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

D2.3 Tracking external efforts technology evolution and business trends (II)

Document Identification			
Status	Final	**Due Date**	28/02/2022
Version	1.0	**Submission Date**	28/02/2022

Related WP	WP2	**Document Reference**	D2.3
Related Deliverable(s)	D2.1, D2.5, D2.6, D7.2, D7.5	**Dissemination Level (*)**	PU
Lead Participant	XLAB	**Lead Author**	Joao Pita Costa
Contributors	ATOS, TUBS, UPC, STS, ALTRAN, SYN, UMINHO, POLITO, TID, SONAE	**Reviewers**	Jasenka Dizdarevic (TUBS) Eva Marin Tordera (UPC)

Keywords:

Market activities, Business trends, Exploitable results, Science landscape, technological landscape, Competitors, Technological imperatives

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

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

Document Information

List of Contributors	
Name	Partner
Joao Pita Costa	XLAB
Lucija Korbar	XLAB
Aleš Černivec	XLAB
Anže Žitnik	XLAB
Jasenka Dizdarevic	TUBS
Mounir Bensalem	TUBS
Nelly Leligou	SYN
Antonio Alvarez Romero	ATOS
Rodrigo Diaz Rodriguez	ATOS
Jose Soriano Diaz	UMINHO
Henrique Santos	UMINHO
Ana Machado Silva	SONAE
Jose Duarte	SONAE
Guillermo Jimenez Preto	ALTRAN
Antonio Pastor	TID
Diego R. Lopez	TID
Ignazio Pedone	POLITO
Cataldo Basile	POLITO
Leonardo Regano	POLITO
Eva Marín Tordera	UPC
Sergi Sánchez	UPC
Kalogiannis Grigorios	STS

Document History			
Version	Date	Change editors	Changes
0.1	2021-12-09	Joao Pita Costa, XLAB	ToC and initial structure
0.2	2021-12-23	Joao Pita Costa, XLAB	Updated sections with KERs
0.3	2022-01-04	Joao Pita Costa, XLAB	Updated section on Market Assessment
0.4	2022-01-10	Joao Pita Costa, XLAB	Added section of legal and regulatory landscape
0.5	2022-01-22	Joao Pita Costa, XLAB	Added section 6 on technological imperatives, progress on the market

		Jasenka Dizdarevic, TUBS José Duarte, SONAE Araceli Rojas Morgan, CAPGEMINI Nelly Leligou, SYN	assessment in section 4, and added initial content on the FISHY research landscape
0.6	2022-01-27	Joao Pita Costa, XLAB	Added executive summary, conclusion section, formatted references and closed sections 1 (introduction), 2 (KERs) and 4 (market assessment update).
0.7	2022-02-01	Joao Pita Costa, XLAB Jasenka Dizdarevic, TUBS Antonio Pastor, TID Rodrigo Diaz Rodriguez, ATOS	TUBS added content to Section 3 and XLAB finalised Section 4. TID's revision of the Section 5.
0.8	2022-02-15	Joao Pita Costa, XLAB Jasenka Dizdarevic, TUBS José Duarte, SONAE Guillermo Jimenez Preto, CAPGEMINI Nelly Leligou, SYN	Final version ready for internal review, with concluded Sections 3 (TUBS) and 6 (XLAB).
0.9	2022-02-22	Jasenka Dizdarevic, TUBS Eva Marin Tordera, UPC	Internal review process finished and requests addressed.
0.9b	2022-02-22	Juan Alonso (ATOS)	Quality assessment
1.0	2022-02-28	Antonio Alvarez Romero, ATOS	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Joao Pita Costa (XLAB)	15/02/2022
Quality manager	Alonso, Juan Andres (ATOS)	24/02/2022
Project Coordinator	Romero, Antonio Alvarez (ATOS)	28/02/2022

Table of Contents

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
BOE	Boletin Oficial del Estado
DoA	Description of Action
EC	European Commission
EDA	Exploitation Domains of Action
EDC	Enforcement & Dynamic Configuration
EIM	Exploitation and Innovation Manager
ER	Exploitable Result
EPO	European Patent Office
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HPC	High Performance Computing
IDS	Intrusion Detection System
IGT	Impact Generation Team
IRO	Intent-based Resilience Orchestration
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KER	Key Exploitable Results
NFV	Network Function Virtualisation
NGFW	Next Generation firewall
NIDS	Network-based Intrusion Detection System
SACM	Security Assurance & Certification Manager
SDN	Software Defined Networking
SEM	Security Event Management
SIEM	Security Information and Event Management
SIA	Secure Infrastructure Abstraction
SIM	Security Information Management

Abbreviation / acronym	**Description**
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SPI	Security & Privacy Dataspace Infrastructure
UDP	User Datagram Protocol
UTM	Unified Threat Management
TCO	Total Cost of Ownership
TCP	Transfer Control Protocol
TIM	Trust & Incident Manager

Executive Summary

Following the rapid changes in the cybersecurity landscape in what respects the important role that supply chains have taken in the most recent cyberattack reports, the second iteration of the FISHY Radar is focusing on the overview of existing technologies and research challenges related to it. In that, it explores the overlaps with the functionalities offered by FISHY, and the research pathways that are being followed in the context of this project. Moreover, the FISHY Radar also elaborates further on the technological imperatives driven by the three use cases in the project, feeding on the collected requirements, current technological developments and final definition of Key Exploitable Results (KERs). Furthermore, we investigate the legal and regulatory landscape that relates to the scope of FISHY, has a European/international, national and regional range, and is based on the experience of the consortium partners. This final report on the FISHY Radar shall guide the further requirement collection, technological development and exploitation activities in the project.

1 Introduction

The objective of this document is to update the tracked external efforts, analysing the scientific and technological landscape centred on research challenges and available solutions in the market that relate to FISHY. The update to business trends is now done in the wider scope of supply chain resilience. The document relates to the scope of the work package helping build the definition of a FISHY architecture for resilient provisioning within supply chains by offering evidence and clarification on what the latter can be based on.

The document reports on the second iteration of the FISHY Radar, existing as a live document promoting the interaction of the consortium in this activity, the appropriate usage of the business intelligence generated, and serving as a basis to communication of new findings. It was extended to include: (i) new research challenges related to the ongoing research activity within the project; (ii) an updated coverage of existing solutions intersecting the FISHY functionality; (iii) the elaborated technological imperatives driven by the FISHY early technology adopters, the use cases; and (iv) the legal and regulatory landscape affecting the FISHY solution at global and local level.

The work presented builds on the know-how developed in the first iteration of the FISHY Radar as published in the deliverable D2.1[31], but also on the exploitation achievements that followed those results, and the analysis of requirements that complement this work and will follow this new iteration. Also, the progress of the impact generation within WP7 and, in particular, the exploitation activities, will build on the achievements reported in this document.

