance
Trustworthy and Incident Manager (TIM)
PMEM & XL-SIEM
Incident Detection
VAT, Trust monitor & Wazuh
Vulnerability Assessment
RAE
Mitigation
Impact Assessment
Smart Contracts
Data management
Adaptation
Anonymization
Enforcement and Dynamic Configuration (EDC)
Controller
Enforcer
Planner
Secure Infrastructure Abstraction (SIA)
SEN
NED
Monitoring & Telemetry
Infrastructure - organization N, domain N
FISHY appliance
IT-2

Figure 3: FISHY architecture IT-1 version 2

The **first change** here involves the Threat/attack Repository which was originally included within TIM, with the purpose to be used only by components within TIM. This component is renamed to Central Repository, which now also includes an event-driven messaging system. Being now outside TIM, the Central Repository, is not only used as a storage system, but also for publish-subscribe communication between all the components in the architecture. The **second change** involves the SPI which becomes transversal to all components in the architecture, in order to better represent that this component is not domain specific, but it has implications on the authentication and identification mechanisms for all the components. The **third modification** is related to the Dashboard which is now represented horizontally to show that now not only relates to IRO, but also includes integration with the rest of the FISHY tools/components. The **fourth change** is related to TIM, where its previously defined functionalities are now mapped to specific tools/components that have been incorporated in FISHY during the development phase. The **last modification** is the addition of the FISHY Appliance, which includes a series of new tools required for the proper data collection from the infrastructure.

It is worth stressing that in this revised version of the architecture designed in the final year of the project, FISHY consortium realized that it would be beneficial of its exploitation and sustainability plans to adopt an architecture that would allow for easy integration of additional components (which we name “tools”) detecting additional attacks or performing additional functionalities in the future.

2.2 Limitations of IT-1 implementation and architectural design

Certain components were not fully implemented during IT-1, so that their final implementations and modifications were left for the second iteration of the FISHY project. These components are: Certification and Security metrics, within SACM; Smart contracts, from TIM; Access policy, Adaptation and Anonymization, from SPI; and Secured Edge Node (SEN) from SIA.

The following changes were required in order to finalize IT-2 architectural design:

From the latest changes made during IT-1, FISHY Appliance was located below SIA in order to facilitate the collection of data from the infrastructure. While this solution worked, it would dismiss the role of SIA to provide network and secure infrastructure abstraction along the whole ICT supply chain. For this reason, this is then solved in IT-2 design (as shown in Figure 4 bellow), by adding specific data collectors on the infrastructure and placing the FISHY Appliance to run over the SIA provider (owner of the infrastructure).

The main reason of changing the Threat attack repository located only in TIM and also the modification of the name into Central Repository, is due to the need of different components for a database (including IRO, TIM and EDC component). Instead of having different databases distributed in each one of the components, we agreed on having only a centralized database located in the FISHY Central Services. Moreover, this centralized database allows the communication between the different components in FISHY by means of a mechanism of PUB/SUB. For instance, when a tool in TIM writes in the Central Repository, IRO can be subscribed to this event, and it is notified about this new info.

In IT-1, SPI was conceptually designed as a unique module for the FISHY Platform. In IT-2, this solution was revealed as non-optimal since the related components perform activities in different levels of the platform and for different purposes. SPI is composed of three components: the Identity Manager, the Access Policy and the Data Management. By their functions and relations, they can be segregated into two main blocks. This segregation took place while other components, which required SPI's services, were being developed throughout IT-1 implementation phase. This in turn has affected FISHY Platform architecture. The Identity Manager and Access Policy components were set to be a high-level block because their operation focused on authentication and authorization capabilities are independent and federative to every other module in the platform, especially those requiring user interaction. On a different side of the platform, SPI Data Manager component aims at data uniformization and privacy enforcement. It was decided that all data collected and stored in the Central Repository should be in Common Event Format (CEF) (reference D4.4 [41] or D3.4 [13]). So, the Data Manager should convert raw data collected by the agents into CEF, as well as security events generated by any TIM tools, along with anonymization modifications before any of that data is stored in the Central Repository. This functionality must be placed at a point of convergence at the entrance to the Central Repository.

The FISHY Dashboard in the initial architecture of IT-1 was located only in IRO. In this sense it could have only shown information coming from the IRO. However, different tools in TIM and EDC also have graphical interfaces which can provide extra information about events, alerts, etc. It was decided to centralize all the GUIs of the different tools as well as the IRO GUI in a single FISHY dashboard.

In IT-2, the Smart Contracts component has been specified, developed and deployed. This was not possible in the first version of the FISHY platform, as a) this component needs to register in the blockchain the detected attacks and each involved component in the IT-1 used a different approach in describing the attacks, which has now been solved since we adopted a common way of describing any attack in the Central Repository and b) this component stores the policies defined by FISHY which had not reached a mature and unified representation approach.

2.3 Reference architecture in IT-2

In order to overcome the limitations of the previous architectures, the last iteration of the architecture in IT-2 also includes a series of updates. Figure 4 shows the final version of the architecture.

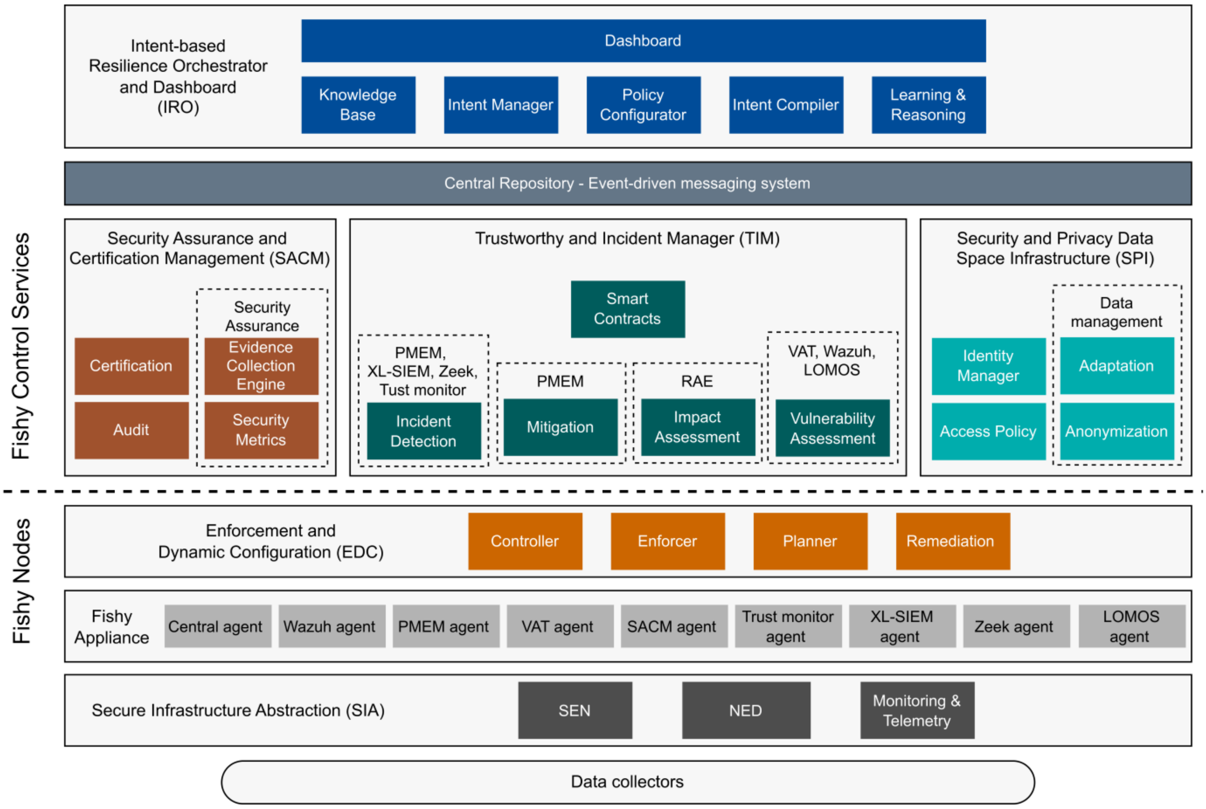

Figure 4: FISHY final architecture (IT-2)

The **first change** involves the FISHY Appliance which is now logically located over SIA, while SIA ensures connectivity between all FISHY domains in the ICT supply chain. The FISHY Appliance now includes all the required agents for each one of the tools monitoring the infrastructure which are: Wazuh Agent, PMEM agent, VAT agent, SACM agent, Trust monitor agent, XL-SIEM agent, Zeek agent and LOMOS agent. The FISHY Appliance also includes a Central agent which aggregates the data fed from each one of the tools. The **second change** considers the inclusion of data collectors which are running directly on the infrastructure administered by the ICT-based supply chain owners. The agents on the FISHY appliance are responsible for establishing communication with these data collectors through SIA. The **third change** is that EDC now includes a new sub-component called “Remediation” module in the EDC, used to suggest remediations for mitigating potential threats. Finally, the **last change** involves the SPI which now is centralized within the FISHY Control Services. In this way, only EDC, FISHY appliance and SIA remain as part of the FISHY nodes. The details about the functionality of each one of these components are described later in Section 3. In Figure 4, there is a distinction between FISHY Control Services and FISHY Nodes. The definition of FISHY Control Services (logically centralized components running outside any organization) has been described in D2.2 [1]. However, now we also include concept of FISHY Nodes, where we assume components deployed per domain basis.

2.4 Platform structure and action areas

As defined in the first architecture deliverable D2.2 [1], the “action areas of concern” are the different types of entities that FISHY considers, which are: **organizations, realms and domains**. Organizations can be either companies, consortiums or law enforcement entities that cooperate with the FISHY Platform. Every organization can be divided into different realms according to the cybersecurity constraints, policies or rules. Within every realm one or more domains can be established between groups of assets with certain relationships, for instance, the same network, location or infrastructure.

In IT-2, we included the mapping between our action areas of concern and the supply chains. In this way, we define two different approaches, a simple one and an advanced one. The simple approach, which was initially included in IT-1, is now updated and shown in Figure 5.

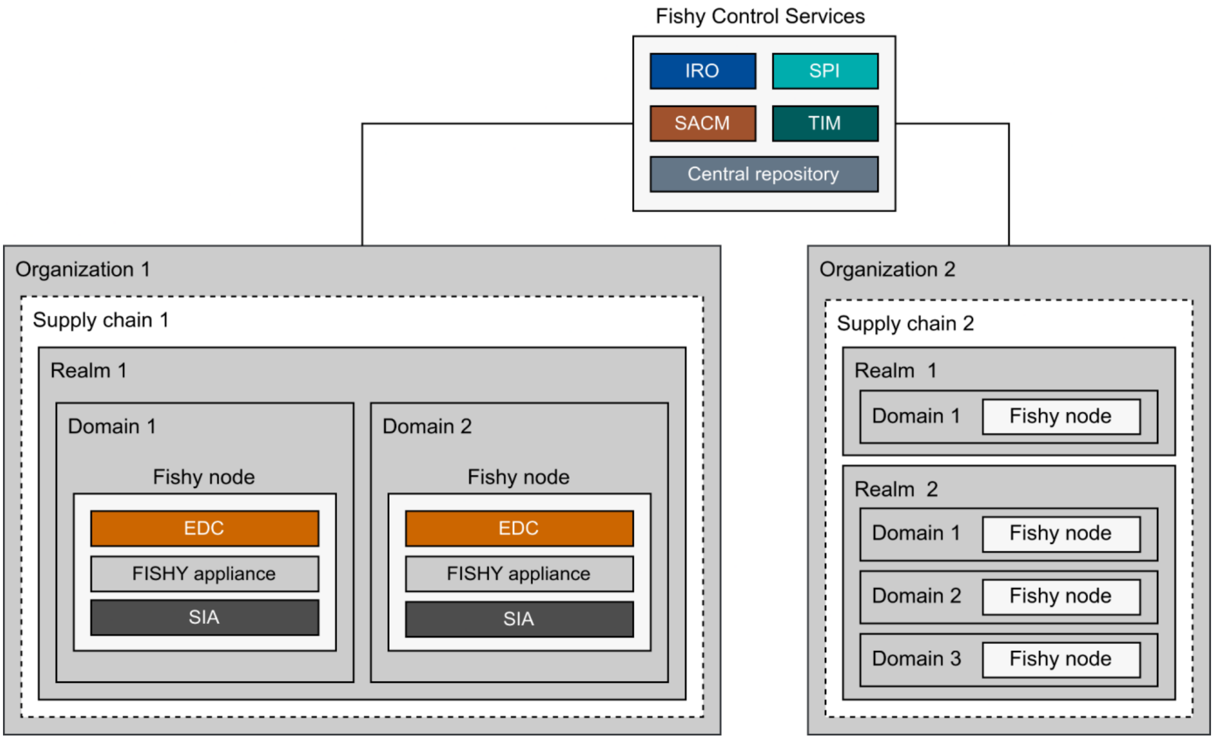

Figure 5: FISHY Platform structure: high-level approach

Compared to the previous version, now the FISHY Control Services also include the SPI and the Central Repository. The components running within each domain are now grouped into what we define as FISHY nodes. Compared to the IT-1 version, the FISHY nodes now include the FISHY appliance as well. The FISHY nodes are deployed per domain basis, so even within the same organization, those components are independently deployed over different domains regardless to which realm they belong to. The FISHY Control Services, on the other hand, are logically centralized components running outside of any organization involved in the supply chain. In this updated version, we can also see the mapping to the supply chains, where each organization manages its own isolated supply chain, with one or multiple realms included. The advanced approach is shown in Figure 6.

