



## The coordinated framework for cyber resilience provisioning guaranteeing trusted supply chains of ICT systems

<https://fishy-project.eu/>



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644

# What are our challenges

The unstoppable evolution of ICT systems, with innovative technologies and business models, is driving a massive digital transformation and the Industry 4.0 revolution. At the same time, the more dependable society on ICT systems, the more critical the effects of even minor ICT infrastructure disruption. Today, the resilience of ICT systems is premium, and every ICT system is expected to implement at least a set of basic mechanisms to prevent, resist, and recover from any type of disruption in a timely manner, thus minimizing the impact on service quality and user experience.

**Challenge 1:** Need for **end-to-end solutions** for **vulnerabilities** and **risks management**.

**Challenge 2:** Lack of evidence-based **metrics for security assurance** and **trust guarantees**.

**Challenge 3:** Cumbersome **coordination** in multi-actor and multi-vendor **supply chains** of **ICT systems**.

**Challenge 4:** **Static cybersecurity networked** configurations and **dynamic systems audit**.





**Challenge 5:** Unlikely wide adoption of integrated **cybersecurity** solutions for composed **ICT systems**.

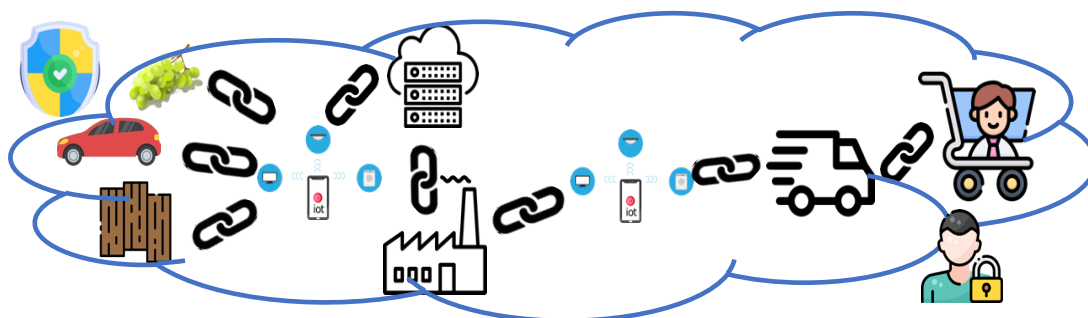
# How are we solving them

FISHY addresses these challenges by developing a **coordinated framework for cyber resilience provisioning** that guarantees a **trusted supply chain of ICT systems**, built upon distributed, dynamic, and often fundamentally insecure and heterogeneous ICT infrastructures.

The FISHY framework considers all the **supply chain** components, from the **IoT ecosystem** to the **infrastructure** connecting them, addressing **security and privacy** functionalities related to **risks** and **vulnerabilities** management, accountability, and **mitigation strategies** as well as **security metrics** and evidence-based **security assurance**

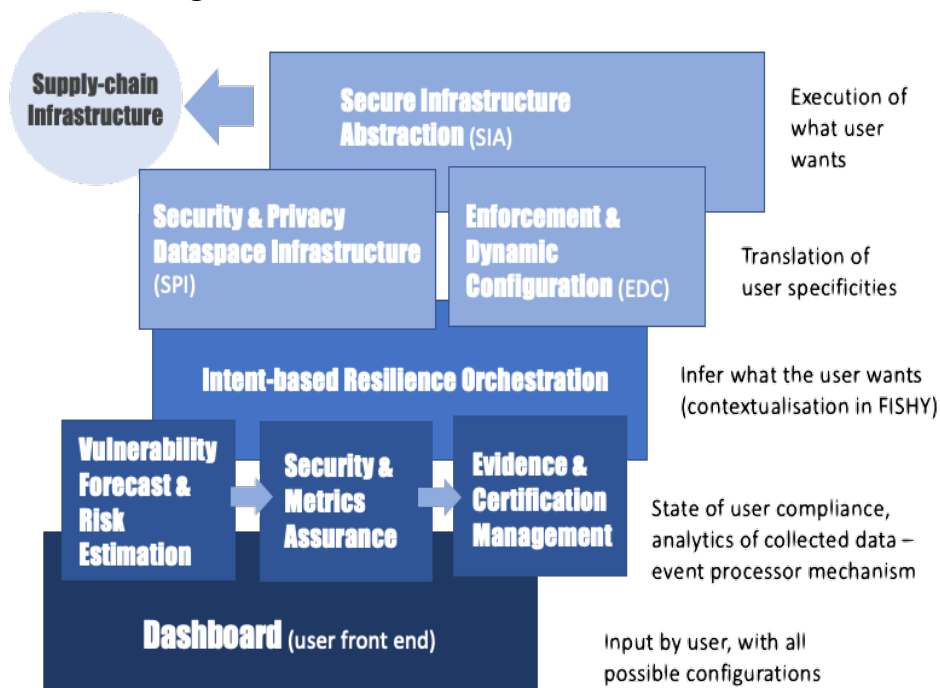
## We are helping industries:

-  Design and develop a functional platform for cyber resilience provisioning for supply chains of complex ICT systems, leveraging trust and security management.
-  Establish an evidence-based security assurance and certification methodology identifying security claims and metrics.
-  Develop a metrology model and system for ICT supply chains leveraging trust among parties relying on distributed interledger technologies as well as forecasting and estimation concepts based on artificial intelligence methods.
-  Deploy, validate and demonstrate the FISHY platform in heterogeneous, real-world pilots.



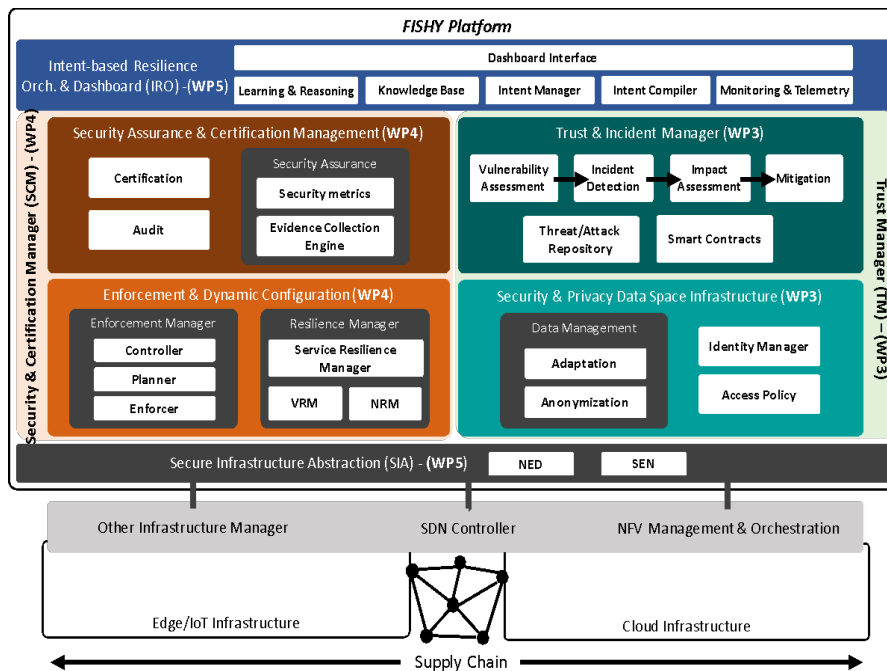
# FISHY concept

The FISHY coordinated cyber resilient platform provides the appropriate set of tools and methods towards establishing trusted supply chains of ICT systems through novel evidence-based security assurance methodologies and metrics as well as innovative strategies for risk estimation and vulnerabilities forecasting leveraging state-of-the-art solutions, leading to resilient complex ICT systems, comprising the complete supply chain, particularly focusing on the IoT devices at the edge and the network systems connecting them.



This end-to-end technology is covered by technological enablers and core technologies developed within FISHY, covering the following domains: Vulnerability Assessment; Risk Assessment, Privacy enhancement, Data Management, Data Quality Control, API/network monitoring API/network monitoring, Orchestration, Security Assesment, Data Quality Control, Security Platform.

# FISHY architecture



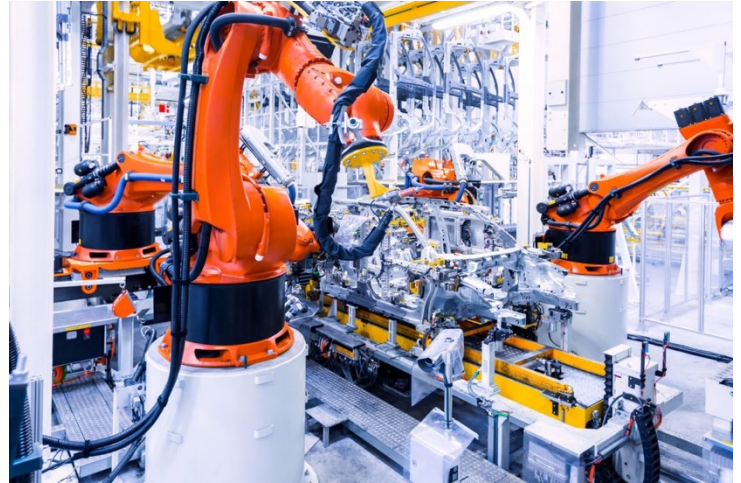
FISHY is envisioned as an extensible and programmable framework that can flexibly orchestrate the whole set of ICT systems and security controls. It will provide an innovative cyber resilience framework, where complex ICT systems performance in an entire supply chain may be analyzed in terms of security, trust and privacy impact on performance. To this end, FISHY seamlessly combines advancements in several domains, including, Software Defined Networking (SDN), Network Function Virtualization (NFV), intent-based networking, AI-based techniques, and Distributed Ledger Technologies (DLT). The final target is the creation of a trusted mosaic of ICT subsystems.