1.1 Relation to other project tasks

This document provides an update in M18 for the relevant scientific, technology and business trends feeding the effort in WP2 (specifications, architecture, use cases), WP6 (PoC Deployment and validation/demonstration strategy). It is the part of the task T2.1 "Research and technology radar, and business models" in the work package "Technology Radar, Business Models, Requirements and Architecture". Together with the architecture design from task T2.3, the outcome of this task will be a set of technological imperatives that service providers will be required to consider, and eventually will deploy and benefit from in the proposed FISHY architecture. The output of this task will help evaluating FISHY use cases (WP6) with respect to their business potential, such that the most viable directions for exploitation can be explored in the context of WP7. Moreover, requirements stemming from the legal and regulatory landscape (e.g., applicable Service Level Agreements, GDPR) will be also considered (relation to WP2). Therefore, the content of this document is closely coupled with the work done within work packages 2, 6 and 7 of the project.

1.2 Structure of the document

This document is structured in 6 major sections. Section 1 is introducing the content of this deliverable putting the work in the context of the other tasks and objectives in the FISHY project. The following section is presenting the update to the exploitable results' distribution throughout domains of action and the definition of Key Exploitable Results (KERs) that drive the further achievements of the Task 2.1 as reported in this document. This is followed by the exposition of the key research challenges addressed in FISHY, updating the science, research and technology landscape published earlier in D2.5[33]. The Section 4 will then focus on the market assessment through the angle of the FISHY end-to-end solution in the context of supply-chain resilience. That is followed by an assessment to the legal and regulatory landscape that relates to FISHY, affecting partner countries over own legislation and based on European Commission directives and initiatives. Finally, Section 6 updates on the technological imperatives in the context of FISHY's use cases and scaling to other potential targets. The document concludes with Section 7 where the future work and the challenges are presented.

1.3 Glossary adopted in this document

The most important terms used in this document and their explanation are listed below.

- **Business Model**. The rationale of a company to generate, deliver and capture value out of their commercial offering and their business relationships.
- **Domain of action.** This is the domain targeted by partners responsible for the KERs.
- **Feature comparison.** The analysis of the competitors based on the comparison with their features and the value they can generate.
- **Key Exploitable Results (KER or plural KERs).** These are the results implying business potential from the technology partners in the project.
- **Legal and Regulatory Landscape.** The legislation basis in relation to the scope of FISHY affecting at international, national and regional levels.
- **Market growth.** The volume and potential of a specific market in the context of the industry and audience it is addressing.
- **Market radar**. Continuous monitoring of relative positioning of the top software vendors within a specific market or niche (or domain of action).
- **Market trend**. The tendencies and dynamics of the market resulting into the attractiveness of the it and what it relates to.
- **Technological imperatives.** The technologies that translate the necessities to be addressed in a specific industry.

2 Key Exploitable Results

In the following section, we update the information of the project's exploitable results, building on what was published in the deliverables D2.5[33], D7.2[34] and D7.3[35], and from that provide a preliminary description of the defined Key Exploitable Results that drive the study and results presented in this deliverable. In Figure 1, we recall and update the exploitable results defined within FISHY exploitation, with the 14 domains of action that they define. The most relevant update was that of moving the *Intent-based resilience orchestrator (IRO)* led by TUBS to the core FISHY technologies section defining its own *Resilience Orchestration* domain of action. For completeness we present below a summary of the analysis of the IRO following the same structure used for presenting presented to other domains of action in the initial FISHY Radar report in the deliverable D2.1[31] earlier published in M6.

- **Problem:** The advances in network infrastructures have driven the development of new network applications that expect specific capabilities from the network. Capabilities may include constraints on traditional network metrics such as delay, minimum bandwidth, jitter, high-level requirements in terms of availability and service downtimes, as well as specialized requirements such as encryption of data along the service path. To achieve a specific objective, the network operator must make sure that related operations are executed, which can become a cumbersome and error-prone manual process.
- **Solution:** 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 fulfil a request. With the use of intents, the applications can treat the underlying network technology as a black-box.

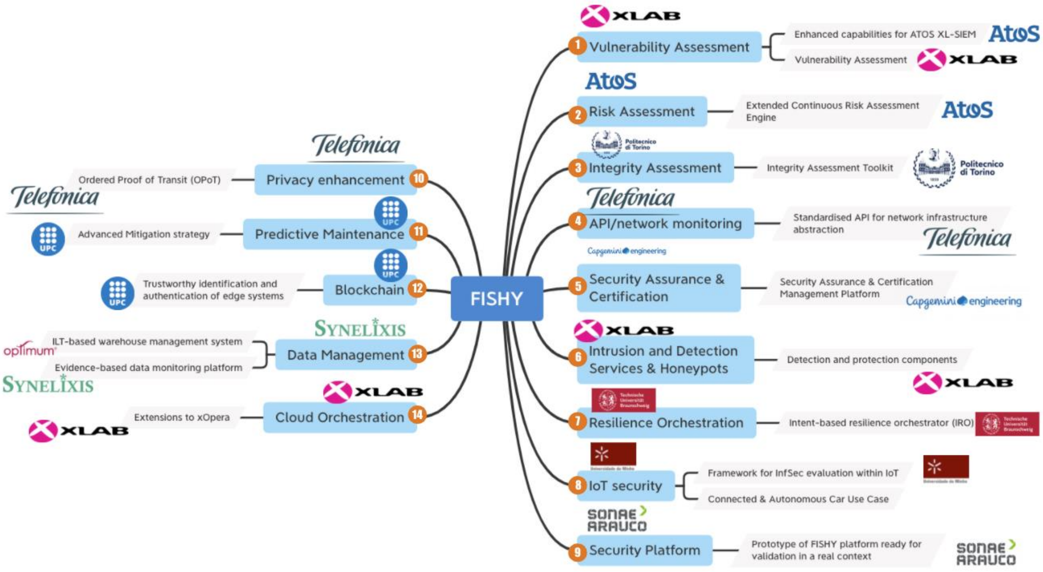
FISHY
1 Vulnerability Assessment
Enhanced capabilities for ATOS XL-SIEM
Vulnerability Assessment
2 Risk Assessment
Extended Continuous Risk Assessment Engine
3 Integrity Assessment
Integrity Assessment Toolkit
4 API/network monitoring
Standardised API for network infrastructure abstraction
5 Security Assurance & Certification
Security Assurance & Certification Management Platform
6 Intrusion and Detection Services & Honeypots
Detection and protection components
7 Resilience Orchestration
Intent-based resilience orchestrator (IRO)
8 IoT security
Framework for InfSec evaluation within IoT
Connected & Autonomous Car Use Case
9 Security Platform
Prototype of FISHY platform ready for validation in a real context
10 Privacy enhancement
Ordered Proof of Transit (OPoT)
11 Predictive Maintenance
Advanced Mitigation strategy
12 Blockchain
Trustworthy identification and authentication of edge systems
13 Data Management
ILT-based warehouse management system
Evidence-based data monitoring platform
14 Cloud Orchestration
Extensions to xOpera

Figure 1 - Exploitable Results (ERs) defining domains of action, and their assigned lead partners

Building from these declared expected exploitable results and corresponding domains of action (earlier described in deliverable D2.1[31] here added by the Resilience Orchestration), we have defined FISHY's Key Exploitable Results that determine the main technological components of the FISHY solution, starting from its backbone *FISHY Platform* and following in close relation to the defined architecture, functionality and user requirements (see Figure 2). The following description closely define each of these KERs that will drive the other aspects of the FISHY Radar.