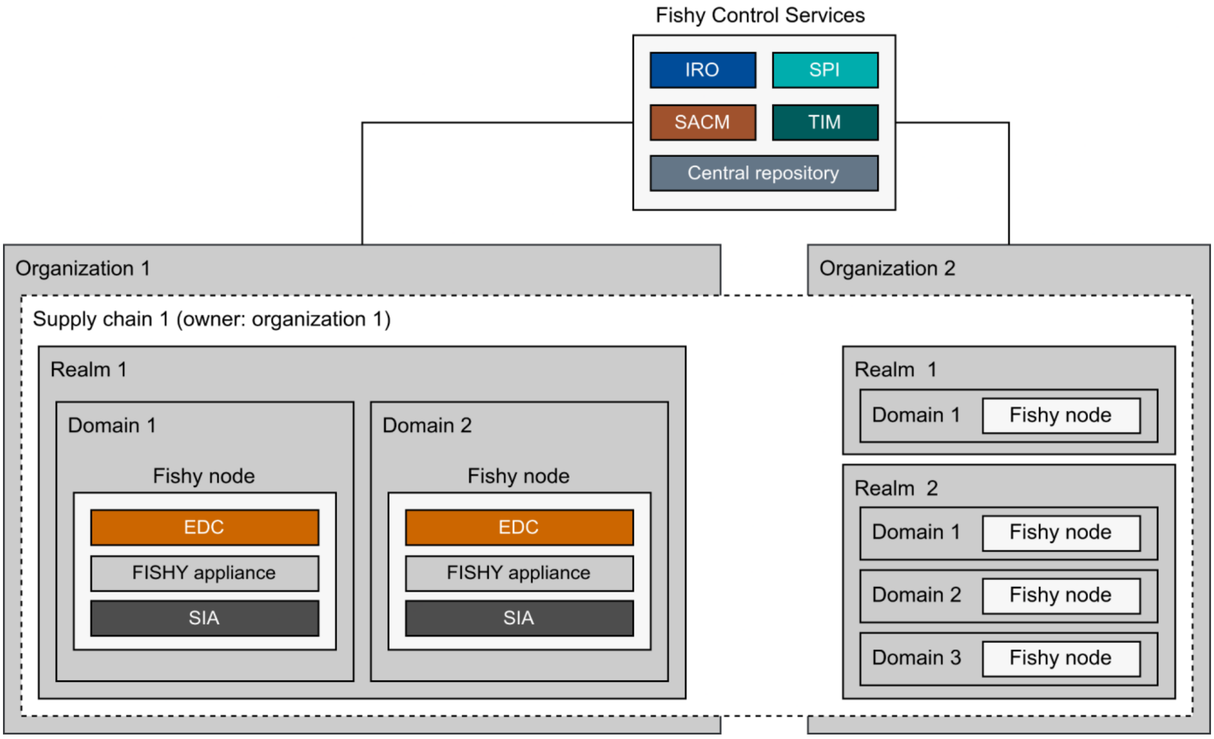

Figure 6: FISHY Platform structure: advanced approach

This advanced approach considers that a supply chain is composed of two or more organizations. In this case, more advanced user and organization roles are required. Depending on the ownership of the structure of the supply chain, there may be domains and realms that are deployed in the premises of a third party, such as a subcontractor, where the supply chain owner does not have permissions to a detailed view of the infrastructure or to make monitoring and policy decisions. However, the supply chain owner would still have access to a high-level view of the status of this part of the supply chain and be notified of potential risks and issues, thus ensuring the security of the whole supply chain.

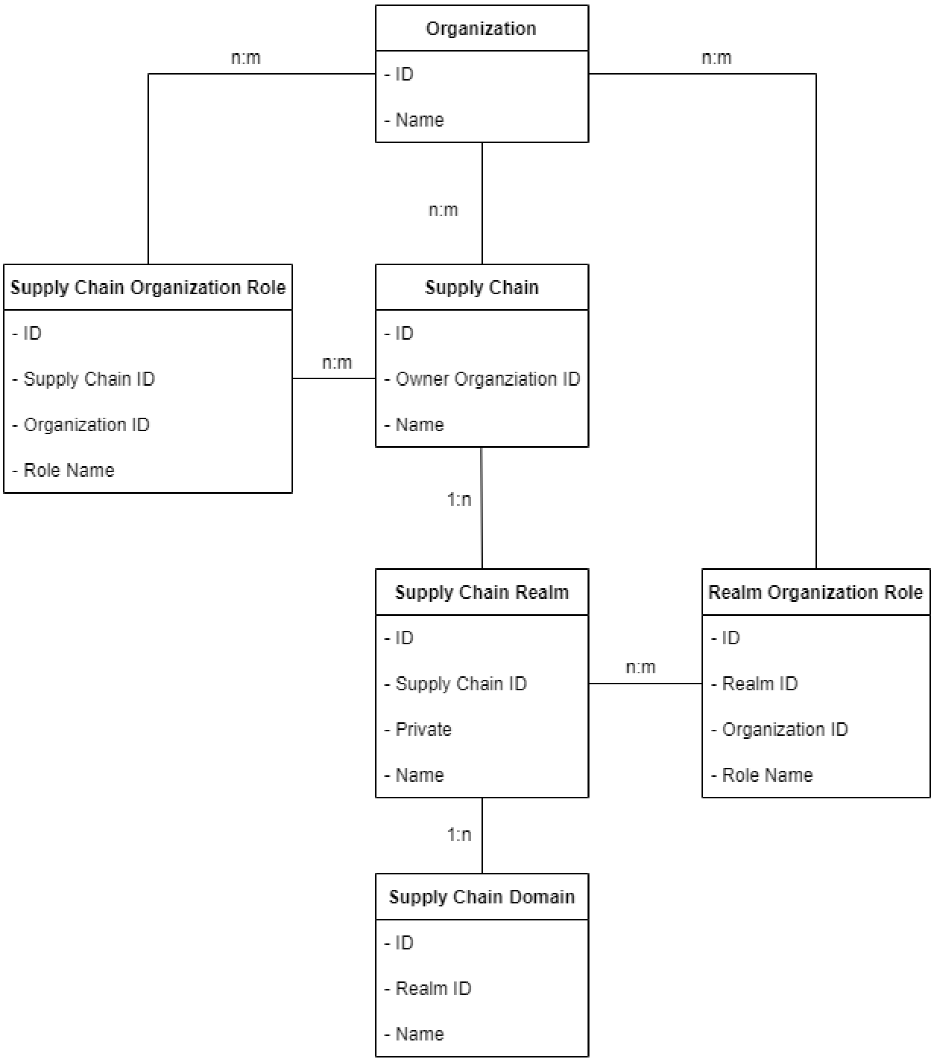

Figure 7: High-level design of user roles that support a multi-organization supply chain

Figure 7 presents the design of user roles that allow the management of a supply chain when two or more organizations are participants. Organizations can be assigned roles on the whole supply chain level, such as owner or participant, and also on the level of a realm of the supply chain, giving realm owners full control of the domains within their control and/or ownership.

3 Architectural Design

In this section, we will provide an overview of the FISHY main modules, shown in the reference architectural design for IT-2, shown in Figure 4. As previously stated, taking into consideration experiences from the practical implementation and integration with use cases in IT-1, some of the components and functionalities have been modified for IT-2.

3.1 Main architectural building blocks

3.1.1 Trust & Incident Management

The modules comprising the Trust & Incident Manager during the IT-1 phase of the project, as described in D2.2 [1] are Vulnerability Assessment, Incident Detection, Impact Assessment, Mitigation, Threat/Attack Repository and Smart Contracts. During the developments in IT-2, further granularity and mapping of functionalities to modules and tools was performed, such as Impact Assessment being renamed to "Prediction and estimation of risks" and adding "Remote Attestation". Additionally, the Threat/Attack Repository was renamed to Central Repository and now serves a wider role of data storage and inter-component communication in the scope of the entire platform, instead of being confined to TIM and also being moved into its own functionality block (see subsection 3.1.6 Central Repository).

The mapping of modules, functionalities and tools is described in D3.4 [13]:

Functionality	Modules	Tools
Vulnerability Assessment	Vulnerability Assessment	Wazuh, VAT, LOMOS
Incident Detection	Incident Detection	XL-SIEM, PMEM, Zeek, Wazuh
Mitigation	Mitigation	PMEM
Prediction and estimation of risks	Prediction and estimation of risks	RAE
Remote Attestation	Trust Monitor	TPM 2.0
Trustworthy mechanisms and collaboration among stakeholders	Smart Contracts	Smart Contracts
Extension/ Expansion scalability	Smart Contracts	Smart Contracts
Global security events storage	Central Repository	Relational Database, Pub/Sub (RabbitMQ)

The subcomponents of TIM tools, which are data collectors, agents and data processors, are located on the monitored infrastructure, the agents are located in the FISHY Appliance and the data processors are located in the FISHY Control Services.

The interaction and data flow between TIM components and other architectural blocks of FISHY Platform is defined as follows:

Networking between the data collectors and the agents in the Appliance is facilitated by the Secure Infrastructure Abstraction (SIA).

The data from the agents in the Appliance to data processors in the FISHY Control Services go through Security and Privacy Data Space Infrastructure (SPI),

Relevant outcomes of monitoring from the data processors are stored in the Central Repository,

IRO (dashboard) is notified about newly available data in the Central Repository via the pub/sub system.

In addition, the role of Smart Contracts in IT-2 is now solidified as the provider of immutability of data and sequence of events. It persists security related events detected by other TIM modules on the blockchain, thus ensuring that the information and the sequence of events cannot be tampered with.

3.1.2 Security & Privacy Data Space Infrastructure

As described in the deliverable D2.2 [1], concerning the architectural requirements for the first iteration of the FISHY Project, the Security & Privacy Data Space Infrastructure (SPI) component is mainly composed of three modules: Identity Management, Access Policy and Data Management. In the second iteration of the FISHY Project, the SPI component undertook tasks that require constant and transversal communication with the other components of the framework. The SPI was designed with the purpose to establish a secure mechanism for communications between low-level components and higher-level modules. As such, it addresses the principles of security and privacy by default and by design. It also performs a key-role in the management of identity and access control for all the platform's components, assuring that the platform is used by only those to whom access has been granted and only perform actions accordingly with their previously defined profile. The SPI Data Management module is related to the need for normalization of the data collected by the agents placed in use cases' infrastructure (see deliverable D3.4 [13] for more details). The normalization aims to provide a common format to store all the events from different agents into the Central Repository. This module is also responsible for enforcing privacy according to rules defined by each data owner. Finally, the Access Policy component is responsible for all management functions to create, verify, and maintain the access control and privacy policies. The SPI modules are located in the FISHY Control Services.

Identity Manager

The Identity Manager module is specially related with user and roles management activities and access control functions which includes authentication, authorization and auditing features. In the second iteration, the identity manager module has many of the features related with access management, and performs activities related with the control of the access to all components technologies of the FISHY Platform. The access control was implemented by OpenID Connect (OIDC) and OAuth2.0 technologies as provided by Keycloak - a well-known and robust open-source implementation (see deliverable D3.4 [13] for more details). This solution was developed to have a centralized authorization server implementing the OAuth2 standard, complemented by an authentication layer based on the OpenID Standard. The centralized authentication system provides services both for users and server-clients relations. Users are authenticated locally or using a federated model (using state-of-the-art mechanisms) while software components use a unique ID and shared key to access the platform, implementing several flows that support all possible software-software relations. The adopted solution specifies a mechanism to use Access Tokens and allows the access to services and enforces authentication on the flow of information across the whole FISHY Platform.

Notwithstanding the central nature of this component, the user and software authentication within the FISHY architecture poses different requirements. While user authentication assumes a global role, to allow access control for users belonging to different domains, or realms, software authentication assumes a local role since there will be no inter-domain access at the software-level. At the current state of the design there will be one Identity Manager in each domain (use case), fulfilling the overall user and software authentication functions. However, if it becomes necessary/desirable to deploy the Identity Manager in a more centralized way for user authentication, the federated capacities of Keycloak will provide a smooth adaptation, interlinking several Keycloak implementations.

Access Policy

The Access Policy module is responsible to manage and apply security and privacy policies defined by the organization. Its main role is the design, verification and maintenance of policies, which are expressed in XACML (Extensible Access Control Markup Language). Using a proper user interface, an administrator defines and develops all the access control and privacy policies and their specific variables such as subjects, objects, credentials, roles, realms, operations and logging conditions. An API and a synchronization mechanism establishes a secure link between the core policy engine and both the Identity Manager and Data Management modules. The overall process is intended to be deployed as a fully automatic mechanism. Supporting these main concepts, it is even possible to develop an interface to import/export policies previously defined in XACML format to be interpreted by the platform. This capacity increases the flexibility of the Access Policy module which will be open to interface with other components, both at the infrastructure and system levels (like a central policy manager eventually available already in an organization).

Data Management

The Data Management module is responsible for the normalization of data and categorization according to system requirements. This module is composed of two main functionalities, such as adaptation and anonymization. The adaptation process is entirely linked with the concept of data normalization (see deliverable D3.4 [13] for more details), in which agents placed into the premises of the organization under study collect data that should be stored in the Central Repository in a unified and standard format, such as the CEF format. The constant production of data retrieved from the different tools that compose the FISHY Project retrieve outputs in different formats and standards. Due to this issue, it is essential to manage and adapt the data collected and transform into CEF. This data format works with a key/value arrangement and their manipulation makes it easily compatible to incorporate JSON/JWT and implementations over Syslog.

The anonymization process is related with the privacy enforcement feature of the FISHY Project. The anonymization concept is associated with a conversion of processed data to preserve the privacy of users and comply with regulatory requirements. This feature is essential to FISHY, since the environment of application is supply-chains and traditionally this kind of organizational environment traditionally is characterized by a high transference of data between different stakeholders.

3.1.3 Security Assurance and Certification Management

The Security Assurance Platform (developed by STS) is a framework composed of models, procedures, and tools that work together to enable the certification of security attributes in services (for its latest detailed overview see deliverable D4.4 [41]). By extending the current Security Assurance solutions, the Security Assurance and Certification Management (SACM) tool will monitor on important processes and parts of the ICT infrastructure with the help of an Evidence Collection Engine created specifically for the task. Based on that input, the tool will present an evidence-based, certifiable view of the security posture of the ICT system, with accountability provisions for changes that occur in that posture and the analysis of their cascading effects, supporting the runtime checking based on sets of associated claims and metrics.

