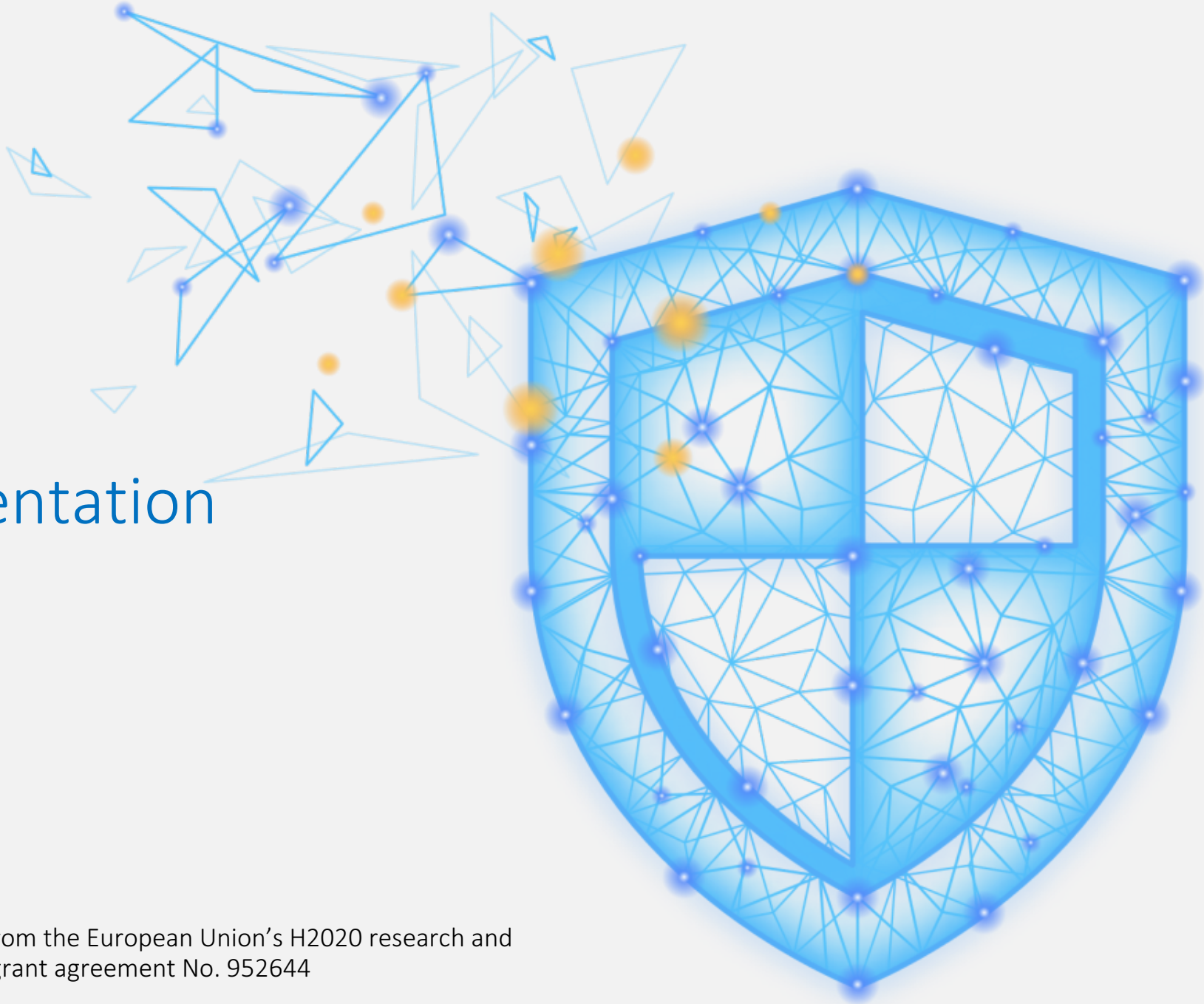
H2020 FISHY presentation



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

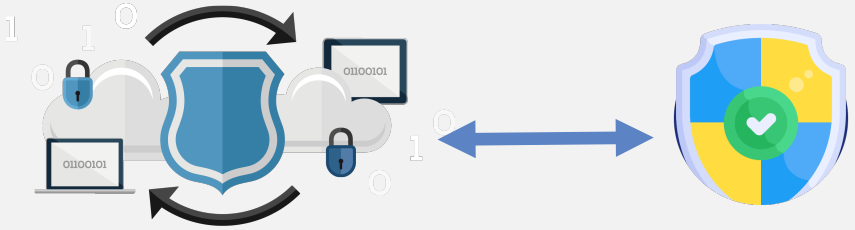
Agenda

1. What is FISHY
2. Who we are
3. Framework
4. Objetives