- KER 1. FISHY Platform: Easing FISHY platform usability, making the whole system user-friendly and ready to be used for different users according to their expected profile and thus permitted functionalities
- KER2. Trust & Incident Manager (TIM): Monitoring and gathering metrics from supply chain infrastructure, performing analysis, raising alerts, proposing mitigation actions
- KER3. Intent-based Resilience Orchestration (IRO): Automation of the interactions between the user defining high level intents and the system applying high level policies
- KER4. Security Assurance & Certification Manager (SACM): Collecting certifiable evidence from the pilots infrastructure, and auditing/reasoning security metrics tailored to the pilots infrastructure
- KER5. Security & Privacy Dataspace Infrastructure (SPI): Organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management
- KER6. Enforcement & Dynamic Configuration (EDC): Translation of high-level policies into low-level configurations for a variety of NSFs (security controls)
- KER7. Secure Infrastructure Abstraction (SIA): Model-based support for data aggregation and preprocessing: normalization, filtering, etc.

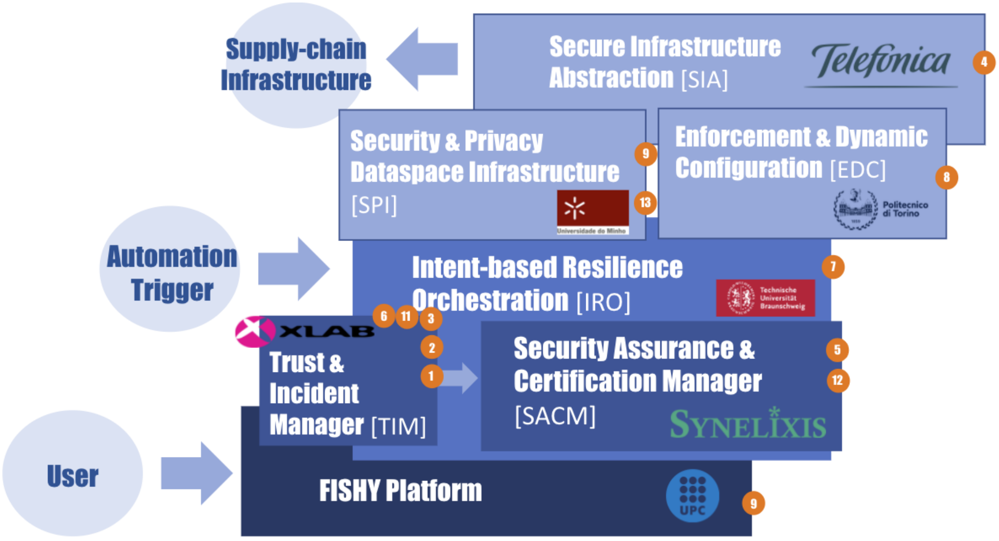
Supply-chain Infrastructure
Secure Infrastructure Abstraction [SIA]
Telefónica
4
Security & Privacy Dataspace Infrastructure [SPI]
9
13
Universidade do Minho
Enforcement & Dynamic Configuration [EDC]
8
Politecnico di Torino
Automation Trigger
Intent-based Resilience Orchestration [IRO]
7
Technische Universität Braunschweig
6
11
3
XLAB
Trust & Incident Manager [TIM]
2
1
Security Assurance & Certification Manager [SACM]
5
12
SYNELIXIS
User
FISHY Platform
UPC
9

Figure 2 - Key Exploitable Results (KERs) in relation to domains of action and their assigned lead partners

3 Research Landscape Update

3.1 Research Challenges

In this section, we give an overview of the research trends and challenges significant for FISHY. We extend the work from the previous deliverable D2.1[31] submitted in M6, which primarily focused on the research in prioritized domains of action, with recent trends or changes. It should be noted that many trends that were relevant at the time of the submission of the deliverable D2.1[31] remain the same (for further details about a recurrent research trend refer to the previous deliverable D2.1[31]). Moreover, in this deliverable we extend past previously defined domains of actions and include research trends in the areas of intent based resilience orchestration, blockchain and IoT security relevant to cyber resilience provisioning in ICT supply chains.

3.1.1 Intent based resilience orchestration

As one of the focus trend for FISHY, intent based resilience orchestration leverages work done in the new emerging networking trend - intent based networking (IBN) in order to advance network automation, orchestration and control functionalities [1]. From FISHY perspective, the main goal in this area is to integrate of AI/ML techniques with resilience orchestration and allow for automation of the interactions between the user, which will be defining high level intents and the system, which will be applying high level policies [2]. However, there are still multiple challenges in this area identified by the researchers, that need to be addressed, such as specification and description of the intents, integration of AI/ML techniques, privacy of user intents and choice of data modelling language [3][4].

The issue of how to actually specify intents has been one of the crucial issues with a lack of standardized solutions [2]. There have been ongoing efforts in advancing the manner of describing the intents to be both human-readable and machine understandable. Some of the approaches include utilization of pure unrestricted language, restricted vocabulary or ontology. In FISHY platform, for IRO component we have opted for utilization of natural language processing (NLP) techniques for translating high level policies into a structured format of an intent, using controlled natural language (CNL) to define a specific intents grammar, which will make the intents easier understandable for the machines. Another current issue is the choice of adequate data modelling language for the intent based orchestration, as this provides a way of describing the orchestration process itself, and device level requirements necessary for the implementation. The currently most studied approaches include YANG [5] and TOSCA [6] based models.

As of the most important benefits of the envisioned intent base orchestration is its autonomous behaviour enabled through different AI/ML techniques the challenge that has to be addressed for the successful integration of these techniques is the identified lack of studies on the utilization of learning based problems [5].

3.1.2 Security in IoT

While the trends in the IoT security area reported in D2.1[31], Section 3.2.4 regarding secure IoT architecture designs, deep learning based intrusion detection systems, vulnerabilities and attacks on IoT wireless technologies, and communication aspect (protocols) of IoT cybersecurity frameworks are still valid, attention is also being paid to the IoT security configurations. This new research trend proposes translation of IoT device configurations (such as security configurations) using intent based policy translation, which would enable IoT users without expertise in IoT environments to efficiently configure their IoT devices regardless of adopted platforms [7]. Combining this trend with FISHY's intent based orchestration (which uses AI/ML techniques) would allow for automatic mapping of high-level intents into low-level device configurations.

3.1.3 Blockchain

Using blockchain technology in a complete ICT supply chain operation is impractical due to its high requirements on processing and storage resources. But even with its partial implementation, the benefits for supply chain management regarding transparency, trustworthiness, traceability and efficiency are expected to be high [8]. Some of the research trends in investigating the potential of blockchain, that are to be leveraged for the utilization in trusted supply chains of ICT systems, include preserving the privacy of shared information, securing the data sharing, and interoperability between heterogeneous systems [8]. These efforts in preserving privacy of shared data are focused on ensuring privacy and traceability of the information exchanged through blockchain. These solutions as can be seen in [9], are based on distributed ledger technology (DLT), and can be integrated with the use of special tags (RFID, NFC and QR codes) for product tracing during supply chain lifecycle. Various efforts have also been reported in using blockchain technology for securing data between supply chain entities. These solutions often rely on storing collected network data by smart contracts and can provide a secure exchange of data through configuration of access policies to the smart contract, so only the authorized SC entities can execute smart contracts and see transaction details [10].