The Security Assurance Platform is made up of three fundamental software modules (located in the FISHY Control Services):

Asset Loader Module

This part is in charge of bringing in the target organization's asset model for the cyber system. This model is based on STS's Assurance Model and covers the assets of the organization, security properties for those assets, threats that may violate those properties, and security procedures that safeguard those assets. The target organization defines the latter data using an excel file supplied by STS. The Asset Loader Module parses this Excel file and automatically creates the appropriate model for the target organization.

The Monitoring - Auditing Module

The Monitoring - Auditing Module is a Java-based runtime monitoring engine that provides an API for defining the monitoring rules that will be audited. The monitoring database and the monitor are the two submodules that make up this module. The module's function is to transmit the runtime events from the properties that the application monitors before obtaining the monitoring results. The latter are kept in the monitor submodule's database together with the monitor database. The auditing module's central submodule, (called Monitor), determines if a monitoring rule is broken or satisfied.

Evidence gathering - Event Captor Module

The Event Captor is a tool that creates a rule or group of rules based on gathered data and triggering events, then sends those rules to the monitoring module for examination. Using lightweight shippers (called Beats), such as Filebeat, MetricBeat, and PacketBeat [47], which centralize log data, Elasticsearch is primarily used to collect data and events. Logstash, an open server-side data processing pipeline that ingests data from a variety of sources, alters it, and then transmits it to Elasticsearch, is another method for gathering data. Through the relevant REST requests from the monitoring module, the Event Captor is started.

The FISHY Platform's security posture will be continuously and in real-time assessed using the Evidence Collection Engine or Event Captor Module, which will also aggregate cross-layer evidence relevant to the security posture of each monitored component in real-time. This module will make use of event captors' incoming data. These are a group of software elements that create a rule or group of rules based on gathered data and triggering events and send them to the Monitoring Module for assessment. The event captor module is embedded into the systems that need to be evaluated as a straightforward dockerized agent/container. The agents' job is to compile evidence from multiple sources (such as network traffic, security logs, system logs, etc.) and package it in an event format that the monitor can understand. The event collector then forwards the events to the monitor.

3.1.4 Enforcement and Dynamic Configuration

The EDC (Enforcement & Dynamic Configuration) is the FISHY component in charge of defining the configurations for the security controls in a FISHY-controlled network (for its latest detailed overview see deliverable D4.4 [41]). The job of the EDC is to configure the security controls and the landscape in general to enforce some security-related requirements. This is achieved through the following two tasks:

- refining the high-level policies into low-level configurations and then sending them to the SIA for their final deployment.
- suggesting remediation actions to mitigate the effects of a network threat or attack.

Policy refinement

The policy refinement mechanism of the EDC is triggered when a new high-level policy is stored in the Central Repository (either written by IRO, pushed by another tool, or manually by an administrator). The refinement process involves the following three sub-components as detailed in deliverables D4.2 [7] and D4.3 [4].

The Controller is in charge of refining high-level policies into medium-level policies. It leverages the power of the CLIPS forward-chaining reasoning systems [42] to correctly adapt its decisions to the landscape, available security controls, and their features.

The Enforcer instead refines the medium-level policies into low-level configurations. Most of the translation abilities of this module stem from the power of the Security Capability Model (described in deliverable D4.3 [4]. In addition to generating the final configurations, this module is also in charge of sending them to the SIA component for their final deployment in a FISHY-safeguarded network.

Finally, the Register & Planner can be considered a structured catalogue containing all the available NSFs and their features according to their Security Capability Model (see deliverable D4.3 [4]). It is used by the Controller and Enforcer modules to perform their jobs to customize their outputs to the desired scenarios.

Network level threat mitigation

The threat mitigation suggestion ability of the EDC allows it to suggest to the administrators some actions to execute to mitigate the consequences of an attack. These proposed actions, or remediations, can span from simple alert messages to high-level policies for reconfiguring an existing node or landscape reconfigurations (e.g., adding or moving a security control).

The recommendation system is implemented by an ad-hoc element in the EDC: the Remediation Module (see deliverable D4.3 [4]). This component reacts when a threat intelligence report is pushed into the Central Repository. The Remediation Module downloads this report, analyzes its content, and, according to a set of internal (and customizable) recipes, suggests a remediation to mitigate the effects of the attack.

3.1.5 Intent-based Resilience Orchestrator and Dashboard

The architecture of the Intent-based Resilience Orchestrator and Dashboard, as detailed in the deliverables D2.2 [1] and D5.1 [10], consists of the following sub-modules: Intent Manager, Policy Configurator, Learning & Reasoning, Knowledge base and Dashboard. The Intent Compiler was removed in this update and its functionality was merged with the Policy Configurator.

In the second iteration, the IRO component is integrated with the Central Repository which has become an independent component from TIM, and remains one of the FISHY Control Services components. IRO is responsible for mapping high-level policies into configured policies that are compatible with the Enforcer component (the EDC), based on the intents received from the user. The communication between IRO and the EDC is now established through the Central Repository, where a policy dedicated end-point is implemented. Furthermore, IRO is integrated with the Smart Contracts component through the Central Repository in order to verify the integrity of collected events and mapped configurations. This collected information will be exposed to the user via the IRO Dashboard.

The functionalities of IRO can be summarized into two main features:

User notifications: this feature has been evolved in the second iteration. A new interface has been developed and deployed to show the collected information from different TIM tools to the user.

Intent configuration: by configuring intents the user can set rules for event detection and alerts, and policy configuration. This will give the user the capability to make decisions and take actions, when needed, through an easy-to-use interface and a high-level intent definition. From an architectural point of view, Intent Manager, Policy Configurator, and the Dashboard will be used to enable the intent configuration.

3.1.6 Central Repository

In the initial architecture of the project, the Central Repository was named "Threat/Attack Repository" and was a TIM component. During discussions encompassing both the architectural design and plans of implementation and integration, it became apparent that most FISHY components need a) a form of storage and b) a method of instant notifications of data available for analysis and/or processing. The Threat/Attack Repository design described in D3.1 [11] was a good fit for this purpose and so its role was expanded from a strictly TIM component to a transversal component that facilitates communication between the various parts of the FISHY Platform in the upper architectural domain, the FISHY Control Services.

In line with its original role, the Central Repository stores the outcomes of TIM tools and its functionality has been expanded to also allow storage and propagation of other forms of data, such as high and medium level policies and configurations. Notifications of newly available data are propagated via a pub/sub system, where other components can subscribe to events related to certain data types and be notified immediately when new data is stored in the Central Repository.

3.1.7 FISHY Appliance

FISHY Appliance is a runtime framework for FISHY cybersecurity tool agents. It is positioned between the monitored infrastructure and the FISHY Platform (see the Figure 4 of the FISHY architecture) and as such, it is a point of integration between data collectors and tool agents in the domain level and server components in the FISHY Control Services.

The Appliance relies on SIA for secure networking (no direct integration) to the monitored infrastructure and the SPI for secure transmission of monitored data to the platform. Appliance agent assists tools agents in the integration (when necessary), offering REST API collection endpoint where tool agents deposit data which is then forwarded to the FISHY Platform via SPI (using RabbitMQ). Multiple instances of the Appliance can be deployed over the nodes in a supply chain.

3.1.8 Secure Infrastructure Abstraction

This section presents a short overview on the SIA, which is a module that is implemented at the lower layer of the FISHY architecture. As described in deliverable D2.2 [1], the SIA provides the following functionalities:

It provides a data-plane interface to support external and inter-domain communications within the FISHY Platform (e.g., between an IoT/edge infrastructure and a cloud infrastructure, or between multiple cloud infrastructures). In addition, it controls the network access to the FISHY domains, protecting data traffic entering and leaving the domains. This functionality is mainly provided by a Network Edge Device (NED) function.

Secondly, it provides the proper means to interact with the NFV infrastructure resources that are available at every domain, regardless of the particular virtual infrastructure management technologies that are used (e.g., OpenStack or Kubernetes). This functionality is provided by a Northbound Interface (NBI) and an Orchestration Function (OF). The OF is deployed at every domain, whereas the SIA NBI can be used by other components of the FISHY Platform, like the EDC.

Conceptually, the NBI can support different functionalities across FISHY domains, including but not being limited to: the deployment of network services on the domains, where a network service is defined as a composition of virtual network functions (VNFs) that can be deployed at different locations, e.g., to provide security-related functionalities; and the management of NFV descriptors (i.e., upload/delete/update the data that describes the network services and VNFs that are to be deployed). A more concrete list of the NBI functionalities is provided in deliverable D2.2 [1].

We would like to highlight that, to keep compatibility with relevant NFV standards, the decision taken in WP5 has been that the SIA NBI will be aligned with the API specification defined by ETSI for their NFV orchestrator, which is included in ETSI NFV-SOL 005 [18]. Moreover, NFV descriptors will follow the YANG models defined in ETSI NFV-SOL 006 [19].

As a final consideration, as previously commented, it is important to observe that the SIA must provide its functionalities regardless of any virtual management infrastructures solutions that are used at a domain. To this purpose, the SIA design includes an adaptable southbound interface (SBI), that precisely supports the interaction with the management and orchestration software stacks that exist in a domain.

3.2 Communication aspect

In this subsection we first describe the high-level communication between all the components in the architecture and then we follow up with detailing the communication at each individual component level.

The main objective of the communication diagram is to represent the high-level operational communication workflow between all components in the FISHY architecture. To this end, the communication diagram is intended to be used when defining workflows at a lower level and also when defining specific workflows for each one of the use cases.

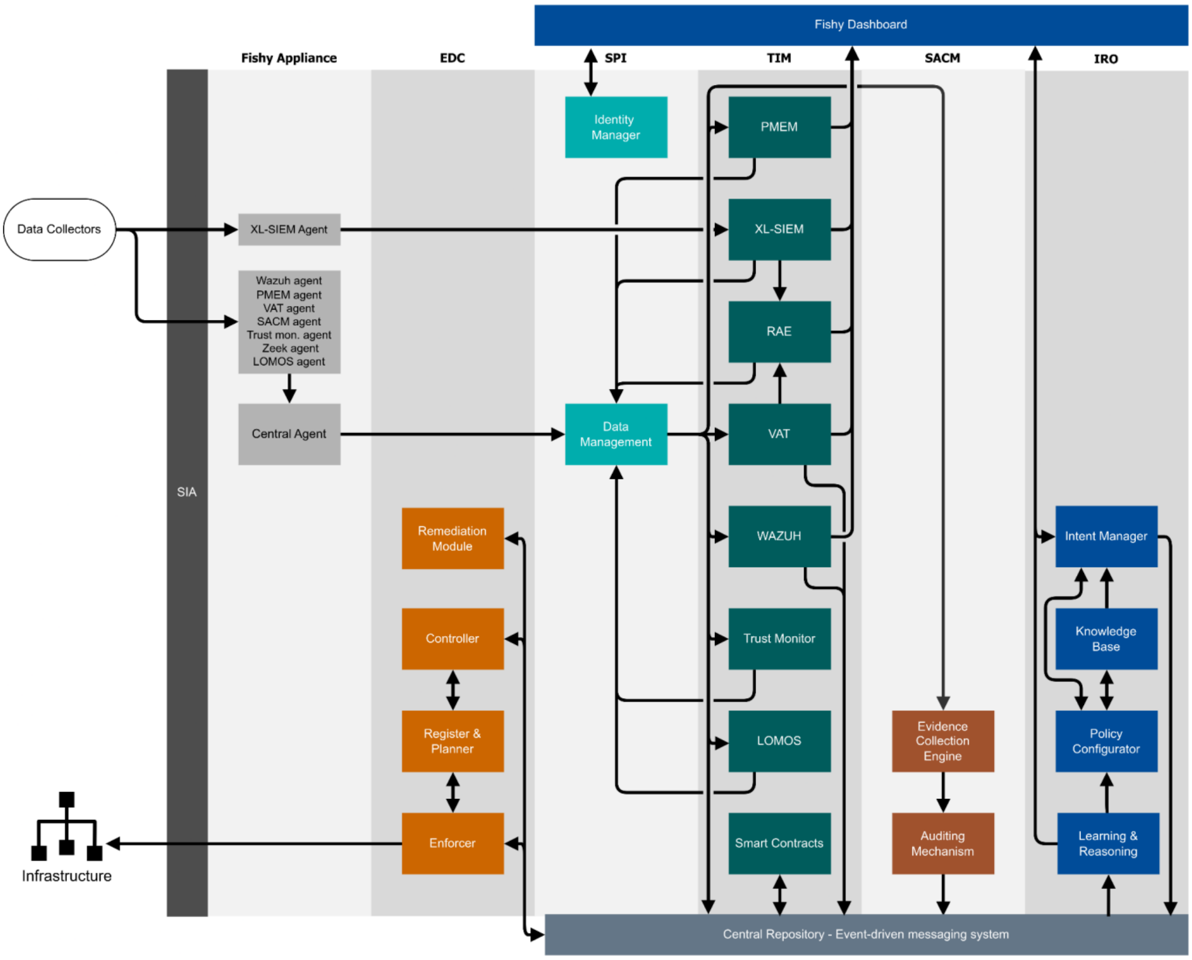

Figure 8: FISHY Platform high-level communication diagram

The communication diagram of Figure 8 contains 6 modules (FISHY Appliance, EDC, SPI, TIM, SACM, IRO) plus the FISHY Dashboard, Central Repository and Data Collectors.

Data collectors forward the data from the different scenarios to the agents in the FISHY Appliance. The data format at this stage is native/raw to each tool. The data is then forwarded to the Central Agent (except for XL-SIEM) and sent to the Data Management at SPI, which then sends the data to each relevant tool at TIM. Data Management receives events in native format from some tools (PMEM, XL-SIEM, RAE), transforms them into CEF format, then sends them to the Central Repository. Other tools (VAT, Wazuh, Smart Contracts) implement the mapping from their native formats to CEF on their own, and send the data directly to the Central Repository. Data collected by the Data Management is also sent to SACM, to the Evidence Collection Engine, then to the Auditing Mechanism, and the results are stored in the Central Repository.