Each stakeholder participates in the supply chain through resources and infrastructure, from data to IT infrastructure. The main FISHY concept relies on designing a security, trustworthy and certification layer, transversal to the whole set of stakeholders in the supply chain intended to make the entire ICT supply chain system resilient, but also to correctly measure the complete security compliance and consequently trigger the required actions (mitigation, reconfiguration, etc.), making sure that guarantees for a certain level of cyber resilience are provided.

FISHY functional architecture proposes four principal functional modules: Intent-based Resilience Orchestrator and Dashboard (IRO), Security and Certification Manager (SCM), Trust Manager (TM) and the Secure Infrastructure Abstraction (SIA).

# FISHY early adopters: Securing Autonomous Driving Function at the Edge

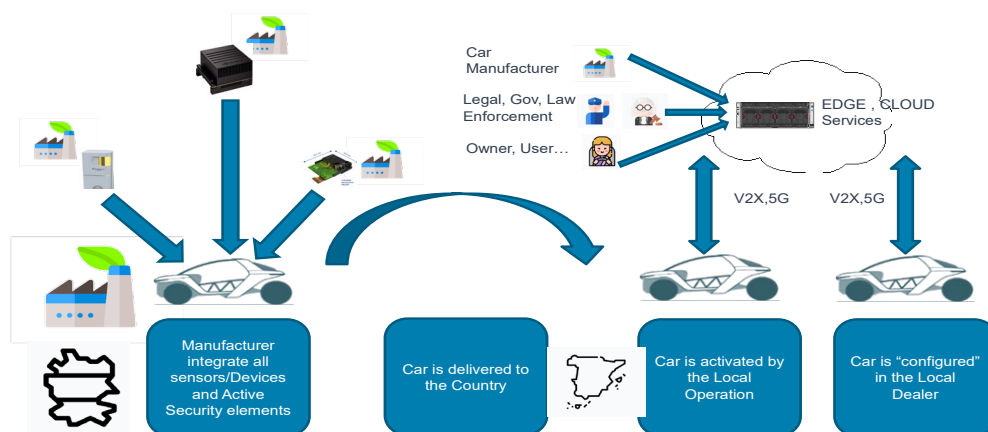
With the increasing number of electronic, intelligent embedded systems and connectivity in the cars plus the impending revolution of the fully connected and autonomous cars, security is becoming a major concern in the industry, regulators and the public.



**Main concerns** about cybersecurity revolve around Software in the Automotive Supply Chain and level of the connectivity in the Connected Car.

**The FISHY platform will provide the following functionalities:**

- **To ensure a homogenous and consistent continuous secure software development life cycle**
  - ✓ To address SW patching and risk in all components.
  - ✓ Independent from the location
  - ✓ Able to segregate in car and its components
- **To enable elaborate access management to private data of the vehicles, ensuring anonymization and data protection**
- **To enforce security policies for addressing cyberthreats, and identify and protect security assets of the cars**



# FISHY early adopters: Farm-to-Fork Supply Chain

Consumers' demand for "safe" food, including organic, is skyrocketing; thus, producers, manufacturers, sellers and end-users are often struggling to **verify the accuracy of data across the whole supply chain of products** (from farm to fork).

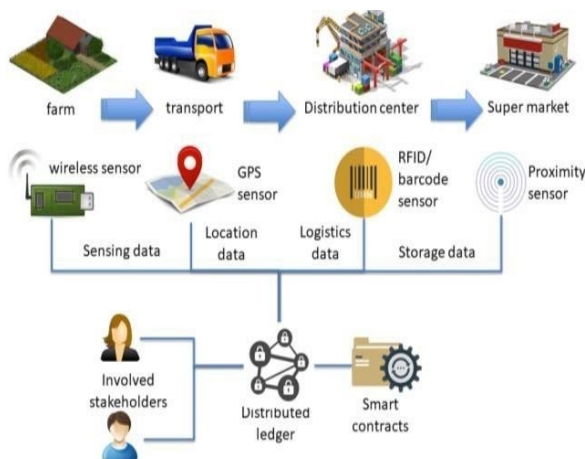
The Farm-to-Fork (**F2F**) use case builds an agricultural supply chain scenario, leveraging a decentralized trusted process intended at facilitating all interested stakeholders to receive information about the conditions under which the products have been cultivated, stored and transported during their entire lifetime.