One of more interesting use case for blockchain can be found in IoT paradigm and its application in ICT supply chain devices, where it can contribute to data security and integrity, ensuring the handling of sensitive data. Such examples of analyzing integration of blockchain technology for the IoT environment are demonstrated in [11]. However, this adaptation of blockchain comes with challenges, due to the traditional blockchain techniques requiring high resource usage (and IoT devices being traditionally resource constrained), resulting in scalability and latency issues. In [12] the authors proposed an architecture to handle these blockchains' limitations by using the concept of Cluster Heads (CHs) in the IoT environment. In [13] blockchain is used for decentralized access to IoT data, using edge nodes to perform cryptographic computations and data collection. But to ensure lightweightness of the authentication process, they proposed to use certificateless cryptography. Other open challenges for the utilization of blockchain as the emerging technology for tackling ICT supply chains management and security issues, which also stem from the current cryptographic algorithms used, are related to the integrity of handling personal data [14].

3.2 Related technologies and projects

In this section we will address several technology trends in different areas which are relevant to FISHY, highlighting any new ones that might have been getting more attention lately. In addition, we will extend on the overview of EC-funded and national projects that relate to FISHY concepts, reported in D2.1[31], highlighting the new projects that can benefit FISHY, and as such should be leveraged. As with research trends, it is important to note that a detailed overview of both technological trends and related projects of interest has been presented in D2.1[31] (M6), and most of this information remains relevant.

Aligned with what has been reported in D2.1[31], there have been new developments concerning technologies developed to provide IoT Cybersecurity, such as OpenID Connect[1] based authentication processes, where the specification has been extended with the concept of so-called Self-Issued OpenID

[1] https://openid.net/connect/

Provider. This will allow a decentralized identification, with OpenID Providers in End-User's local control, allowing them to authenticate themselves, rather than to relying on third-party providers.

Regarding additional EU projects since the last report, that could enhance the further development of FISHY related technologies we identified 4 ongoing projects in the areas of risk assessment and orchestration and management of future networks with relevant use cases in security:

- SPIDER (a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services) [15] project aims to deliver a next generation 5G cyber-range platform that extends and combines the capabilities of existing testbeds and cyber ranges into a unified facility with the final objective of training cybersecurity professionals to be prepared for future incidents in this new environment. All data captured in this virtual environment will be analysed in real-time to predict the evolution of the attack and its associated economic impact. For this purpose, innovative risk analysis methodologies and econometrics models will be developed in the project to help decision makers to take optimal investment decisions. Although the models developed in SPIDER will address the specific threats of 5G infrastructures, they may be of interest for FISHY since the telecommunication infrastructure is a core technology in any complex supply chain ICT system, and consequently, it is critical to understand the impact of potential threats affecting them to minimize the impact of cascading effects.
- ENSURESEC (End-to-end Security of the Digital Single Market’s E-commerce and Delivery Service Ecosystem) [16] project will integrate inductive and deductive tools and technologies to protect e-commerce operations. Combined human, cyber and physical risk scenarios will be continuously assessed aiming to identifying critical assets as well as its corresponding cascading effects. The risk models defined in ENSURESEC combining hybrid threats and analysing the links among them can be also an interesting input to consider in FISHY, since some of the potential threats affecting e-commerce infrastructure can be also included in the scope of the FISHY project.
- TERAFLOW (Secured Automatic traffic management for a Tera of SDN Flows) [17] is focused on creating a novel cloud-native SDN controller for Telecom Operators. This new SDN controller shall be able to integrate with current NFV and MEC frameworks as well as to provide revolutionary features for flow aggregation, management (service layer) and network equipment integration (infrastructure layer). One of the project objectives involves developing monitoring interfaces to provide telemetry to obtain data for detecting attacks. Carrier-grade telemetry interfaces and specifications are relevant for 5G related scenarios in FISHY.
- The HEXA-X [18] project ambition includes to develop key technology enablers in the areas of (i) new high frequencies radio access technologies, connected intelligence though AI-driven governance for future networks and (iii) 6G architectural enablers, with the objective to provide the global industry leadership for the B5G/6G era. Two essentials areas are security, and management and orchestration based on the application of data-driven and automation mechanisms to E2E management and orchestration.

4 Market Assessment Update

To better understand the market potential of the technology developed within FISHY and building on the market assessment published in D2.5[32] based on the defined exploitable results, we wide the scope of the assessment update and use the new KERs as drivers of this effort. In the following paragraphs, we will be elaborating on market trends and existing competitor solutions focusing the cybersecurity of supply chains, regarding target audiences and functionality. This will be used as input and further explored in the context of the exploitation of FISHY.

4.1 Trend Overview

The cybersecurity and resilience of supply chains have been a matter of worldwide attention in the recent past due to the cyberattacks that profit from the weak preparedness of the supply chains. The complexity of this problem also makes of it a difficult problem to address in full by existing technological solutions.

Cybersecurity Automation

Due to the early stage of the digital transformation of most industries, the complexity of supply chains is a bottleneck to their cybersecurity. The automation of processes can help the adoption of cybersecurity approaches in full, optimising resources but also protecting them better against threats. This allows them to develop new strategies, while letting the automation take care of minor tasks to be automatically completed by the system. Though, DevOps teams must have in mind the security from the design phase and not as an afterthought covering the complexity of the systems on an end-to-end basis. According to Digicert [19] the vulnerability that led to the data breach in SolarWinds was the incomplete implementation of code signing best practices. The weakness of security practices in DevOps is sometimes due to the shortcut of any steps delaying the CI/CD build and release to ensure them to be agile and to deliver on time. According to the Security Magazine [20], some of that weakness is also due to the slow progress of security capabilities of individuals and organizations, and the solutions made available for the supply chain industry, working on updating systems that have been in place for years. The update and upgrade of ICT systems in parallel to an appropriate security infrastructure is vital to the right protection of a supply chain. The relevance of this aspect is boosted by the coronavirus pandemic hit that push forward the remote work and, in particular, the access to remote machines to ensure workflows, even though the workforce gap was reaching 4 million according to the estimations of the (ISC)2 Cybersecurity Workforce Study [21]. These estimates suggest that solutions such as FISHY can help companies to relieve the workload of their existing staff. Automation solution can ensure that resources are better focused on protecting against new threats and developing new strategies, while leaving minor tasks to be automatically completed by the system.