IRO reads the information from the Central Repository which is processed and shown in FISHY Dashboard. The user enters intents which are then processed by the Intent Manager and Policy Configurator, and the result is stored into the Central Repository. IRO can as well receive reports from different tools, which are stored in Central Repository, using RabbitMQ messaging system, and automatically generating the corresponding policies based on previously defined user requirements.

The EDC receives the policies created by IRO from the Central Repository for Remediation, Controller and Enforcer components. After processing, the produced output is applied into the infrastructure through SIA.

The FISHY Dashboard integrates in a single browser window, multiple tabs comprising the graphical interfaces of five (PMEM, XL-SIEM, RAE, VAT and Wazuh) TIM tools, two from IRO (Learning and Reasoning and Intent Manager) and one from SPI (Identity Manager).

4 Cyber resilience related constraints and requirements

In D2.2 [1], the first list of concrete requirements and constraints that the FISHY Platform should meet/respect was defined, based on which the first version of FISHY architecture was designed. In this deliverable, this list is revised mainly in the direction of making them more concrete since the pilot partners are now more informed about what the FISHY Platform can offer them, and thus, they can provide more concrete requirements. The piloting process helped all piloting partners understand better the scope and boundaries of the FISHY Platform. In the following sections, we list the revised user requirements and constraints and also describe the deployment of FISHY in each use case.

4.1 Functional requirements (IT-2)

The revised list of functional requirements and of the functional and non-functional constraints follow. The tables include the Requirement Identifier, its name, the description, the priority level following the MoSCoW approach (Must, Should, Could, Will not) and the main component of the FISHY architecture that is responsible for the satisfaction of the requirement.

To produce these lists, first (Step 1) each pilot partner defined a set of requirements and constraints and then, (Step 2), the list was checked for similar or duplicate requirements. We consider a requirement to be "duplicate" when the same requirement has been identified by more than one use case. The duplicate requirements have been removed and the one that was kept appears with a requirement ID followed by a parenthesis where ID of the similar requirement that was removed is mentioned, e.g. REQ-WBP-05 (Similar to REQ_F2F_01).

Table 1: List of functional requirements

REQ ID	Name	Description	Priority	Component
REQ-F2F-01	Multi-device and multi-system protection	The FISHY Platform must monitor the connectivity and security of multiple IT systems comprising of tens of sensors	MUST	SIA, Dashboard, SACM, TIM
REQ-F2F-02	Access to authentication and authorization events	The FISHY Platform must be informed about unsuccessful authentication and authorization attempts made to the platforms it protects (e.g. the F2F platform) and must be able to detect such types of attacks	MUST	SIA, TIM, SACM, SPI

REQ-F2F-03	Unauthorized device attempt detection	The FISHY Platform must be able to detect the event where a device from an unauthorized platform attempts to enter information in the F2F solution and prevent it from harming the F2F platform	MUST	TIM, IRO, EDC Dashboard
REQ-F2F-04	Network performance monitoring	The FISHY Platform should ensure efficient monitoring mechanisms to timely identify network level attacks	SHOULD	TIM, SIA
REQ-F2F-05	Surveillance of all nodes registering information	The FISHY Platform must survey all entities registering information in the databases (such as the consortium ledger)	MUST	TIM, IRO, EDC Dashboard
REQ-F2F-06	Multiple authentication attacks detection	The FISHY Platform must be able to detect potential threats from external entities with respect to user authentication, wallet ID authentication, and DID level authentication of entities	MUST	TIM, SACM
REQ-F2F-07	Security auditing	The FISHY Platform must be able to audit and certify the level of security provided by the platform e.g., by providing the number and types of attacks for specific time spans	MUST	SACM
REQ-F2F-08	FISHY user authentication	The FISHY Platform must support strong user authentication and authorization mechanisms.	MUST	SPI
REQ-F2F-09	FISHY user capabilities - 1	The FISHY Platform could support the FISHY user in defining sub-systems of the platform they operate.	COULD	Dashboard, IRO

REQ-F2F-10	FISHY user capabilities- 2	The FISHY Platform must support each user to configure the details of the system to be monitored/ assessed and analyzed also including security metrics by the FISHY platform.	MUST	SACM , IRO, EDC, TIM
REQ-F2F-11	FISHY user roles	The FISHY Platform could support role-based access management to support different levels of privileges for the supply chain actors	COULD	SPI
REQ-F2F-12	Policy configuration	The FISHY Platform must define configuration that mitigates the detected attacks (threatening the individual infrastructure - SynField operator, ABERON operator, user application operator)	MUST	IRO, EDC
REQ-F2F-13	Notification/ recommendation provisioning	The FISHY Platform must notify/ alert/ recommend the user about attacks and reconfiguration of the platform he operates and its subsystems.	MUST	IRO/dashboard, SACM, EDC
REQ-F2F-14	Alert provisioning	The FISHY Platform must alert the user when an attack that cannot be automatically handled by the FISHY platform is detected (so that he takes actions)	MUST	TIM, IRO, PMEM
REQ-F2F-15	Network reconfiguration	The FISHY Platform could enforce the network reconfiguration of the infrastructure in case of a threat detection	COULD	EDC

REQ-F2F-16	Security reporting	The FISHY Platform must allow the user to obtain the results of the cyber security monitoring process of the FISHY platform	MUST	TIM, SACM
REQ-F2F-17	Reporting per subsystem	The FISHY Platform could offer the ability to the user to request audit per subsystem or system	COULD	SACM, TIM, IRO
REQ-F2F-18	Certificate provisioning	The FISHY Platform could provide (upon request) the user with certificates of the platform he operates (certificate issuing)	COULD	SACM, TIM
REQ-F2F-19	Certificate provisioning per subsystems	The FISHY Platform could provide (upon request) the user with certificates of the sub-systems of the platform he operates (certificate validation)	COULD	SACM
REQ-F2F-20	Security results presentation	The FISHY Platform offers visualized view of the results of the monitoring process to the FISHY user	MUST	Dashboard
REQ-F2F-21	Dissemination of new attacks information	The FISHY Platform could disseminate the detected threats or attacks to FISHY users when deemed relevant (e.g. similar platforms)	COULD	TIM, IRO Dashboard
REQ-WBP-01	New devices: real-time monitoring	The FISHY Platform must detect and continuously display the information collected in real time	MUST	TIM, IRO
REQ-WBP-02	Authorized devices: IoT telemetry	The FISHY Platform should alert whenever the collected information does not arrive at the destination.	SHOULD	TIM , SACM, IRO

REQ-WBP-03	New devices: access management	The FISHY Platform must ensure that the information is only used/accessed by those authorized.	MUST	SPI
REQ-WBP-04	New devices: detection of new devices	The FISHY Platform must identify and alert the existence of new IoT devices/sensors. Operator ACK: - If an authorized device, add to the database. - If not an authorized device, open the incident.	MUST	TIM
REQ-WBP-05 (Similar to REQ_F2F_01)	New devices: connectivity and security monitoring	The FISHY Platform must monitor the connectivity and security of multiple IoT devices/sensors	MUST	TIM, SPI, SIA
REQ-WBP-06	IoT security incidents: detection	The FISHY Platform must be able to detect security incidents in components of IoT platforms	MUST	TIM, SACM
REQ-WBP-07	EDI security incidents: detection	The FISHY Platform must be able to detect security incidents coming from the sap web dispatcher on EDI communications	MUST	TIM
REQ- WBP-08	Security incidents: impact analysis	The FISHY Platform should analyze the impact that an incident may have on an organization	SHOULD	TIM
REQ- WBP-09 (Similar to REQ_F2F_13)	Security incidents: recommendations for mitigation / resolution	The FISHY Platform must recommend needed actions to "incident teams" on what is necessary to resolve or mitigate an incident effectively	MUST	TIM, IRO, EDC

REQ- WBP-10 (Similar to REQ_F2F_14)	Anomaly detection: assessment	The FISHY Platform must detect and alert anomalies of the network traffic or network infrastructure of the production line	MUST	SACM, TIM
REQ-SADE-01 (Similar to REQ_F2F_12)	Users Sign-up	The FISHY Platform must provide a way to register users.	MUST	SPI
REQ-SADE-03	System access from top and bottom	The FISHY Platform must be able to access information from the user side and vehicle side.	MUST	Dashboard, IRO, SIA
REQ-SADE-04	Vehicle registration	The FISHY Platform must provide a way to register new vehicles.	MUST	Dashboard, SPI
REQ-SADE-05	Add certified IOT software versions	The FISHY Platform must provide a way to manage and register lists of certified software versions and keep it securely saved. Should contain version, manufacturer, and model. Optionally, checksum or link to a safe storage with the update file.	MUST	Dashboard, SPI
REQ-SADE-06	Revoke certified IOT software versions	The FISHY Platform must provide a way for SW administrators to revoke or update specific versions from the certified list (or allow FISHY to do that automatically).	MUST	Dashboard, SPI
REQ-SADE-07	Filtered search	The FISHY Platform must provide a way to filter lists of certified software versions by Sensor, Car, Vendor, Country, etc.	MUST	Dashboard, SPI

REQ-SADE-08	IOT Software Version monitoring	The FISHY Platform must be able to audit and certify that the level of software patches of each IOT device in every vehicle is aligned to security versions provided by manufacturers.	MUST	SACM, SIA
REQ-SADE-11	Vehicle configuration for car owners	The FISHY Platform must support each owner user to configure and see information about his owned vehicles.	MUST	Dashboard, SPI
REQ-SADE-12	Vehicle configuration for privileged users	The FISHY Platform must support each dealer/car manufacturer user to configure their vehicles	MUST	Dashboard, SPI
REQ-SADE-13	Role model for users	The FISHY Platform must support role-based access management to support different levels of privileges for actors	MUST	SPI
REQ-SADE-14	Policies definition	The FISHY Platform must provide a way to define policies and actions to be performed when some conditions are taken.	MUST	IRO, SACM, TIM, EDC
REQ-SADE-15	Notifications about actions	The FISHY Platform notifies/ alerts the users about policies triggered to vehicles or EDGE infrastructure.	MUST	IRO, EDC, SIA, TIM
REQ-SADE-16	Policies enforcement into elements	The FISHY Platform must be able to enforce policies into the isolated devices and to group elements: Sensor, Car, Vendor, Country, etc.	MUST	IRO, EDC, SIA, TIM

REQ-SADE-17	Allow several kind of policies	The FISHY Platform must include policies that will not only block certain traffic, or users from the car itself but eventually will ensure that only selected encryption mechanisms are used, or algorithms are updated.	MUST	IRO, EDC, SIA, TIM

4.2 Non-functional constraints and requirements (IT-2)

The revised list of non-functional requirements is presented in the sequel. No modification with respect to constraints was considered necessary.

Table 2: List of non-functional requirements

REQ ID	Name	Description	Priority	Component
REQ-F2F-10 REQ-WBP-11	Extension/ Expansion scalability	The FISHY Platform should support expandability. For example, if a new IT system is connected to an existing supply chain, the FISHY Platform should be able to handle this as a whole	SHOULD	Dashboard, SACM
REQ-F2F-11 REQ-SADE-02 REQ-WBP-12	Geographic dispersion support	The FISHY Platform must take into consideration geographic dispersion of the supply chain entities	MUST	SIA, IRO, EDC,
REQ-F2F-18 REQ-WBP-13	User friendliness	The FISHY Platform should offer intuitive user-friendly interfaces.	SHOULD	Dashboard
REQ-SADE-18 REQ-WBP-14	Trustworthy mechanisms and collaboration among stakeholders	The FISHY Platform could support trustworthy mechanisms and facilitate collaboration among stakeholders based on trust and evidence comprising the supply	COULD	SACM, TIM

		chain		

4.3 Use cases mapping to FISHY architecture

Use case 1: overview of the FISHY deployment

The first two years of the project and the piloting activities helped us understand better what is needed to protect our Farm-to-Fork (F2F) platform from different attacks. Now, taking into account the revised architecture and the farm-to-fork scenario, we have concluded that there are two main options for utilizing FISHY to protect the farm to fork actors. In the farm to fork scenario, three (farmer, transporter, warehouse) or more (retailer, additional transporters, e.t.c.) actors are involved which are represented as operating different realms, as shown in Figure 9 (based on high-level approach shown in Figure 5).

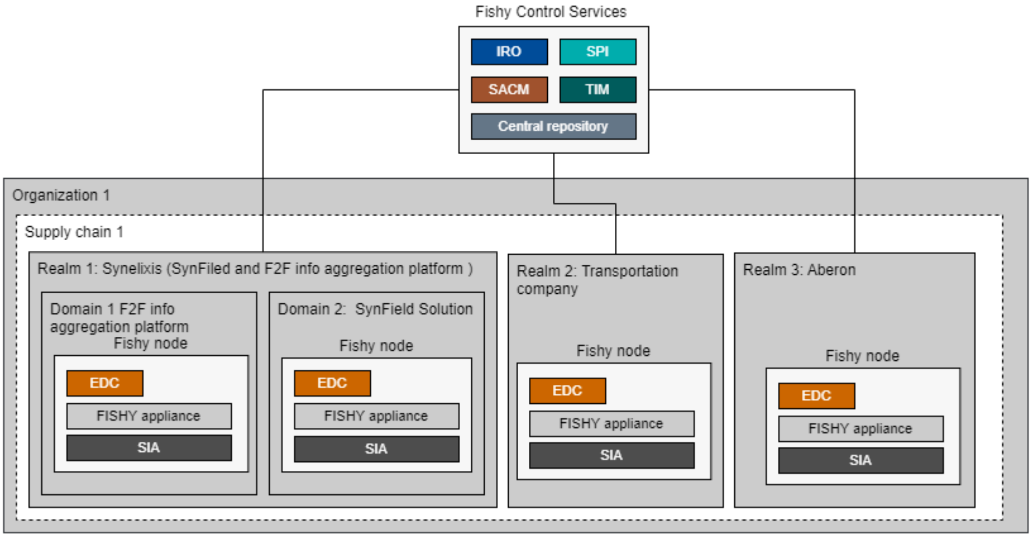

Figure 9: Deployment of FISHY in Farm to Fork use case - option 1

Aberon indicated in the Realm 3 is the IT solution deployed in the warehouse. These three actors deliver the information that is relevant to a specific product to one of the actors (Realm 1 in the figure) which makes it available to the end users (consumers or actors of the supply chain). For this reason, we consider that we have **one organization which consists of a small consortium**. As each of the actors operate a different realm and each of them may have one or multiple domains (as is the case for Synelixis which operates both the SynField Solution and the platform that aggregates the data from the farm, transportation and warehouse), they all need to deploy in their premises the part of FISHY services that is responsible for the collection of data that will enable the detection of attacks and for the deployment of policies that FISHY will suggest. In the case of SYNELIXIS, two domains are distinguished: one is devoted to the aggregation of information from the farm (domain 2) and the other is devoted to the aggregation of information relevant to a specific food product from the IT systems of all the actors (domain 1). In the option presented in the figure (which we denote as option 1), all actors may deploy an instance of the FISHY node in their IT systems. They may all use the same deployment of FISHY Control Services or could (in principle) use different instances of FISHY Control Services.