5. FISHY Use Cases

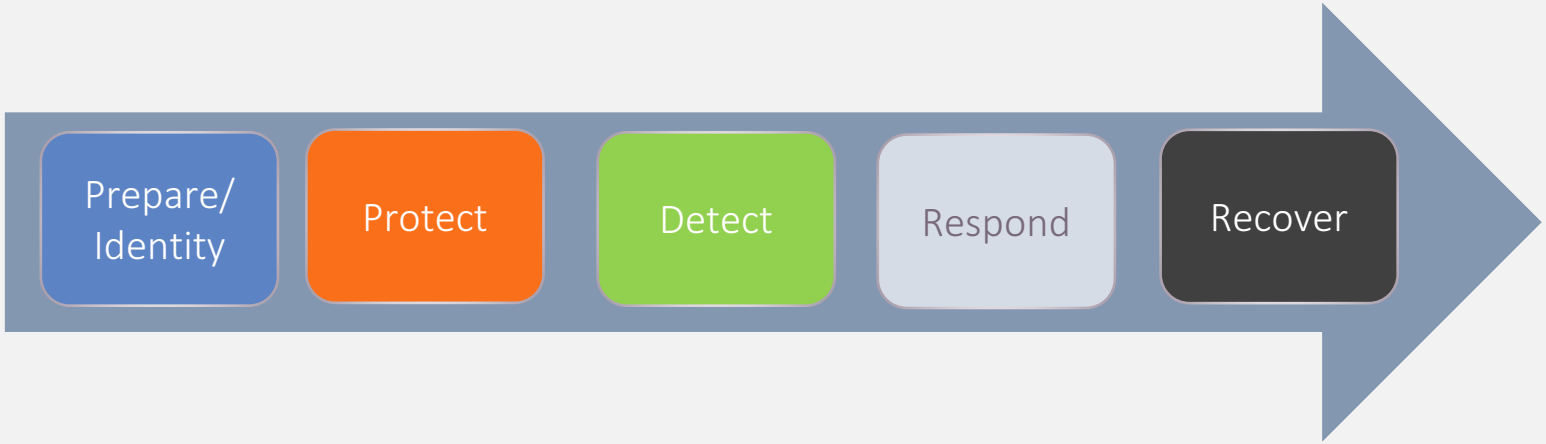
What is FISHY

What is FISHY: Motivation

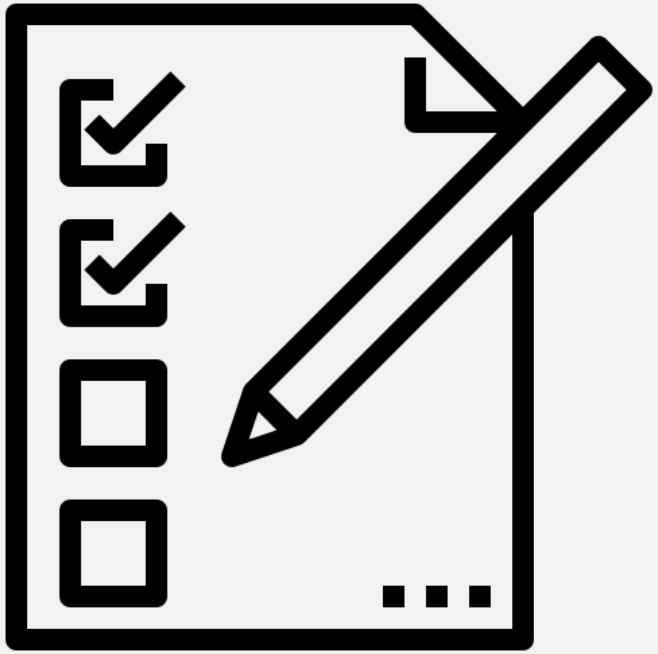
- Establishing the proper link between **cyber resilience** and **cybersecurity**.