IoT/Edge security

Building on the discussions published in the earlier deliverable D2.5[32] on the specific cybersecurity challenges in IoT, vulnerabilities are driven by the lack of well-established standards, infrequent interaction with human operators as often located in inaccessible locations, and the limited resources available, prioritising low power consumption. The specific security challenges in this IoT domain include both the implementation and assessment to the security controls, and to the efficiency of those. The proliferation of IoT devices continues at an exponential rate, with the number of connected devices expected to grow from 13.8 billion units in 2021 to 30.9 billion by 2025. Though, most of the existing devices were not architected with a particular focus on security [22]. FISHY has a particular focus on the cybersecurity challenges driven by IoT, being aware of the importance of this ICT domain for the digital transformation of supply chains and to their nodes (e.g., the digital twin of a port allowing for the optimisation of operations also facilitating the ecologic transition, is based on IoT [23]). The attacks on IoT devices are rising at an alarming rate making 33% of the infected devices in the end of 2020 [24]. The changes brought by the popularisation of 5G ecosystems also open ample opportunities for malicious actions leveraging the vulnerability in IoT. According to the white paper of Schneider Electric [25], this common problem also in edge computing must be properly addressed by best practices that include a good selection criteria for used devices, the secure network design, the appropriate device configuration, and the efficient operation and maintenance having security in mind. According to PurpleSec's 2021 cybersecurity trends report [26], 63% of successful attacks originate from internal sources, either from control, errors or fraud.

Cloud security

The simplification of remote access and the growing need for better fit functionality within well-established technology is leading the decision of many companies to transfer their applications and services to the cloud. This implies the need for higher levels of protection, enhancing the cloud-based security that requires regular and extensive penetration tests, imperative to check the cloud solution for potential vulnerabilities. According to ENISA's report on supply chain attacks [27], 58% of the supply chain attacks aimed at gaining access to data, mostly aiming at customer data, including personal data and intellectual property. This is addressed by FISHY's Trust and Incidence Manager (TIM) that monitors and gathers metrics from the supply chain infrastructure, performing analysis, raising alerts, and proposing mitigation actions. Most of the innovation made available by FISHY is cloud-ready taking into consideration this upcoming market reality.

Data Protection

Given the growing degree of digitisation across companies, the responsibilities in the protection of the collected and stored data need to be properly addressed. This can be a challenge for small and medium-sized enterprises, and to research institutions developing technological solutions. Besides ensuring the best possible protection for the data, they also need to be familiar with the key data-protection requirements laid down in the EU GDPR. Larger companies may outsource that responsibility to an external advisory services or data protection officer. This is addressed by FISHY's Security & Privacy Dataspace Infrastructure (SPI) securing data transfer between the monitored infrastructure and the FISHY platform, with data anonymization, enforcing privacy and access Control rules, including Identity Management.

Compliance with Standards

The COVID-19 driven lockdowns and new local and global regulations impacted suppliers in their common workflows leading them to explore alternative strategies and to restructure existing processes. These circumstances are pressuring the supply chain industry into the digitalisation of a growing number of sub-processes, or even entire processes. As earlier discussed, the IoT-driven smart connectivity and remote control of a complex network of multiple devices is an important factor in the context of a cybersecurity vulnerability of the supply chain, also due to the lack of widely adopted standards. To ensure the protection of the supply chain dependent on these IoT devices against cyberattacks, their design, development and security need to be well standardised so that they can be tested and certified against objective criteria. The EU Cybersecurity Act [28] is an European Commission regulation initiative that came into effect in June 2019 to establish the regulatory framework for the EU-wide security certification of products, services and processes. This regulation ensures compliance of ICT products with standardised security requirements from the earliest stages of design and development as well as in production (promoting "security by design" and "security by default"). FISHY is addressing this with a comprehensive effort towards compliance but also contribution to standards.

5 Legal and regulatory landscape

In the following section we shall elaborate on the legislation and regulation affecting European countries in the context of FISHY activities. This survey has European, country and region-level granularity to provide a representation map for needed compliance, with input from the consortium partners and from the existing sources online.

5.1 Overview

Taking into account the activities of FISHY relating to security and privacy, particularly in relation to the overall European regulation overviewing the data-related aspects of the system (e.g. GDPR), and the complexity that a supply-chain ICT infrastructure can represent, it is pertinent to ensure compliance. Moreover, the specifics of local regulation and legislation, either at a national, regional or municipality granularity, can further endure the compliance to a level that can be secured. The proof of well addressed supply chain security is becoming a de facto standard for doing business in most industry sectors as, e.g., telecommunications, critical infrastructure, aerospace and defense [29].

According to the data collected by the FISHY WP7 team, the regulator being the EC for the range of European Union, the regulation considered mostly regards aspects of the data protection legislation (including GDPR) and the national interpretations of this (see #3, #4, #11 and #13 below). This EU-wide regulation also regards the promoting fairness and transparency for business users of online intermediation services. Other EU-wide regulation is specified by the agency ENISA regarding the open internet regulation, or the Directive 2016/1148 of the European Parliament and the Council, that defines minimum security controls for information and network security across the EU (it is a Directive, but several countries already adopted it to national laws). Moreover, at a wider international context, we also consider ISO 9001 focusing the quality management system, and ISO 27001, focusing the information security management, both of which regulated by ISO.

According to our study, in the national context, the legal and regulatory landscape has a much more specific impact, mostly being regulated by the state and with a noticeable lower impact to FISHY. The latter includes legislation affecting the provision of electronic communications networks and the implementation of electronic communications services, the security of networks and information systems and the security documentation and security measures, and regulating criminal offences. It also regulates services and contracting through electronic means and the security of information systems, and the measures for the protection of public critical infrastructure and the framework for that protection.

5.2 Landscape

In the following we expand on the legislation and regulation identified by the FISHY consortium with a local (regional/national) or global range that is estimated to impact FISHY in regards to its domains of action, and are to be taken into consideration. Each of the regulatory instances are referenced and have an indication of low, medium and high impact on FISHY.

5.2.1 International and EU-wide Regulations

The General Data Protection Regulation (GDPR)[2]

Regulator: EC / Region: EU / Reference: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Impact on FISHY: High - GDPR requirements

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This text includes the corrigendum published in the OJEU of 23 May 2018. The regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens.

Regulation (EU) 2018/1807 of the European parliament and of the council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union[3]

Regulator: EC / Region: EU / Reference: N/A

Impact on FISHY: Low

The purpose of this Regulation is to ensure the free movement within the European Union of data which are not of personal nature by laying down rules on the requirements for data localization requirements, availability of data for public administrations and data portability for professional users.

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[4]

Regulator: EC / Region: EU / Reference: N/A

Impact on FISHY: Low

The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down rules to ensure that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities.

ISO 9001 quality management system[5]

Regulator: ISO / Region: International / Reference: N/A

Impact on FISHY: Low

This regulation focus the quality management of a system.

ISO 27001 Information security management [6]

Regulator: ISO / Region: International / Reference: N/A

Impact on FISHY: Low

This regulation focus the security management of a system.

Open Internet Regulation (Regulation (EU) 2015/2120)[7]

Regulator: EC / Region: EU / Reference: ENISA [30]

Impact on FISHY: Low

[2] https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02016R0679-20160504&qid=1532348683434

[3] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=EN

[4] URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1150&from=EN

[5] https://www.iso.org/iso-9001-quality-management.html

[6] https://www.iso.org/isoiec-27001-information-security.html

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=EN

Apply to internet service providers, and specifically to Net neutrality. Article 3.3 defined cybersecurity and safety as a valid exception to alter the neutrality.