A second option which is the one adopted during the FISHY project lifetime is shown in Figure 10 (based on the high-level approach shown in Figure 6). In this case, the FISHY node is deployed in the Realm 1 in domain 1 to protect the IT system that aggregates the information from all the actors of the supply chain. While from a first view it seems that this option leaves the rest of the realms uncovered, it has been proven feasible to monitor the flow of information that originates from these realms into the domain 1 and thus be able to identify the origin (realm) where the attack has occurred, provide suggestions and enforce policies. It is worth stressing that the points that should be monitored have to be decided by the administrator/operator of the system together with the rules to apply. Once this is done, the diverse tools of FISHY offer rich capabilities, i.e., are capable of detecting many different types of attacks depending on the needs of each realm.

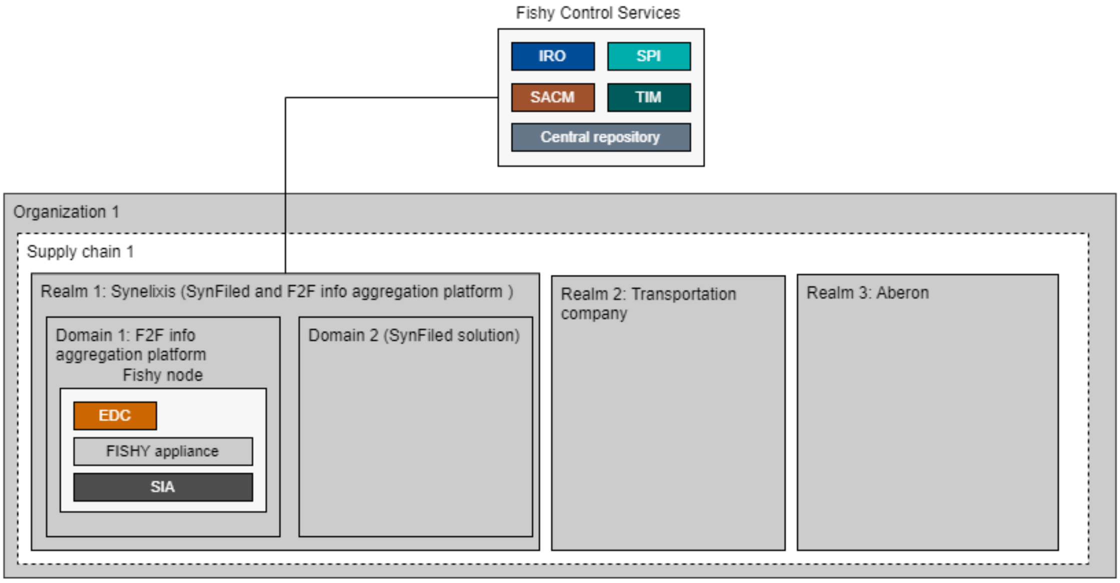
Fishy Control Services
IRO
SPI
SACM
TIM
Central repository
Organization 1
Supply chain 1
Realm 1: Synelixis (SynFiled and F2F info aggregation platform)
Domain 1: F2F info aggregation platform
Fishy node
EDC
FISHY appliance
SIA
Domain 2 (SynFiled solution)
Realm 2: Transportation company
Realm 3: Aberon

Figure 10: Deployment of FISHY in Farm to Fork use case - option 2

From proposed FISHY deployment, in the F2F use case the following modules are used:

IRO / DASHBOARD: It will provide a solution to input/add, and properly configure the components of the F2F infrastructure. It will also provide the dashboard for users at Synelixis to monitor their infrastructure and receive alarms/notifications; With respect to alarms/notifications, through the dashboard they will be able to check whether this information is validated in the blockchain.

TIM: in the Farm to Fork use case, TIM is used to detect the attacks (e.g., LOMOS and Trust monitor) and the Smart contracts component is used to verify the detected attacks and recommended policies.

SACM: is used to detect a subset of the attacks to the F2F platform and to generate “audit certificates” for the operators of the platform.

SPI: Users (Administrator/Security Manager profiles) in order to get access to the system via FISHY dashboard will require to be first registered and secondly logged into the system. This is done using the SPI module (Identity Manager). The Identity Manager will validate the access to provide the right permissions for the specific user profile.

EDC: is used to identify and enforce appropriate policies to mitigate the detected attacks (e.g., ban a specific IP address or a specific wallet id).

Use case 2: overview of the FISHY deployment

The wood base panels use case of Sonae Arauco is composed of 2 major fields of action:

The connected factory: Ensuring the connectivity of the equipment and machines, 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);

The EDI communications: EDI (Electronic data interchange) 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 (both clients and suppliers) by electronic process.

From proposed FISHY deployment, in the WBP use case the following modules are used:

IRO/DASHBOARD: It provides the dashboard for users at Sonae Arauco to both monitor/configure the FISHY integrated tools and their generated alarms/notifications, and interact with the components for needed manual configurations and intents. It will also provide a solution to input/add, and properly configure, new IoT devices to the platform database. Other modules, such as the SACM and the TIM, require information about certified/authorized IoT devices so that its components could either alarm/inform the user/FISHY administrator in the vicinity of a risky situation/attack or certify the readings if normal pattern behavior is identified. In this regard, IRO must make this information available and readable by both modules;

TIM: It will use the XL-SIEM component to collect and evaluate a set of rules regarding the logs sent both from the IoT devices (intermediated by a cyberagent in the EDGE domain) and the Sap Web Dispatcher (intermediated by a cyberagent in the CLOUD domain). The rules will classify the logs as non-threatening or threatening. If the result is the last one then it will classify the events as attacks (brute force, session hijacking, denial of service, malicious malware depending on its characteristics), both generating alarms, to be displayed in the FISHY dashboard, and increasing the level of cyber risk in the RAE component.

SACM: It will firstly collect network traffic readings (evidence collection engine component) from IoT devices via Zeek. These data will be sent to the SACM auditing component for reasoning if a custom based rule, based on expected pattern thresholds criteria is violated or not. Results of the latter reasoning will be displayed on its own GUI (SACM platform) on a real time basis while informing the operators of the FISHY Platform via the Central Repository.

SPI: Users (Administrator, Security Manager and Operator profiles) in order to get access to the system via FISHY dashboard will require to be first registered and secondly logged into the system. This is done using the SPI modules (Identity Manager & Access Policy). The Identity Manager will validate the access to provide the right permissions for the specific user profile.

EDC: It is used to suggest appropriate remediations to mitigate the attacks detected by other FISHY threat intelligence components (e.g., prevent attackers to reach their target machines). The operators evaluate and select specific remediations (via the FISHY dashboard), if the selected remediations imply changes in the security policies, the EDC refines them into low-level configurations that are presented in a human-understandable format. Indeed, the automatic deployment is not required as it is against SONAE security policies.

The envisioned way the FISHY Platform components will be used in this use case is shown in Figure 11, consisting of one organization, Sonae Arauco, and 2 realms, one which corresponds to Information Technology and the other to Operational Technology. Realms can consist of more than one domain, and here we assume OT realm consists of Industrial Production and Edge domain, while IT realm consists of Cooperate and Cloud domain. All realms use the same deployment of FISHY Control Services. The details of the specific use case settings have been described in deliverable D6.3 [6].

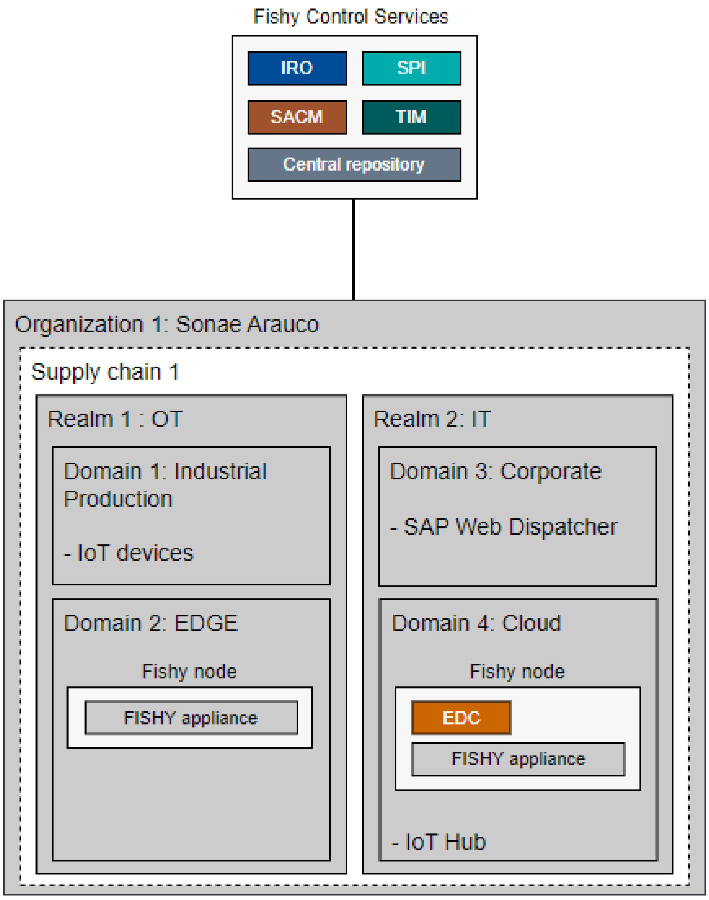

Figure 11: Deployment of FISHY in WBP use case

Use case 3: overview of the FISHY deployment

Capgemini engineering SADE and Facial Key Use Case has 3 major components:

5G Enabled Car: represents a 5G connected car, which follows Capgemini's REMOTIS and AD framework, and where part of the intelligence and ADAS functions, SW management, Facial recognition algorithms are moved to the 5G MEC. Communications between 5G Enabled Car and Edge are protected under 5G mechanisms and under a private mobile connectivity. 5G Enabled Car is not directly integrated to FISHY but indirectly through the Edge.

Edge abstraction of the car at MEC: all logics, intelligence and sensitive data from the car is stored temporarily in the closest Edge node to the car itself. Functions are temporal and deployed on-demand once a car is under the area of serving of a certain CSP Edge node. This component is directly integrated with FISHY and will be under the domain of each the Edge serving the car under a CSP network and under car manufacturer ORGANIZATION.

Car Manufacturer/IoT Provider Clouds: Functions at Car Manufacturer cloud environment (Distributed, centralized, at hyperscale or private cloud) and IoT manufacturer, providing from infotainment to SW management and end-user personal data repository. This component will be the one interacting directly with many of the FISHY modules and will be under the domain of Car Manufacturer Cloud and under Car Manufacturer organization.

From proposed FISHY deployment, in the SADE use case the following modules are used:

IRO: It will provide a mechanism to orchestrate and manage the intents. First of all, SADE UC defines some policies using the IRO dashboard. Then, when SACM detects a revoked certification or TIM detects unauthorized access -for example- , they must generate an intent in accordance with these policies -previously defined by SADE UCs in IRO- and send it to the IRO. IRO is in charge of notifying the EDC to apply actions according to these policies when receiving an intent. It can be under the Car Manufacturer organization and Car Manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

DASHBOARD: It will provide the dashboard for users at Car Manufacturer organization to access to the system to control the SW supply chain of the IoT Components of the car, it will interact with Car Manufacturer Cloud server via a REST API to get SW status and repository of each car, Edge domain where the car is located. It can be under the car manufacturer organization and car manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

SPI: Users (Car Manufacturer, Administrator, Dealer, Owner, IT Supplier) in order to get access to the system via dashboard will require to be first registered and second to log into the system. This is done against the SPI module (Identity Manager). This Identity Manager will interact via API with the car manufacturer API (SADE API). SADE API (located in a Car Manufacturer Cloud domain) will validate this token to provide the right access to the information user will have access via a from at IRO which is provided by the SADE API. It can be under the car manufacturer organization and car manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

EDC: the EDC will be initially triggered by IRO when new intents or policies are created, or the existing ones are updated. These updates can be due to an automatic reaction (e.g. an automatic response to an ongoing attack) or manually by the administrators (via the dashboard). IRO will compile the intents into a set of high-level policies, and it will store them into the Knowledge Base. The EDC will then react to the Knowledge Base change and will enforce the high-level policies by deploying and configuring the appropriate NSFs via the SIA). When TIM detects an unauthorized driver trying to start the vehicle, or SACM detect a compromised component, they create an intent in IRO. According with policies, EDC will trigger notifications or updates using Car Manufacturer API (SADE API), located in a Car Manufacturer Cloud domain. EDC can be under the car manufacturer organization and Car Manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

SACM: It will provide:

- **Evidence Collection Engine**: will interact via API with the Car Manufacturer RabbitMQ (SADE RabbitMQ). From SADE RABBITMQ (located in a Car Manufacturer Cloud domain) SACM will consume real time status of SW components for the car. SADE RabbitMQ will be fed from the EDGE components associated with the car.
- **Certification**: It will get the list of certified components and SW versions via API with the car manufacturer API (SADE API).
- **Audit**: it will use information gathered above to compare the evidence generated list with the list of certified components and report it back to IRO.