- Establishing a proper evaluation of the **cybersecurity process**, following the **five pillars for security evaluation**:



What is FISHY: Challenges



- **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.**

What FISHY offers you

- Project **FISHY** will develop a **coordinated framework** for **cyber resilience provisioning** guaranteeing trusted **supply chains of ICT systems**.
- **FISHY** will deal with **all the supply chain components** addressing **security and privacy functionalities:**
  - ✓ risks and vulnerabilities
  - ✓ accountability,
  - ✓ mitigation strategies
  - ✓ security metrics
  - ✓ evidence-based security assurance

Who we are

Who we are

Coordinator: José Francisco Ruiz, Atos Spain

Funding: Grant agreement No 952644

Duration of the Project: from 1 September 2020 until 31 August 2023

Website: https://fishy-project.eu/

@H2020Fishy

https://www.linkedin.com/groups/8979556/

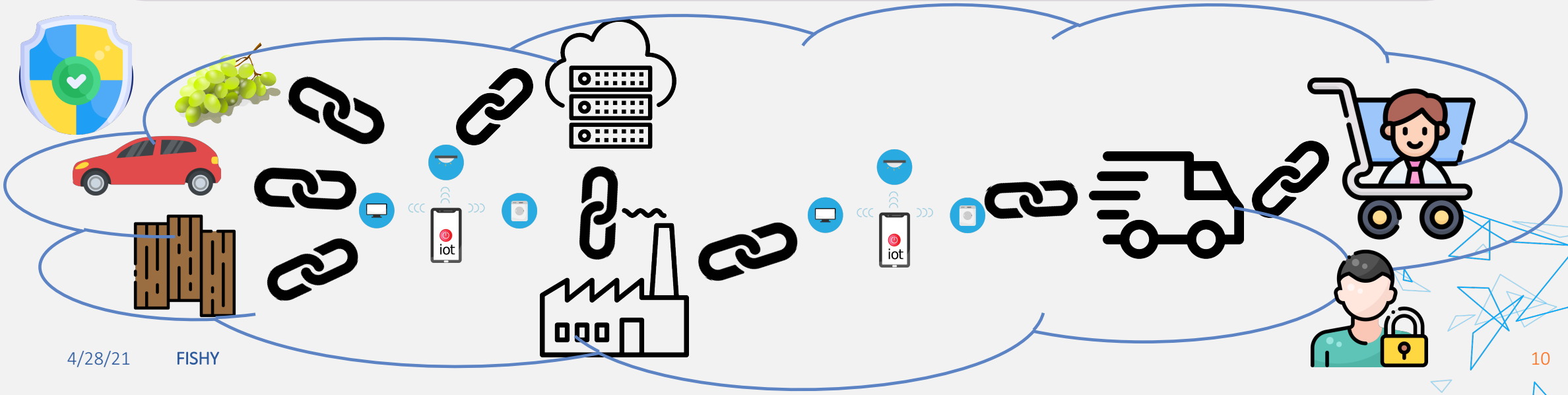
FISHY H2020

3

Framework

Framework

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**.



Objectives

What is FISHY: Objectives

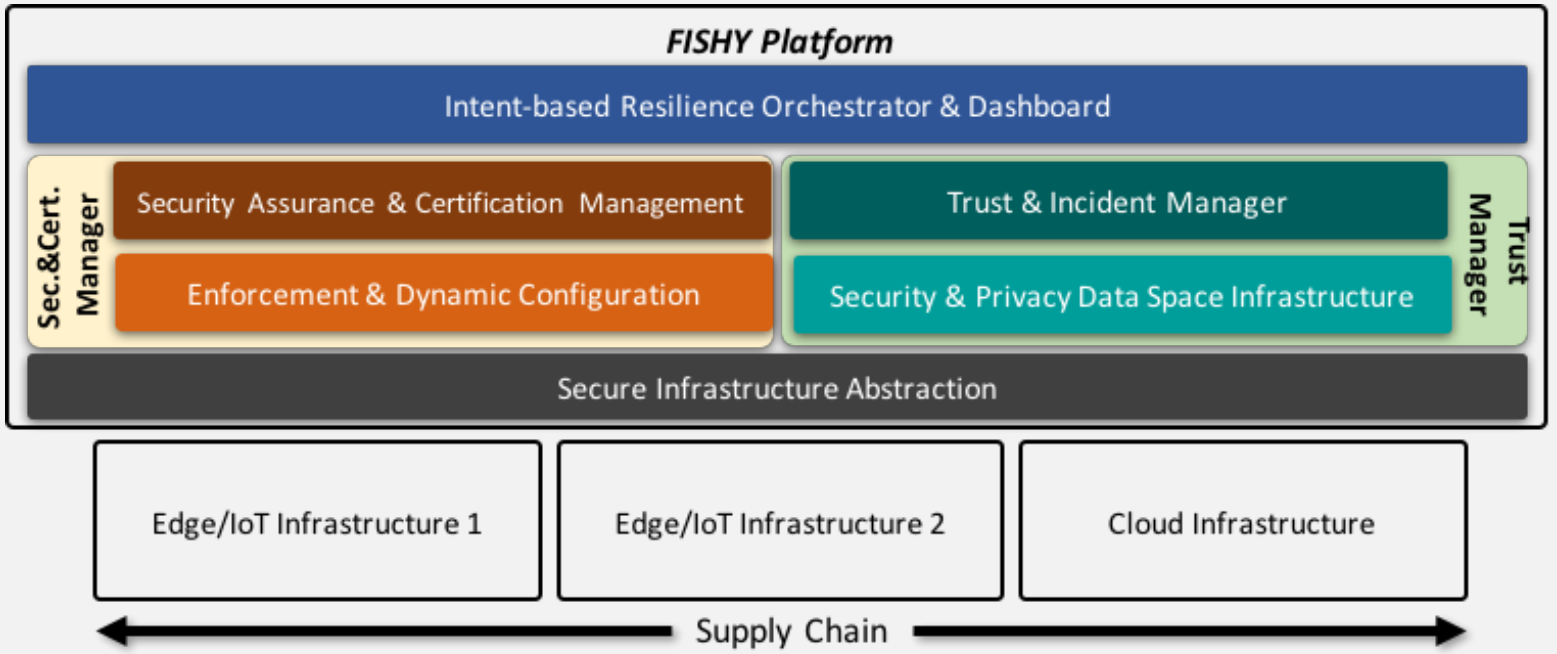
- ***Objective 1:*** *Design and develop a functional* ***platform*** *for* ***cyber resilience provisioning*** *for* ***supply chains*** *of complex* ***ICT systems****, leveraging* ***trust and security management****.*
- ***Objective 2:*** *Develop an* ***evidence-based security assurance*** *and* ***certification methodology*** *identifying security claims and metrics.*
- ***Objective 3:*** *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.*
- ***Objective 4:*** ***Deploy, validate and demonstrate*** *the FISHY platform in heterogeneous,* ***real-world pilots****.*
- ***Objective 5:*** ***Accelerate*** *the adoption and maximize the* ***impact*** *of the project.*