5.2.2 National Regulations

Legislation: Electronic Communications Act (ZEKom-1)[8]

Regulator: State / Region: Slovenia

Impact on FISHY: Low Impact

This law regulates the conditions for the provision of electronic communications networks and the implementation of electronic communications services, ensuring universal service, ensuring competition, the management of the radio frequency spectrum and numbering resources is governed by more efficient construction and installation of electronic communications networks and sharing of existing physical infrastructure, lays down the conditions for the restriction of property rights, determines the rights of users, regulates the security of networks and services and their operation in exceptional situations, ensures the exercise and regulates the protection of the right to communication privacy of users of public communication services, regulates the resolution of disputes in the field of this Act, regulates the competencies, organization and operation of the Agency for Communication Networks and Services of the Republic of Slovenia (hereinafter: the Agency) as an independent regulatory body and the competencies of other bodies performing tasks under this Act and other issues related to electronic communications.

Legislation: Information Security Act (ZInfV)[9]

Regulator: State / Region: Slovenia / Reference: http://www.pisrs.si/

Impact on FISHY: Low Impact

This Act regulates the field of information security and measures to achieve a high level of security of networks and information systems in the Republic of Slovenia, which are essential for the smooth operation of the state in all security conditions and provide essential services for maintaining key social and economic activities in the Republic of Slovenia. It lays down minimum security requirements and incident reporting requirements for those liable for this Act. It also regulates the competences, tasks, organization and operation of the competent national information security authority (hereinafter: the competent national authority), single contact points for information security (hereinafter: single contact point), national security incident teams, electronic networks and information.

Personal Data Protection Act (ZVOP-1)[10]

Regulator: State / Region: Slovenia / Reference: Data protection officer's home page

Impact on FISHY: High Impact - national GDPR requirements

This Act determines the rights, obligations, principles and measures that prevent unconstitutional, illegal and unjustified encroachments on the privacy and dignity of an individual (hereinafter: individual) in the processing of personal data.

Draft version of Personal Data Protection Act (ZVOP-2)[11]

Regulator: State / Region: Slovenia / Reference: Data protection officer's home page

Impact on FISHY: High - national GDPR requirements

[8] https://www.gov.si/teme/informacijska-varnost/

[9] https://www.gov.si/teme/informacijska-varnost/

[10] http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906

[11] https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208

Implements GDPR directly into the state law. It will be a new version of national's Personal Data Protection Act.

Personal Data Protection Act in the field of dealing with criminal offenses (ZVOPOKD)[12]

Regulator: State / Region: Slovenia / Reference: www.pisrs.si

Impact on FISHY: Low - not in the context of FISY (mostly public services)

(1) This Act regulates the protection of personal data processed by the police, state prosecutor's offices, the Probation Administration of the Republic of Slovenia, the Administration of the Republic of Slovenia for the Execution of Criminal Sanctions and other state bodies of the Republic of Slovenia. The detection or prosecution of criminal offenses or the execution of criminal sanctions (hereinafter: the competent authorities) shall be processed for the purposes of the exercise of these powers.

(2) This Act also regulates when courts deciding in criminal matters apply the provisions of this Act on the processing and access to personal data in criminal matters.

(3) This Act also regulates the conditions for lawful and fair processing of personal data, procedures and methods of detecting and preventing illegal interference with the rights of an individual (hereinafter: individual) to whom personal data relate, methods of exercising his rights and transferring personal data to third countries and international organizations. In order to effectively protect the legality and fairness of the processing of personal data, it also regulates the supervisory powers and supervisory measures of the supervisory body and the liability for misdemeanours regarding their breaches.

Regulation on the definition of essential services and a more detailed methodology for determining the providers of essential services[13]

Regulator: State / Region: Slovenia / Reference: www.pisrs.si

Impact on FISHY: Low - aimed at essential services in the state of Slovenia

This Decree determines those services from the Decree on the Standard Classification of Activities (Official Gazette of the Republic of Slovenia, No. 69/07 and 17/08; hereinafter: SKD), which for the purposes of implementing the Information Security Act (Official Gazette of the Republic of Slovenia, No. 30) / 18, hereinafter: ZInfV) are considered essential, and the methodology for determining the providers of essential services (hereinafter: IBS), including the evaluation of cross-sectoral and sectoral factors.

Rules on security documentation and security measures for essential service providers[6]

Regulator: State / Region: Slovenia / Reference: www.pisrs.si

Impact on FISHY: Low - aimed at essential services in the state of Slovenia

These rules specify the content and structure of security documentation, the methodology for preparing risk management analysis and for determining key, control and monitoring information systems and parts of the network and related data and the minimum scope and content of security measures of essential service providers.

Decree on information security in state administration[14]

Regulator: State / Region: Slovenia / Reference: www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198

Impact on FISHY: Low - applies to state administration bodies

This Decree lays down minimum common requirements regarding information security, which include uniform frameworks for information security management and basic supervision for ensuring information security in the state administration, unless the Decree provides otherwise. This Decree

[12] https://www.gov.si/teme/informacijska-varnost/

[13] https://www.gov.si/teme/informacijska-varnost/

[14] https://www.gov.si/teme/informacijska-varnost/

applies to state administration bodies (hereinafter: the body). The Regulation also applies to other state bodies, local community bodies, public agencies and holders of public authority, as well as other entities that are connected to the central information and communication system (hereinafter: related entity).

BOE-A-2018-16673 The Organic Law 3/2018 of December 5 on Protection of Personal Data and Guarantee of Digital Rights[15]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: High - national GDPR requirements

LO3/2018 is the national law that adapts to the content of the RGPD.

Law 34/2002 of 11 July 2002 on information society services and electronic commerce[16]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

This Law governs the legal regime of information society services and contracting through electronic means, as regards the obligations of service providers, including those acting as intermediaries, those who act as intermediaries in the transmission of contents through telecommunication networks, commercial communications by electronic means, prior commercial communications by electronic means, the information to be provided when contracting electronically etc.

Royal Decree-Law 12/2018 of 7 September 2018 on the security of networks and information systems[17]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

The purpose of this Royal Decree-Law is to regulate the security of networks and information systems used for the provision of essential services and digital services, and to establish an incident notification system.

Measures for the protection of public critical infrastructure[18]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

The purpose of this Law is to establish the appropriate strategies and structures to direct and coordinate the actions of the different bodies of the Public Administrations with regard to the protection of critical infrastructures, after identifying and designating them, in order to improve the prevention, preparation and response of Spain to terrorist attacks or other threats affecting critical infrastructures. To this end, the collaboration and involvement of the managing bodies and owners of such infrastructures will also be promoted, in order to optimize their degree of protection against deliberate attacks of all kinds, with the aim of contributing to the protection of the population.

Framework of the protection of critical infrastructure[19]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

The purpose of this regulation is to develop the framework provided for in Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures, in order to specify the actions

[15] https://boe.es/buscar/act.php?id=BOE-A-2018-16673

[16] https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

[17] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

[18] https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

[19] https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

of the different bodies that make up the Critical Infrastructure Protection System (hereinafter, the System) as well as the different planning instruments of the System.