SACM can be under the car manufacturer organization and Car Manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

TIM: It will retrieve access attempts information via API with the car manufacturer API (SADE API) which is located in a Car Manufacturer Cloud domain). From that information it will detect: (I) failed logins (unauthorized access attempt) to SADE API and (II) Unauthorized drivers trying to use the car (unauthorized driver). TIM can be under the Car Manufacturer organization and Car Manufacturer Cloud domain or in a different organization if SW Supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers.

SIA: It will provide the abstraction and secured communications among all the components:

FISHY Control Services Cloud: This can be under the Car Manufacturer organization and Car Manufacturer Cloud domain or in a different organization if SW supply chain is managed by a third entity such as an outsourcing company managing those services for several car manufacturers. A NED Entity will be providing the required connectivity

Car Manufacturer Cloud Domain: Central services from Car Manufacturer. A NED Entity will be providing the required connectivity

Edge CSP Domain: Temporal instantiation of car services close to the actual car. A NED Entity will be providing the required connectivity.

The required architecture will be following below diagram:

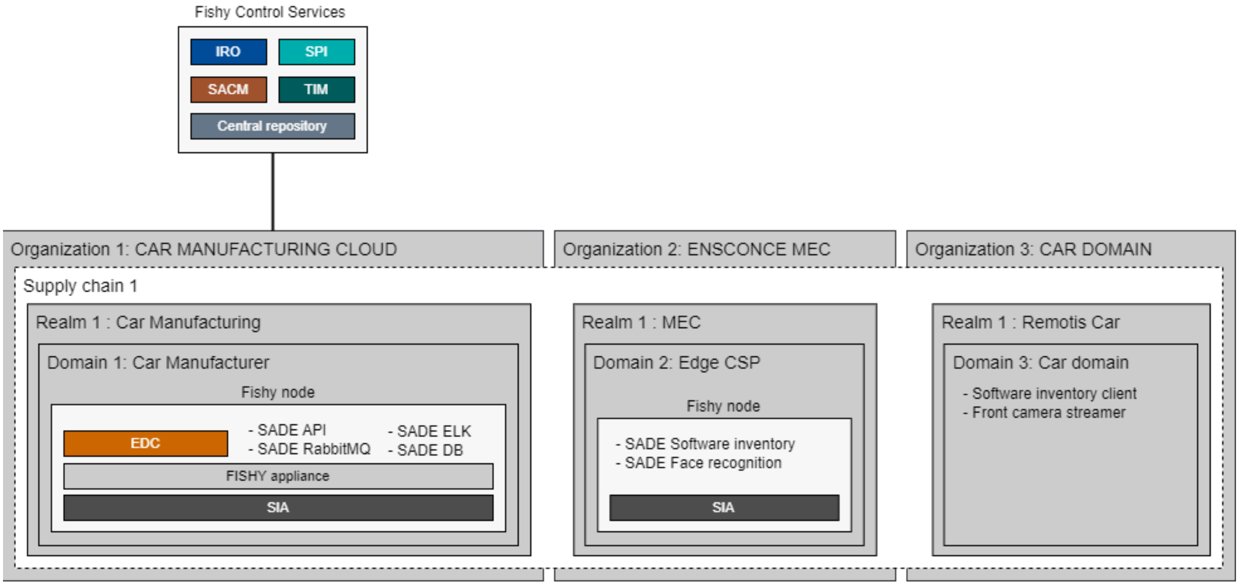

Figure 12: Deployment of FISHY in SADE use case

5 FISHY radar final update

During this this final stage of the technological radar, the work of the FISHY team was focused on improving the usability of the available data by consortium partners (the data collection and description is described in the deliverables D2.1 [5] and D2.3 [2], and in improving the existing resources based on the feedback of its usage and the needs envisioned.

In the following sections, we discuss the highlights of the FISHY Radar in its final stage, its interaction with other tasks in the project, and the sustainability of it in relation to the sustainability of FISHY itself. We will continue with the work together with use case owners to further identify technological imperatives in the context of the exploitation of the opportunities deriving from their business cases. We also provide an update on the technological and market landscape through the IP-focused whitespace analysis, guided by the KERs elaborated across this project and their innovation. Finally, we will present the extension of the legal and regulatory landscape, including the legislation in Greece, Switzerland, Germany and Portugal, extending the already existing coverage for Slovenia, Spain and Italy (leveraging the input from Consortium partners), and the standards that the project relates with. While this mostly European coverage will be improved with the further extension when a technological adopter's regulatory environment is not reflected in this coverage, it is diversified enough to provide us with a clear perspective on what to expect. In regard to the standards included, this work is further developed in the context of the task 7.2 and will be published in the final impact generation deliverable, D7.4 (public version) and D7.7 (confidential version).

5.1 Main achievements of the FISHY Radar

In this final reporting period for Task 2.1 we have updated the FISHY Radar in its several dimensions, overviewing the scientific, technological, market competitive and regulatory landscapes. We have evaluated the overall novelty through the white space analysis of the FISHY solution guided by the 7 KERs. The usefulness of radar is boosted by the update described in this section, based on the live document that is the core of the FISHY Radar (initially described in the deliverable D2.1 [5]) that also contributes to the sustainability of the project. The following table (Table 3) wraps-up the activities of the FISHY Radar and exposes the valuable content it holds over a KPI measurable format. The details of these achievements are discussed throughout Section 6, and build on the information published in the public deliverables D2.1 [5] and D2.3 [2] and on their confidential versions D2.5 [8] and D2.6 [9].

Table 3: KPIs for the FISHY Radar activities

Landscape	KPI	Description	Metric	Status
Science and Technology Landscape	Technological Trends	Identification of trends in related domains	# of domains of action analysed	9
	Research Questions	Questions driving the research in the project	# of questions	12
	White Space Analysis	The most related IPO patent classes to KERs	# of related CPC classes	10
Market Landscape	Market Trends	Identification of market trends and segments	# of analysed market trends	12
	Competitors	Competitors' identification &	# of analysed	38

		analysis	competitors	
	Competitor Features	Identification of main features & differentiators	# of competitors’ features	71
	Business Models	Competitors’ business (including BMC/SWOT)	# of analysed business models	20
Legal and Regulatory Landscape	Legislation and Standards	Legislation & regulation affecting FISHY	# of legislation items	36
Technological Imperatives	Technological Imperative Features	Main technological needs in competitors by use case owners	# of features	14
	Alternative Technologies	Analysis of advantages of alternative technologies at use case owners	# of technologies	15

5.2 Technological imperatives from use cases

In this section we will be discussing the work done with the project’s use case owners towards the identification of exploitation opportunities from the analysis of their technological imperatives. This work builds on what was published in the deliverables D2.1 [5] and D2.3 [2] over the same topic. Its outcomes contribute to the other tasks in WP2, complementing the collection and analysis of requirements, the architecture of the FISHY solution, but also provide valuable input to the competitors analysis and exploitation activities in WP7.

For this analysis we have used the eight domains of action defined in the deliverable D2.1 [5] and extended in D2.3 [2], referenced below as follows:

- D1. Vulnerability Forecast & Risk Estimation (TIM)
- D2. Security & Privacy Dataspace Infrastructure (SPI)
- D3. Secure Infrastructure Abstraction (SIA)
- D4. Enforcement & Dynamic Configuration (EDC)
- D5. Intent-based Resilience Orchestration (IRO)
- D6. Security Metrics Assurance / Evidence & Certification Management (SACM)
- D7. Evidence & Certification Management
- D8. Dashboard & Platform

The technological imperative features were collected by the direct input of use case partners in a total of 14, classified based on the MoSCoW methodology [25] based on: M - Must have, S - Should have, C - Could have, W - Won't have. In the following we describe each of the features in analysis, per use case, (the alternative technologies in place that will be substituted or complemented by the FISHY solution in the use case premises are reported in FISHY Radar live document and are still to be updated as part of activities of WP7.

UC: Securing Autonomous Driving Function at the Edge (SADE)

- **F1**. [Must] Deployment of software updates from the cloud to any connected device able to fix problems, provide new functionalities, or counter emerging methods of attack, and in that way enhance the support personnel’s time and productivity.
- **F2**. [Must] Independent of devices.
- **F3**. [Must] Offering a way to abstract the vehicle communications within the EDGE.

- **F4**. [Must] Allow applying GDPR and similar regulations.

UC: Farm-to-fork Supply Chain

- **F5**. [Must] Providing controlled access to immutable information from three actors in the supply chain.
- **F6**. [Must] Protection against cybersecurity attacks to (web/e-mail) servers and databases, and attacks to cloud environments and components (e.g. Openstack, Kubernetes, OSM).
- **F7**. [Must] Ensuring controlled access to actor-specific information (anonymization and encryption).
- **F8**. [Should] Protection from blockchain threats.
- **F9**. [Must] Collecting information from the different network parts from the diverse organizations participating in the supply chain so as to monitor the operation and evaluate the security level of the whole supply chain.
- **F10**. [Must] System audit and providing “certificates” for the supply chain as a whole.

No alternative technologies have currently been reported in the FISHY Radar.

UC: Wood-based Panels Trusted Value-Chain

- **F11**. [Must] Ensuring that information is accessible only by the authorized stakeholders.
- **F12**. [Must] identifying, assessing and suggesting mitigation actions against security/privacy risks in a complex, distributed and interconnected ICT environment.
- **F13**. [Must] To be agnostic in terms of technologies, thus allowing for the integration of different ICT systems (IoT devices).
- **F14**. [Must] To be agnostic in terms of technologies, thus allowing for the integration of interconnected electronic data interchange platforms (EDI).

In the following table (Table 4), we represent the matrix of technological imperatives, indicating the features provided by the use cases, and their impact per domain of action. It highlights that some of those features relate to as much as six out of eight domains of action, while others can relate with only one of those domains. Moreover, all the domains of action have technological imperative features relating to each of them, with most relating to TIM (D1), SIA (D3) and EDC (D4).

Table 4: Matrix of technological imperative features per domain of action

Feature	D1	D2	D3	D4	D5	D6	D7	D8
F1			X					X
F2			X					
F3			X					
F4						X		
F5		X						
F6	X			X				
F7		X						
F8	X			X				
F9	X	X	X		X			X
F10							X	
F11	X	X		X		X		X

F12	X	X		X		X		X
F13	X	X	X	X		X		X
F14	X	X		X				

5.3 Technological and market landscape update

Building on the work done in the Task 2.1 regarding the technology and market overview in the context of the FISHY Radar strategy, with results published in the deliverables D2.1 [5] and D2.3 [2], and extended in their subsequent confidential versions, we have prepared the whitespace analysis for the FISHY technology. This methodology consists of the evaluation of the existing products, services, and markets to address unmet customer needs, complementing the traditional feature-based market analysis, and adding to it an IPR management perspective.

To access the information on CPC classes (Cooperative Patent Classification) and patents we have used the Google Patents search engine[1], that provides the detailed information about the identified patents and related CPC classes, and the well-known Espace.net [26] that has useful advanced search options to look for CPC classes and patents from key phrases related to the technology in analysis.

We have used the 7 KERs to guide this analysis, considering in the IP search: (i) the keywords that can focus the findings; (ii) the innovation highlighted in the exploitation results; and (iii) the exposure that these had in the lifetime of the project. As this analysis has an important IP sense to it, the exposure of results in publications, conferences and blog posts can affect its IP protection. On the other hand, the essential innovation will allow us to better determine the novelty of the FISHY assets in the context of the related CPC classes and identified patents.

5.3.1 KER 1: Platform

Keywords: Security Platform, flexible dashboard, APIs for integration, multi-tenant design, hierarchy of authorization.

Innovation: Intelligence for the IDE tailored to the current needs of cybersecurity for supply chains, with different approaches, user interfaces and tools adapted to accommodate the FISHY needs and technical specifications.

Exposure: journal papers, and conference talks and proceedings, GitHub repo.

5.3.2 KER 2: TIM

Keywords: vulnerability assessment, risk estimation, impact assessment, mitigation, incident detection.

Innovation: storage component with an integrated pub-sub layer, ML-based incident detection system

Exposure: blog post and GitHub repo.

5.3.3 KER 3: IRO

Keywords: orchestration of security processes, intent compilation, machine-readable intents

Innovation: built from scratch, create high-level security intents, and incorporate smart contracts

[1] https://patents.google.com/

Exposure: journal papers, and conference talks and proceedings, GitHub repo, blog post, social media

5.3.4 KER 4: SACM

Keywords: Security Assessment, Data Quality Control, Evidence & Certification Management, Security Metrics Assurance

Innovation: extending the security metric/rules STS already has, providing regulatory compliance and SLA support.

Exposure: GitHub repo, blog post, social media, journal papers.

5.3.5 KER 5: SPI

Keywords: Privacy enhancement, Data Management, Data Quality Control, identity and access management, data anonymization

Innovation: Semantic Data Aggregator to incorporate new pre-processing mechanisms (anonymization, new metadata models…)

Exposure: GitHub repo

5.3.6 KER 6: EDC

Keywords: API/network monitoring, analysing infrastructure capability, generation of policies to be enforced.

Innovation: make use of a highly flexible security capability model and an inferential engine to smartly refine high level policies into low level configurations.

Exposure: journal papers, conference talks and proceedings, GitHub repo

5.3.7 KER 7: SIA

Keywords: API/network monitoring, execute a policy, secure cross-domain connectivity

Innovation: Inter-Domain Connectivity Orchestrator aware of the FISHY framework

Exposure: GitHub repo, blog post, social media.