## The challenges

- Different actors use IT systems of different providers and technologies
- Cybersecurity attacks to servers, databases, cloud environments and components could affect the whole system
- There exists a need for controlled access to resources and information
- Need to shield from blockchain threats

## The FISHY platform will:



- Offer enhanced security and real time monitoring of all elements of the IT chain
- Develop auditing mechanism to safeguard accountability based on evidence and not only trust
- Provides security from blockchain-oriented threats providing interledger solutions

# FISHY early adopters: Wood-based Panels Trusted Value Chain



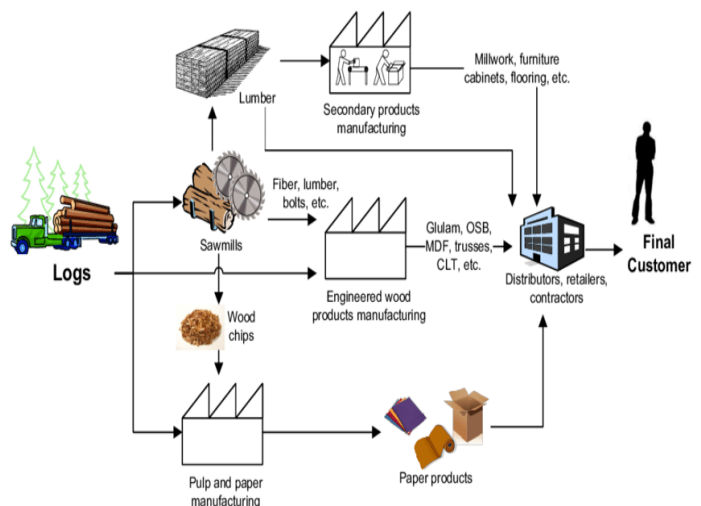
Manufacturing of wood-based panels is done in a continuous process involving the feeding of raw materials (wood and resins from external suppliers), their processing (through heat and pressure) and finishing of the panels (sanding and cutting) or further processing (such as surfacing with decorative papers from external suppliers). Requirements from those B2B clients, in terms of product quality, standards compliance and service levels, are more and more demanding. And diversity in the product mix is increasing.

## The challenges

- Extraction and integration of data from different machineries and suppliers, work with seamless connectivity and integrate cybersecurity in the whole system

## The FISHY platform will:

- offer trust guarantees and security assurance of individual IoT devices, the ecosystem of IoT devices and the edge and cloud infrastructures in place
- enable IoT security auditing
- provide a mixture of traditional IoT security controls, gateways and virtualized network security functions to provide security-on-demand





# Who are we

The FISHY consortium is composed of experts in different technical areas, with special focus in cybersecurity and supply chain. The project is based in designing and developing innovative solutions that can be intergrated naturally in the supply chain infrastructure, covering the whole life cycle and different elements/characteristics of these systems. The FISHY platform will be a central element for industry organizations that will be able to analyze and identify early threats, vulnerabilities, and the impact of cascading effects in the whole system. Finally, trust and assurance is a key pillar of the project so organizations using FISHY will be able to provide these aspects to their clients, which are also an important aspect of the project.

## Atos



## optimum.

## SYNELIXIS

Capgemini  engineering



[fishy-project.eu](http://fishy-project.eu)

[@fishy-project](https://www.linkedin.com/company/fishy-project)

[@H2020Fishy](https://twitter.com/H2020Fishy)

[FISHY H2020](https://www.youtube.com/channel/UC...)

### Project duration

1.9.2020 - 31.8.2023

### Project manager

José Francisco Ruiz, Atos Spain  
[josefrancisco.ruiz@atos.net](mailto:josefrancisco.ruiz@atos.net)

### Dissemination manager

Eva Marin, UPC  
[eva@ac.upc.edu](mailto:eva@ac.upc.edu)

### Technical manager

Xavi Masip, UPC  
[xmasip@ac.upc.edu](mailto:xmasip@ac.upc.edu)

### Innovation manager

Joao Costa, XLAB  
[joao.pitacosta@xlab.si](mailto:joao.pitacosta@xlab.si)



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644