Measures of motivation by the Information Society[20]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

This law sets out a number of principles to encourage the use of electronic means when using and/or contracting different services.

Law 9/2014, of 9 May, General Telecommunications[21]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

This law governs the legal regime for the operation of electronic communications networks and the provision of electronic communications services.

Data protection of the electronic communication and public communication network[22]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

The purpose of this Law is to regulate the obligation of operators to keep the data generated or processed in the framework of the provision of electronic communications services or public communications networks, as well as the duty to transfer such data to the authorized agents whenever they are required to do so through the corresponding judicial authorization for the purpose of detection, investigation and prosecution of serious crimes contemplated in the Criminal Code or in special criminal laws.

BOE-A-2005-6970 Royal Decree 424/2005, of 15 April, approving the Regulation on the conditions for the provision of electronic communications services, universal service and user protection[23]

Regulator: State / Region: Spain / Reference: N/A

Impact on FISHY: Low

The purpose of this regulation is to govern the conditions for the provision of services or the operation of electronic communications networks, in development of the General Telecommunications Law.

Guidelines on the use of cookies and other tracking tools[24]

Regulator: State / 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.

Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies[25]

Regulator: State / 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.

[20] https://www.boe.es/buscar/act.php?id=BOE-A-2007-22440

[21] https://www.boe.es/buscar/pdf/2014/BOE-A-2014-4950-consolidado.pdf

[22] https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

[23] https://www.boe.es/buscar/act.php?id=BOE-A-2005-6970&p=20181229&tn=2

[24] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876#english

[25] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654

Vehicle Geo-Location and Employer-Employee Relations[26]

Regulator: State / Region: Italy / Reference: N/A

Impact on FISHY: Low

This regulation can have some impacts on the SADE use case.

Law 46/2018, of 13 August, legal framework for cyberspace security.[27]

Regulator: State / Region: Portugal / Reference: Law 46/2018

Impact on FISHY: Medium

Establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148, of the European Parliament and of the Council, of 6 July 2016, on security controls to ensure a high standard level of network and information security across the Union – obligatory for Critical Infrastructures and Public Administration.

Law 65/2021, of 30 July, Cyberspace Security Legal Regime.[28]

Regulator: State / Region: Portugal / Reference: Law 65/2021

Impact on FISHY: High

Regulates the Cyberspace Security Legal Regime and defines the obligations in terms of cybersecurity certification according to Regulation (EU) 2019/881 of the European Parliament, of 17 April 2019. It applies to Public Administration entities, Critical Infrastructure, Essential Service Operators and Digital Service Providers.

Resolution of the Council of Ministers n. 92/2019, of 5 June, National Cyberspace Security Strategy.[29]

Regulator: State / Region: Portugal / Reference: Resolution 92/2019

Impact on FISHY: Low

Council of Ministers Resolution that approved the first National Cyberspace Security Strategy to deepen the security of networks and information systems and promote a free, safe and efficient use of cyberspace by all citizens and public and private entities.

Law 58/2019, of 8 August, Personal Data Protection Law.[30]

Regulator: State / Region: Portugal / Reference: Law 58/2019

Impact on FISHY: Medium

Enforces the implementation, in the national legal system, of Regulation (EU) 2016/679 of the Parliament and the Council, of 27 April 2016, on the protection of individuals concerning the processing of personal data and the free movement of such data.

[26] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2444921

[27] https://dre.pt/dre/detalhe/lei/46-2018-116029384

[28] https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988

[29] https://dre.pt/application/file/a/122498847

[30] https://dre.pt/dre/detalhe/lei/58-2019-123815982

6 Technological imperatives

6.1 Overall technological imperatives

The following is building on the work presented in the earlier published D2.1[31], where we have described per use case the early request of features needed in FISHY and the existing technologies in the workflow of the use cases that can compete with the KERs offered by the projects outcomes. To further understand the analysis of technological imperatives in the context of the FISHY workflow, we turn to the complementary effort on the first iteration on constrains and requirements as published in the Section 3 of D2.2[32] based on the input from the FISHY use cases.

To this aim we have surveyed FISHY's use cases based on their contributions to the first iteration on technological imperatives as published in D2.5[33], and on the following questions:

- What are the alternative technologies used and what are they used for?
- Any in-house developed solutions?
- Any planned sw/hw acquisitions? Any tools you must have to improve the cybersecurity of your supply-chain?
- What dependencies need to be taken into consideration?
- What is the regulation/legislation you must comply with?

Moreover, guided by the newly defined KERs, we have explored the functionality required of each KER by each use case in FISHY, to settle KER aims and target that will be addressed in the following exploitation reports within the impact generation deliverables D7.3[35] and D7.4[36]. This is part of the lean exploitation strategy that interacts with the FISHY early adopters (i.e., the use cases) to understand how does FISHY impact their market positioning, product efficiency/capability and business opportunities. This will then allow us to scale the application of FISHY using the use cases as references. It is worth to mention, that FISHY may be customizable for each current, and for future use cases; allowing to implement the required functionalities, and their corresponding KERs. For sake of demonstration, the three use case in the project will implement all the functionalities required for each KER.

The analysis has shown that the existing technologies with cybersecurity functionality are part of other more general solutions (e.g. Microsoft Connected Factories in one of the use cases, which can also be used to feed data to FISHY workflow) that can complement the functionality of FISHY and do not represent a competition per se. As briefly discussed in the Section 4 above, there is great value on the interaction between FISHY and the solutions already integrated in the workflows on the customer side, throughout the nodes of the supply chain. The difficulty to substitute functioning technology in production was earlier pointed out by the EAB, and the modularity inherent to the architecture and the joint exploitation model in FISHY is addressing this.

Moreover, the use cases do not have in-house technologies to be considered, and the digital transformation across industries reduces those occurrences due to the multiplicity of existing solutions (some of which with enough customisation potential) that are cheaper than to make your own from scratch. Though, this is always a case to be considered due to the technical challenges in integration it can raise. The regulation and legislation affecting the use cases is included in our analysis in Section 5, showing the good coverage of that investigation but also the loose local and global regulation and standards in the supply chain sector, to which also FISHY is actively contributing.

7 Conclusions & Future Work

This final report on the FISHY Radar is describing the second iteration regarding the related activities, building on the business intelligence collected in the first iteration reported in the deliverable D2.1[31] that included the overview of research and technology, the market assessment that helped build the first exploitation strategy (as reported in the deliverable D7.2[34]). This work was guided by the initial exploitable results and respective domains of action, and was now steered towards the final FISHY KERs recently established. The second iteration of the FISHY Radar updates the existing live document to add new knowledge on the current research on Intent-based resilience, security in IoT and the meaningful application of blockchain technologies. This can guide the further research in the context of this project, serving as a new iteration of the scientific review of the highlighted research topics. Moreover, the update to the market assessment focusing on the analysis of technological solutions that cover the functionality of some of the FISHY KERs, expands the initial work on the first iteration to have a wider perspective on what are the main market trends and industry problems most addressed by the companies focusing on supply chain cybersecurity and resilience. In this context, we expand our perspective based on the most recent reports including those problems in industry, and the partial coverage of available solutions in the market, noticing the difficulty to cover the full range of functionalities offered by FISHY, and the current vendor-lock that can relate to the lack of open source tools in this technological landscape.