Based on the above we have identified 10 CPC related classes that relate to several aspects of the FISHY technology, as shown through the matrix (Table 5) in below.

- **CPC 1**. G06F21/45 Structures or tools for the administration of authentication
- **CPC 2**. G06F11/30 Monitoring
- **CPC 3**. G06Q10/0639 Performance analysis
- **CPC 4**. G16Y20/00 Information sensed or collected by the things (in IoT)
- **CPC 5**. G16Y40/00 IoT characterised by the purpose of the information processing
- **CPC 6**. G06F16/21 - Design, administration or maintenance of databases
- **CPC 7**. G06F16/00 Information retrieval; Database structures; File system structures
- **CPC 8**. G06F9/4881 Scheduling strategies for dispatcher, e.g., round robin, multi-level priority queues
- **CPC 9**. H04L9/00 arrangements for secret or secure communications; Network security protocols
- **CPC 10**. G06F21/00 Security arrangements for protecting computers, components thereof, programs or data against unauthorized activity

All the above CPC classes are described in detail on Google Patents[2] or Espacenet[3]. In this IP context we have also identified 2 patents that relate to FISHY but are not a bottleneck to the project's innovation. These are:

- **US9716595B1** - System and method for internet of things (IoT) security and management [27]: established to ensure secure communication between several IoT devices, using digital tokens for authentication through a unique identification key.
- **US2022232040** - Advanced cybersecurity threat mitigation using software supply chain analysis [28]: ensures a comprehensive cybersecurity threat assessment of software applications based on vulnerabilities at all the levels of the software supply chain.

Table 5: Matrix of white space analysis

Feature	KER 1	KER 2	KER 3	KER 4	KER 5	KER 6	KER 7
CPC 1	X	X					
CPC 2		X		X			
CPC 3			X	X			
CPC 4					X		
CPC 5					X	X	
CPC 6			X				
CPC 7					X		
CPC 8							X
CPC 9							X
CPC 10	X	X				X	

5.4 Further legal and regulatory landscape

In the following section we update the legal and regulatory landscape in the FISHY Radar, including the input of consortium partners on the coverage at Greece (SYN), Portugal (SONAE) and Germany (TUBS), extending the input of Italy, Spain, Slovenia, European and worldwide international. We also add the relevant standards, in collaboration with TID, considering those that most affect the technological development and operations of FISHY.

In this regard we describe in detail the legislation and regulation identified as affecting FISHY, as well as the standards that follow this scope, adding from all the items already published in the FISHY Radar update deliverable, D2.6 [9]. This update includes the ISO 28001:2007 in the landscape, as well as four European Commission's regulations regarding online businesses, open internet, electronic communications and the Digital Single Market. This update also includes regulations specific to Italy, Portugal and Germany that affect FISHY or its use cases, having had the review of SYN to ensure that the regulations standing in Greece on this regard are in the scope of the collected landscape.

Regulation: **(ISO) Requirements and guidance for security management systems for the supply chain** [29]

Regulator: UN / Region: Worldwide / Reference: ISO 28001:2007

Impact on FISHY: Medium

[2] https://www.google.com/?tbm=pts
[3] https://worldwide.espacenet.com/

Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance. General framework on security mechanisms for international supply chains.

Regulation: **(EU) 2019 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services** [30]

Regulator: EC / Region: EU / Reference: PE/56/2019/REV/1

Impact on FISHY: Medium

Defines the European Standards Organisations, their interaction with regulation and their cooperation framework, updating the version of 25 October 2012 with the reference 1025/2012.

Regulation: **(EU) 2015 of the Open Internet Regulation** [31]

Regulator: EC / Region: EU / Reference: 2015/2120

Impact on FISHY: Low

Applies to Internet service providers, and specifically to Net neutrality. Article 3.3 defined cybersecurity and safety as a valid exception to alter neutrality.

Regulation: **(EU) 2018 on European Electronic Communications Code** [32]

Regulator: EC / Region: EU / Reference: 2018/1972

Impact on FISHY: Low

Reference directive for all types of electronic communications in Europe.

Regulation: **(EU) European Economic and Social Committee regulation on the Digital Single Market Strategy** [33]

Regulator: European Economic and Social Committee / Region: EU / Reference: N/A

Impact on FISHY: Medium

Define the European strategy for implementing the Single Market in digital spaces.

Regulation: **(IT) Guidelines on the use of cookies and other tracking tools** [34]

Regulator: Italian Government / Region: Italy / Reference: N/A

Impact on FISHY: Low

This decree dictates how cookies should be used to avoid tracking purposes - this might have some implications on the dashboard or other web base UIs.

Regulation: **(IT) Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies** [35]

Regulator: Italian Government / Region: Italy / Reference: N/A

Impact on FISHY: Low

This decree dictates how cookies should be used to avoid tracking purposes - this might have some implications on the dashboard or other web base UIs.

Regulation: **(IT) Vehicle Geo-Location and Employer-Employee Relations** [36]

Regulator: Italian Government / Region: Italy / Reference: N/A

Impact on FISHY: Low

This can have some impacts on the SADE use case.

Regulation: **(PT) of the Cyberspace Security Legal Framework and defines the obligations regarding cybersecurity certification pursuant to Regulation (EU) 2019/881 of the European Parliament** [37]

Regulator: Portuguese Government / Region: Portugal / Reference: N/A

Impact on FISHY: Low

The present decree-law carries out the Regulation on the legal framework for cyberspace security, concerning measures to ensure a high common level of network and information security across the Union; the implementation of European regulations on cyber security certification.

Regulation: **(DE) of the Federal Data Protection Act (BGBl. I p. 2097), last amended by Article 10 of the law of June 23, 2021 (BGBl. I p. 1858; 2022 I 1045)** [38]

Regulator: German Government / Region: Germany / Reference: N/A

Impact on FISHY: Low

Amendment complements and specifies the Datenschutz-Grundverordnung (German implementation of GDPR) where gaps are left to state-level regulations. This includes processing of employee's data, commission of a data protection officer, as well as video surveillance.

Regulation: **(DE) of the IT Security Act, increasing the security of information technology systems** [39]

Regulator: German Government / Region: Germany / Reference: N/A

Impact on FISHY: Low

Defines duties and protocols for operators of critical infrastructure with respect to security incidents.

Regulation: **(DE) of the IT Security Act 2.0** [40]

Regulator: German Government / Region: Germany / Reference: N/A

Impact on FISHY: Low

Extends the definition of critical infrastructure from the IT Security Act.

5.5 Research Landscape Update

In this section, we give an overview of the research trends and challenges significant for FISHY. This section has been updated from the previous deliverable versions D2.1 [5] and D2.3 [2] which were submitted in months M6 and M18, respectively, to reflect important changes in the last 12-month-interval. However, it should be noted that many trends that were relevant at the time of the previous submissions remain the same (for further details about recurrent research trends refer to the mentioned deliverables D2.1 and D2.3). This section elaborates on the research trends, and questions over each of the ten domains of action defined in FISHY.

5.5.1 Intent-based networking and orchestration

Intent-based interfaces have emerged as the preferred north-bound interfaces in programmable network management concepts which can provide applications with a syntax to define what is desired from the network which can be agnostic of the underlying technology or the specific mechanism / algorithm to fulfill a request. With the use of intents, the applications can treat the underlying network technology as a black-box.

The main research questions that the FISHY team has been focused on in regard to the IRO are: *(i) Can we design an autonomous intent-based orchestration interface able to assure the resilience of an ICT supply chain? (ii) How can AI be used to create general self-healing networks?*

In D2.3 [2], we reported that a significant number of recent works have promoted the integration of AI/ML techniques with resilience orchestration for automation of the interactions between the user and the system through definition and application of high-level intents. In addition, the following trends have recently emerged in the literature:

- Intent-Based Data Centers: As the network infrastructure has become more and more disaggregated, there are increasing requirements for different approaches in network management. SDN has been proposed as a key technology to manage the network, but existing SDN products are limited to specific vendors. Thus, scaling applications in a heterogeneous infrastructure, such as a multi-cloud environment, becomes a difficult task to achieve. One of the potential solutions in network management, which aims at enabling easy network orchestration in a heterogeneous environment, lies in Intent-Based Data Centers [14].

- Automation of the intent-based service operation: Development of an intent-based network that would automate or make all parts or processes of the network intent-based, the intent orchestrator, having a holistic control over the infrastructure, and would manage all aspects of the network [15].
- Intent-based network operations using natural language texts: This approach includes development of a robust conflict solving engine for intent-based networking that identifies potential disruptions by incumbent intents [16].
- Self-configuration: A proactive self-configuration solution of intent-based networking using artificial intelligence methods has been presented and described in [17].

This high-relevance research topic has seen its outcomes published in two conference papers ([44] and [45]) and a IRO-specific blog post [46], with several other publication works in preparation.

5.5.2 Security in IoT

Security in IoT comprises the techniques, controls and procedures already studied under the Information Security umbrella, adapted and, in a few cases, extended, to the emerging ICT developing paradigm known as the Internet of Things (IoT). It was a topic of discussion both in the initial deliverable D2.1 [5] and its follow-up D2.3 [2], both in the context of the scientific and the market landscapes. There are two main questions that the experts of FISHY have been focusing on regarding this highly-relevant research topic: *(i) How to adequately characterize an OT (Operational Technology) environment in terms of cybersecurity requirements/objectives?; and (ii) How to evaluate the effectiveness of security controls in complex ICT environments based on the IoT paradigm?*

The research questions involved are vast and can receive contributions from different areas. Based on the available use cases in the FISHY project and especially within the scope of WP3, the focus has been on Access Control (preventive) and the detection of anomalies in terms of network traffic caused by the dysfunction of one or more IoT components. In Access Control and more specifically in the Authentication and Authorization functions, an infrastructure adapted to the requirements of FISHY was created, using the OpenID Connect and OAuth2 protocols - using open-source solutions - to control the access of users and software modules to any internal data source. Furthermore, some efforts have been devoted to developing a formal process for specifying and verifying Access and Privacy Policies in this context. Experiences are in progress with XACML tools.

For network traffic anomaly detection, an extensive dataset was captured in one of the use cases related to industrial activity, exploring open-source tools for collecting metrics and data analysis. This work in progress should be fully functional on the project's IT-2. A study on taxonomies of metrics suitable for the ICT context and focused on OT has been developed in parallel to this task.

Finally, some efforts have been devoted to studying a common format to leverage the correlation potential of all FISHY-integrated tools. This work resulted in the choice of CEF, with very generic characteristics and able to accommodate all types of events generated in FISHY. Subsequently, an internal format conversion service was developed to have all events in the CEF format in the Central Repository.

The outcomes of this research were published in the proceedings of: (i) the 16th International Conference on Availability, Reliability and Security in 2021 **¡Error! No se encuentra el origen de la referencia.**; and on (ii) the 18th International Conference on the Design of Reliable Communication

Networks (DRCN) in 2022 [55]. A blog post focusing on this topic is in preparation, together with other scientific publications.

5.5.3 Blockchain in supply chain operations

This domain of action is focusing on the use of blockchain technology in a complete ICT supply chain operation with partial implementation to make it practical and effective. *The main research question is: Can we improve the authentication of IoT devices related to the supply chain?*

This is a research with a high potential, explored in the deliverable D2.3 [2], but not yet reported in any deliverable of WP5. Initial conversations are being held between UPC, UC3M and TID to use SEN for authenticating IoT devices. In the Use Case infrastructure, in some cases these IoT devices may be considered data collectors providing security data to the FISHY platform. Moreover, there is a conference paper [20] and a blog entry [21] related to this research.

An additional research question has been identified in the last year of the project: *Can we use blockchain technology so that security platform offers immutable information to their users?*

The answer is positive and the deployment of smart contract component in FISHY will be disseminated in this last year of the project.

5.5.4 Vulnerability Management

Vulnerability assessment is a domain of action defined already in D2.1 [5] and represents a critical component of the vulnerability management and IT risk management lifecycles in the companies of any size, protecting systems and data from any unauthorized access and data breaches; and improving overall security of companies' systems. Its outcomes are reported in the deliverables D3.1 [11], D3.2 [12], D3.3 [3] and D3.4 [13], and published in the blog post [22].

The main research question pursued in FISHY in this context is*: Can AI improve the vulnerability assessment process traditionally done through rule-matching?* This is of medium relevance mostly because it is not an early-defined priority in the project, but it represents an important value added to the FISHY technology aligned with the most recent market trends.

The mentioned WP3 deliverables describe the scopes of vulnerability assessment offered by FISHY.

5.5.5 Risk Assessment

Risk Management is a key process to identify, evaluate and control threats that could endanger a company. FISHY brings RAE (Risk Assessment Engine) as one of the building blocks constituting the Trust & Incident Manager (TIM) which in turn is part of the Trust Manager (TM). Building on top of what is explained in D2.1 [5], and putting the main focus on the innovation roadmap associated to RAE, briefly presented in D3.1 [11], there are different research lines open to enhance the RAE with associated ongoing work to address research questions like *1) integrating Threat Intelligence information in order to influence cyber risk evaluation; 2) evaluating each single infrastructure element taking into account the cyber climate of other neighboring infrastructure elements and 3) identifying cyberattacks to which the verticals of the three FISHY use cases show to be prone, and once identified develop tailored cyber risk models that would extend the existing model catalog.*

5.5.6 Security Platforms

Security Platforms integrate several tools to help enforce security and resilience of communication infrastructures, applications, networks and services. It is a domain of action defined in D2.1 [5] with a main research question: *Can we provide a platform by means of a dashboard integrating all the tools and providing the whole workflow from the data gathering to the attack detection, to security* *assurance, risk assessment and finally the mitigation and network enforcing? and in a friendly environment*. Ongoing efforts are being done to integrate under a single umbrella all tools to be considered in FISHY. This umbrella must include a single-sign-on when possible, to facilitate access while also guaranteeing users authentication. The proposed dashboard will use different integration profiles according to the task/tool to be shown, thus accommodating both users and tools needs and requirements. Moreover, in all the deliverables, mostly in those of WP5 (integration of the whole FISHY Platform reported in deliverable D5.1 [10]) and WP6 (validation of the FISHY Platform reported in deliverable D6.1[6]) the progress in research in this shown. There are different research publications and blog entries that also show this progress, including three related conference papers ([48], [49] and [50]) and three blog posts were published on the topic ([51], [52] and [53]).

5.5.7 Security Assurance & Certification Management

This domain of action defined in D2.1 [5] corresponds to the KER 4 with the same name and is focusing on security assurance as the actual measurement of confidence that security practices and features, including procedures and architecture of an information system which enforces the security policy. It is considered of medium relevance in the research pathways of FISHY, following the research questions: *Measurement of confidence that security practices and features, including procedures and architecture of an Information System is a resource demanding procedure. Is there a technology/architecture that can boost this procedure? Is there a universal language that can describe the access policy rules?*

WP4 deliverables (particularly D4.3 [4]) describe the core implementation of STS Security and Assurance platform, which include the core component of the auditing mechanism (monitor). The latter is based on Drools technology [43], a group of tools that provide the ability to make sense of the logic and where data is present in business processes. On the other hand, Assurance platform uses Event Calculus, a logical language for representing and reasoning about actions and their effects as time progresses. It has one published research paper solving incident handling in healthcare for supply-chain management.

5.5.8 Intrusion and Detection Services

This domain of action explores the potential of IDSs offering the ability to analyze types and frequency of the threats and accordingly security controls, security responses and overall strategies can be improved. The research potential in the context of FISHY is low, complementing other developments of bigger relevance. It is nevertheless advancing with the research question: *How to successfully combine host-based and network-based IDS system and enhance their performance with a second layer of ML assisted anomaly detection?*

Its main outcomes are published in the blog post [22] and reported in the WP3 deliverables describing the comprehensive IDS "net" cast by FISHY. XL-SIEM and Wazuh complement each other with event correlation and an out-of-the-box large set of rules capable of detection of events on a wide range of devices and software. FISHY further enhances the IDS capabilities by LOMOS performing a second pass on the gathered data and produces anomaly scores using an ML-supported method.

5.5.9 Integrity Assessment

The angle of FISHY on integrity assessment is focusing on a zero-trust security system that relies on the idea that nothing and nobody should be trusted, so that the security controls should not only inspect the perimeter of an IT infrastructure, but also safeguard the security from the inside.

The main research question here is: *Can zero-trust security systems be used to safeguard the integrity of a physical/virtual node with a high level of trust and a minimum level of effort for the administrators?*

The WP3 deliverables (in particular D3.1 [11] and D3.3 [3]) report the features, capabilities, and integration within the FISHY ecosystem of the Trust Monitor, the tool used to perform the integrity assessment. The Trust Monitor leverages the TPM 2.0 hardware capabilities and several Linux kernel modules to perform the integrity assessment of physical nodes and Docker containers. These results are still unpublished and will be used to prepare a journal paper.

5.5.10 Cloud-native networking API

The path towards cloud-native approaches to all kinds of services (from connectivity to AI) will enable a cloud-edge continuum and the integration of networks and clouds in a unique, distributed information processing machinery. To achieve this vision, a consistent set of APIs is required.

In particular, we consider here a networking API able to support seamless connectivity, in all its phases: fulfillment (supporting policy-controlled requests), assurance (supporting dynamic monitoring) and decommissioning (supporting ordered shutdown).

The research questions guiding this high relevance research work are: *How to incorporate intent into requests and associate it to service offerings? How to translate intent into SLAs and verify their enforcement? How to define monitoring criteria and dynamically apply them during service lifetime? How to address resource and service conflicts? How to incorporate smart contracts to SLA enforcement?*

The work in SIA has allowed the FISHY team to come with a first proposal on this kind of cloud-native API. Currently, SIA offers a consistent connectivity model, able to combine SDN programmability with cloud-native elasticity. Progress has been made as well in addressing monitoring procedures, and its outcomes are being reported in the deliverables D5.1 [10] and D5.2 (due in M32), as well as in the blog post [23] and in the research paper [24].

6 Conclusions

This deliverable describes the second version of the FISHY architecture and the final stage of FISHY Radar (aligned to iteration 2). It presents an updated and modified architectural design based on the limitations and experiences reported during the deployment and integration phases of the IT-1, and the development of its modules.

The resulting deliverable offers a modified architectural solution, described in detail in Section 2, along with revised description of action areas of concern considered by the FISHY team. A more detailed description of the FISHY updated modules of IT-2 architectural design, which takes into consideration experiences from the practical implementation and integration of modules, is described in Section 3. This section also offers an updated specification of the high-level operational communication workflow between all components of the FISHY final architecture. In Section 4, new mapping and deployment between modified FISHY architectural solution and defined use cases is explained. This section also includes the revision of general requirements and constraints necessary for a successful development of the FISHY architecture, which were first identified in IT-1 and reported in D2.2 [1].

As the last step, in Section 5, the final stage of the FISHY Radar is overviewed, providing an update on the technological and market landscape in relation to FISHY's domains of action, as well as the research pathways, and the legal and regulatory landscape extended to more geolocated legislation and including related standards (in line with the work developed in the Task 7.2).

References

[1] [FISHY] - *D2.2 IT-1 architectural requirements and design.* A. Jukan, J. Dizdarević. 2021

[2] [FISHY] - *D2.3 Tracking external efforts, technology evolution and business trends (II),* J. Pita Costa, 2021

[3] [FISHY] - *D3.3 Trust Manager components design and implementation (IT-2),* H. Santos and A. Oliviera, 2022.

[4] [FISHY] - *D4.3 Security and Certification Manager components design and implementation (IT-2),* G. Kalogiannis, 2022.

[5] [FISHY] - *D2.1 Tracking external efforts, technology evolution and business trends (I),* J. Pita Costa, 2021.

[6] [FISHY] - *D6.3 Use cases settings and demonstration strategy (IT-2),* Antonis Gonos, 2021.

[7] [FISHY] - *D4.2 Security and Certification Manager IT1 integration*, Jose Francisco Ruiz, 2021.

[8] [FISHY] - *D2.5 Tracking external efforts, technology evolution and business trends – CO (I)*, Joao Pita Costa, 2021.

[9] [FISHY] - *D2.6 Tracking external efforts, technology evolution and business trends – CO (II)*, Joao Pita Costa, 2022.

[10][FISHY] - *D5.1 IT-1 FISHY release integrated,* Jose Manuel Manjón, 2022.

[11][FISHY] - *D3.1 Trust Manager components design and implementation (IT-1),* Diego López, Antonio Pastor, Luis Conteras, 2021.

[12][FISHY] - *D3.2 Trust Manager IT1 integration,* Eva Marin-Tordera, 2021.

[13][FISHY] - *D3.4 Trust Manager IT2 integration,* Eva Marin-Tordera, 2023 (to be submitted in M30).

[14]Kerravala Z. (2018), *Intent-based data centers: are the next evolutionary step for enterprises*, White Paper, ZK Research A Division of Kerravala Consulting.

[15]Kuroda T., Yakuwa Y., Maruyama T., Kuwahara T. and Satoda K. (2022), *Automation of Intent-based Service Operation with Models and AI/ML*, NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 2022, pp. 1-6, doi:10.1109/NOMS54207.2022.9789924.

[16]Saha B. K. , Haab L. and Podleski L. (2022) , *Intent-based Industrial Network Management Using Natural Language Instructions*, 2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6, doi: 10.1109/CONECCT55679.2022.986573.

[17] Velasco L., Barzegar S., Tabatabaeimehr F. and Ruiz M. (2022), *Intent-based networking and its application to optical networks [Invited Tutorial]*, in Journal of Optical Communications and Networking, vol. 14, no. 1, pp. A11-A22, January 2022, doi: 10.1364/JOCN.438255.

[18] ETSI GS NFV-SOL 005 V3.6.1 https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/005/03.06.01_60/gs_NFV-SOL005v030601p.pdf, retrieved 2022-12-01.

[19]ETSI GS NFV-SOL 006 V4.3.1 https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/006/04.03.01_60/gs_NFV-SOL006v040301p.pdf, retrieved 2022-12-01.

[20]Martínez M., Marin-Tordera E. and Masip-Bruin X. (2021), *Scalability analysis of a blockchain-based security strategy for complex IoT systems,* Proceedings of 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR).

[21]Martínez M. (2021), *Securing IoT nodes in supply of chains*. FISHY Blog. https://fishy-project.eu/blog/securing-iot-nodes-supply-chains, retrieved 2022-12-29.

[22]Antić J. (2021), *The importance of early detection of vulnerabilities and attacks for a healthy supply chain*. FISHY Blog. https://fishy-project.eu/blog/importance-early-detection-vulnerabilities-and-attacks-healthy-supply-chain, retrieved 2022-12-29.

[23]Manjón Cáliz J. M. (2022) *A reference framework for FISHY*. FISHY Blog Post. https://fishy-project.eu/blog/reference-framework-fishy, retrieved 2022-12-29.

[24]Gonzalez L. F. , Vidal I., Valera F. and Lopez D. R. (2022), *Link Layer Connectivity as a Service for Ad-Hoc Microservice Platforms*, in IEEE Network, vol. 36, no. 1, pp. 10-17.

[25]Clegg D., Barker R. (1994). *Case Method Fast-Track: A RAD Approach*. Addison-Wesley.

[26]Espacenet: free access to over 140 million patent documents. https://worldwide.espacenet.com/?locale=en_EP, retrieved 2022-12-01.

[27]US9716595B1, *System and method from Internet of Things (IoT) security and management*, https://patents.google.com/patent/US9716595B1, retrieved 2022-12-01.

[28]US20220232040A1, *Advanced cybersecurity threat mitigation using software supply chain analysis*, https://patents.google.com/patent/US20220232040A1, retrieved 2022-12-01.

[29] ISO 28001:2007. Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance, https://www.iso.org/standard/45654.html, retrieved 2022-12-01.

[30]EUR-Lex Document 32019R1150. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150, retrieved 2022-12-01.

[31]REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=EN, retrieved 2022-12-01.

[32]DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN, retrieved 2022-12-01.

[33]Digital Single Market Strategy , Reference: TEN/574-EESC-2015-03604-00-01-AC-TRA. https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-single-market-strategy , retrieved 2022-12-01.

[34]Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876]. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876#english, retrieved 2022-12-01.

[35]Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies - 8 may 2014.https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654 , retrieved 2022-12-01.

[36]Vehicle Geo-Location and Employer-Employee Relations - 4 October 2011 [2444921].https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2444921, retrieved 2022-12-01.

[37]Decreto-Lei n.º 65/2021, de 30 de julho. https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988, retrieved 2022-12-01.

[38]Bundesdatenschutzgesetz (BDSG). https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html, retrieved 2022-12-01.

[39]Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1676566397110, retrieved 2022-12-01.

[40]Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1676566402279, retrieved 2022-12-01.

[41][FISHY] - *D4.4 Security and Certification IT2 integration,* Jorge Martinez, 2023 (to be submitted in M30).

[42]C Language Integrated Production System (CLIPS). https://clipsrules.net/?q=AboutCLIPS, retrieved 2023-01-10.

[43]Drools - Business Rules Management System (BRMS) solution. https://www.drools.org/, retrieved 2023-01-10.

[44]Bensalem M., Dizdarević J., Carpio F. and Jukan A. (2021), *The Role of Intent-Based Networking in ICT Supply Chains,* 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), pp. 1-6, doi: 10.1109/HPSR52026.2021.9481801.

[45]Bensalem M., Dizdarević J. and Jukan A. (2022), *Benchmarking Various ML Solutions in Complex Intent-Based Network Management Systems,* 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 476-481, doi: 10.23919/MIPRO55190.2022.9803584.

[46] Bensalem M. (2022), *Intent-based Resilience Orchestration in Supply Chains*. FISHY Blog. https://fishy-project.eu/blog/intent-based-resilience-orchestration-supply-chains, retrieved 2022-12-29.

[47] Lightweight data shippers. https://www.elastic.co/beats/, retrieved 2023-01-10.

[48]Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., López, D., Santos, H., Gonos, A., Silva, A., Soriano, J., Kalogiannis, G. (2021), *Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture*. *Sensors* 2021, *21*, 6057. https://doi.org/10.3390/s21186057

[49]Soriano J. , Jiménez G., Correa E. and Ruiz N. (2021), C*hallenges in the Automotive Software Supply Chain, Connected Car : Benefits from an Intent Policy framework*, 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), pp. 1-5, doi: 10.1109/HPSR52026.2021.9481853.

[50]Trakadas P. , Leligou H. C. , Karkazis P. , Gonos A. and Zahariadis T. (2021), *Farm to fork: securing a supply chain with direct impact on food security,* 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), pp. 1-6, doi: 10.1109/HPSR52026.2021.9481866.

[51]Silva A. M. and Duarte J. (2021), *The importance of security in the Industry 4.0 paradigm*. FISHY Blog. https://fishy-project.eu/blog/importance-security-industry-40-paradigm, retrieved 2022-12-29.

[52]Ruiz J. F. (2021), *FISHY: trustful and smart cybersecurity for supply chain*. FISHY Blog. https://fishy-project.eu/blog/fishy-trustful-and-smart-cybersecurity-supply-chain, retrieved 2022-12-29.

[53] Gonos A. and Leligou N. (2022), *Experiences from validation of FISHY in the Farm-to-Fork use case*. FISHY Blog. https://fishy-project.eu/blog/experiences-validation-fishy-farm-fork-use-case, retrieved 2022-12-29.

[54]Santos, H., Oliveira, A., Soares, L., Satis, A., and Santos, A. (2021), *Information Security Assessment and Certification within Supply Chains,* In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-6).

[55]Oliveira A and Santos H. (2021), *Continuous Industrial Sector Cybersecurity Assessment Paradigm: Proposed Model of Cybersecurity Certification,* 2022 18th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltrú, Spain, pp. 1-6, doi: 10.1109/DRCN53993.2022.9758022.