The further analysis of the technological imperatives from the existing reports, and the interviews and surveys to the FISHY use cases, show that most rely on limited functionality of supply chain tools and show interest in acquiring focused solutions that can better fit the complexity of their operations. This is complemented by the analysis to the regulations and legislation affecting the consortium partners in the scope of FISHY, from an European (and international) to a national (and even regional) range. As expected, the GDPR and its national implementation takes an important role in the landscape, but the legislation regarding the security of telecommunications and critical infrastructure is also highly relevant and to be taken into consideration. We have not identified specific legislation directly related to the cybersecurity of supply-chains, maybe due to the novelty of the global threat.

The progress of this work shall relate to the iterations within WP2 regarding the further requirement analysis and to the overall technological development. Moreover, the exploitation activities in WP7 will build on the findings reported in this deliverable to further the product development and business plans towards a well-established impact generation strategy.

8 References

[1] A. Clemm and e. al (2019) *Intent-based networking-concepts and overview*, Internet Engineering Task Force, Internet-Draft.

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

[3] M. Mehmood, K. Kralevska and D. Palma (2021) *Intent-driven Autonomous Network and Service Management in Future Networks: A Structured Literature Review*, arXiv, no. arXiv:2108.04560.

[4] E. Zeydan and Y. Turk (2020) *Recent Advances in Intent-Based Networking: A Survey*, IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 1-5.

[5] T. Zhou, S. Liu, Y. Xia and S. Jiang, *Yang data models for intent-based network model* [Online]. Available: https://datatracker.ietf.org/doc/html/draft-zhounetmod-intent-nemo-00, retrieved 19 1 2022.

[6] P. Lipton, C. Lauwers, M. Rutkowski, C. Noshpitz and C. Curescu (2020) *Tosca simple profile in yaml version 1.3.* [Online]. Available: https://docs.oasis-open.org/tosca/TOSCASimple-Profile-YAML/v1.3/os/TOSCA-Simple-ProfileYAML-v1.3-os.html, retrieved 19 1 2022.

[7] C. Chung and J. P. Jeong (2020) *A Design of IoT Device Configuration Translator for Intent-Based IoT-Cloud Services*, 22nd International Conference on Advanced Communication Technology (ICACT), 52-56.

[8] S. Al-Farsi, M. M. Rathore and S. Bakiras (2021) *Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities*, Applied Sciences, 11(12), 5585.

[9] F. M. Benčić, P. Skočir and I. P. Žarko (2019) *DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management*, IEEE Access, 7, 46198-46209.

[10]Q. Wen, Y. Gao, Z. Chen and D. Wu (2019) *A Blockchain-based Data Sharing Scheme in The Supply Chain by IoT*, IEEE International Conference on Industrial Cyber Physical Systems (ICPS), 695-700.

[11]Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song and M. P. M. Zhou (2018) *Towards decentralized IoT security enhancement: A blockchain approach*, Computers & Electrical Engineering, 72, 266-273.

[12]A. Dorri, S. Kanhere and R. Jurdak (2017) *Towards an Optimized BlockChain for IoT*, IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI).

[13]R. Li, T. Song, B. Mei, H. Li, X. Cheng and L. Sun (2018) *Blockchain for large-scale internet of things data storage and protection*, IEEE Trans. Serv. Comput.

[14]W. Afrifah and e. al. (2022) *Barriers and opportunities in cyber risk and compliance management for data-driven supply chains*, in Hawaii International Conference on System Sciences.

[15]European Commission (2022) *SPIDER project* [Online]. Available: https://spider-h2020.eu/, retrieved 10 2 2022.

[16]European Commission (2022) *ENSURESEC* [Online]. Available: https://www.ensuresec.eu/, retrieved 10 2 2022.

[17]European Commission (2022) *TERAFLOW* [Online]. Available: https://www.teraflow-h2020.eu/, retrieved 31 1 2022.

[18]European Commission (2022) *HEXA-X* [Online]. Available: https://hexa-x.eu/, retrieved 31 1 2022.

[19]Digicert (2022) *Secure software close the loop* [Online]. Available: https://www.digicert.com/campaigns/secure-software-close-the-loop, retrieved 10 1 2022.

[20]M. Jones (2022) *Supply chain cybersecurity trends: What professionals should be aware of and how to prepare for 2022*. Security Magazine [Online]. Available: https://www.securitymagazine.com/articles/96304-supply-chain-cybersecurity-trends-what-professionals-should-be-aware-of-and-how-to-prepare-for-2022, retrieved 10 1 2022.

[21](ISC)^2 Cybersecurity Workforce (2019) *Strategies for Building and Growing Strong Cybersecurity Teams*, (ISC)^2.

[22]Global Banking & Finance (2021) *Cybersecurity trends 2022: Ransomware and supply chain attacks are major threats* [Online]. Available: https://www.globalbankingandfinance.com/cybersecurity-trends-2022-ransomware-and-supply-chain-attacks-are-major-threats/, retrieved 10 1 2022.

[23]Joao Pita Costa et al (2021) *Advantage of a Green and Smart Port of the Future*, WIT Transactions on The Built Environment, 204, 203-217.

[24]Nokia (2022) *Nokia Threat Intelligence Report warns of rising cyberattacks on internet-connected devices* [Online]. Available: https://www.nokia.com/about-us/news/releases/2020/10/22/nokia-threat-intelligence-report-warns-of-rising-cyberattacks-on-internet-connected-devices/, retrieved 10 1 2022.

[25]Schneider Electric (2021) *Schneider Electric White Paper: An Overview of Cybersecurity Best Practices for Edge Computing* [Online]. Available: https://go.schneider-electric.com/WW_202105_WP12-IT-PROFESSIONAL-An-Overview-of-Cybersecurity-Best-Practices-for-Edge-Computing_EA-LP.html, retrieved 10 1 2022.

[26]PurpleSec (2021) *PurpleSec's 2021 cybersecurity trends report* [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/, retrieved 10 1 2022.

[27]ENISA (2020) *ENISA threat landscape for supply chain attacks*, ENISA, 2020.

[28]European Commission (2021) *Cybersecurity Act, 11 8 2021*. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, retrieved 10 1 2022.

[29]R. Hu (2020) *Securing the supply chain*, 17 9 2020 [Online]. Available: https://www.accenture.com/us-en/insights/consulting/securing-the-supply-chain, retrieved 10 1 2022.

[30]ENISA (2018) *Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation*, 12 12 2018 [Online]. Available: https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation, retrieved 15 12 2021.

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

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

[33] [FISHY] - D2.5 Tracking external efforts, technology evolution and business trends – CO (I)

[34] [FISHY] - D7.2 Report on dissemination, standards and exploitation (Y1), Jose Manuel Manjón, 2021

[35] [FISHY] – D7.3 Report on dissemination, standards and exploitation (Y2)

[36] [FISHY] – D7.4 Report on dissemination, standards and exploitation (Y3)