FISHY Concept

FISHY concept: High level architecture

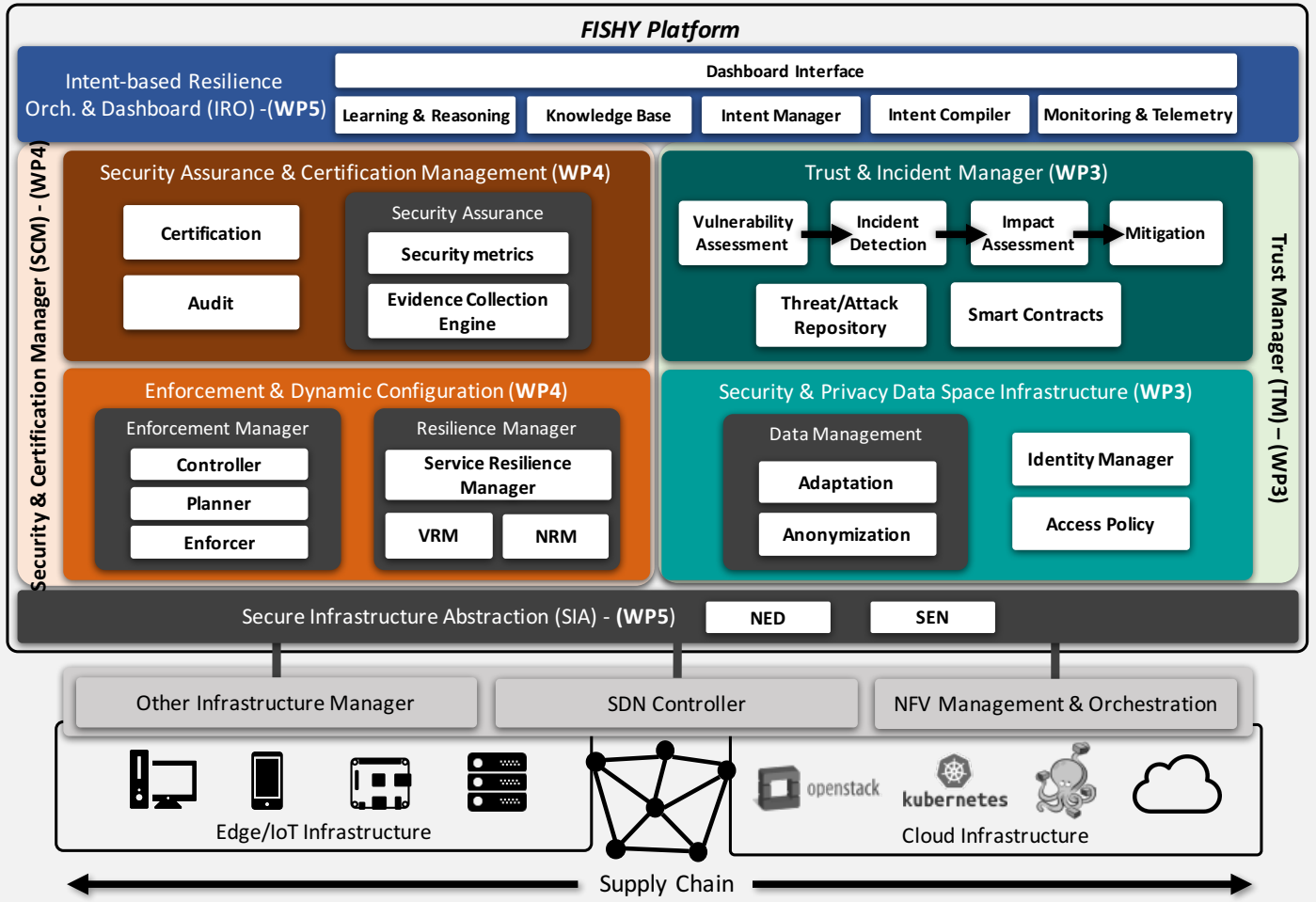
FISHY Platform:

- *Intent-based Resilience Orchestrator and Dashboard (**IRO**)*
- *Security and Certification Manager (**SCM**)*
  - Secure Assurance & Certification Management
  - Enforcement and Dynamic Configuration
- *Trust Manager (**TM**)*
  - *Trust & Incident Manager*
  - *Security & Privacy Data Space Infrastructure*
- *Secure infrastructure Abstraction (**SIA**)*



FISHY concept: FISHY architecture

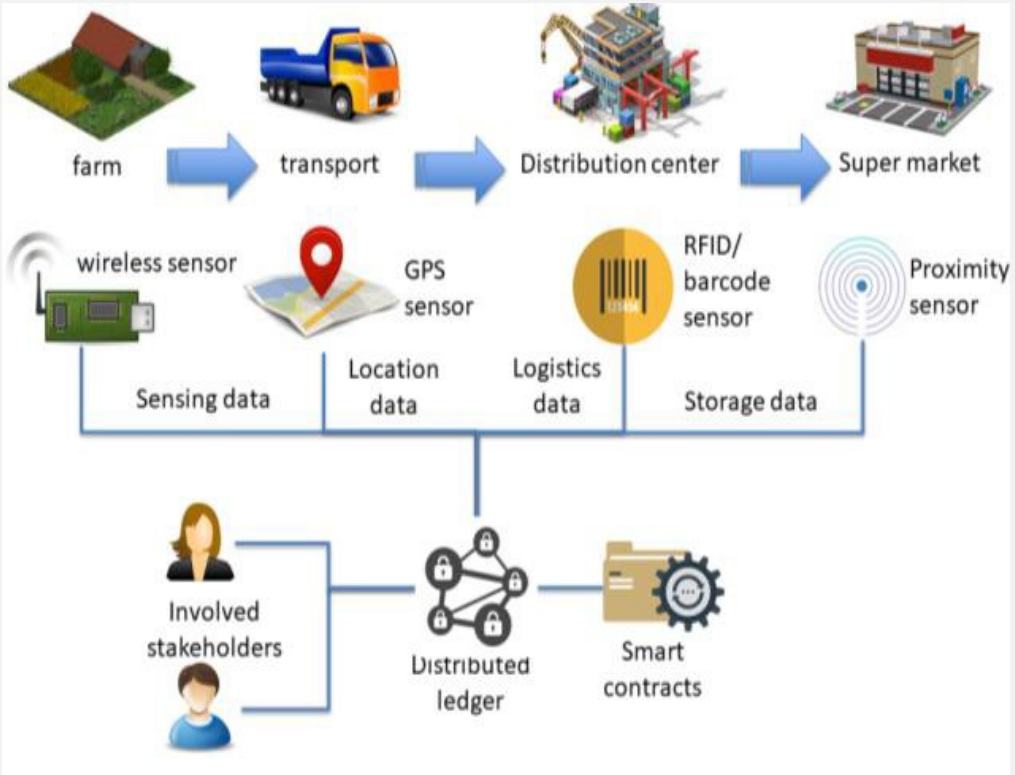
FISHY functional architecture in the entire ICT system



FISHY Use Cases

FISHY Use Cases: Farm-to-Fork Supply Chain

- 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.



FISHY Use Cases: Farm-to-Fork Supply Chain

The challenges

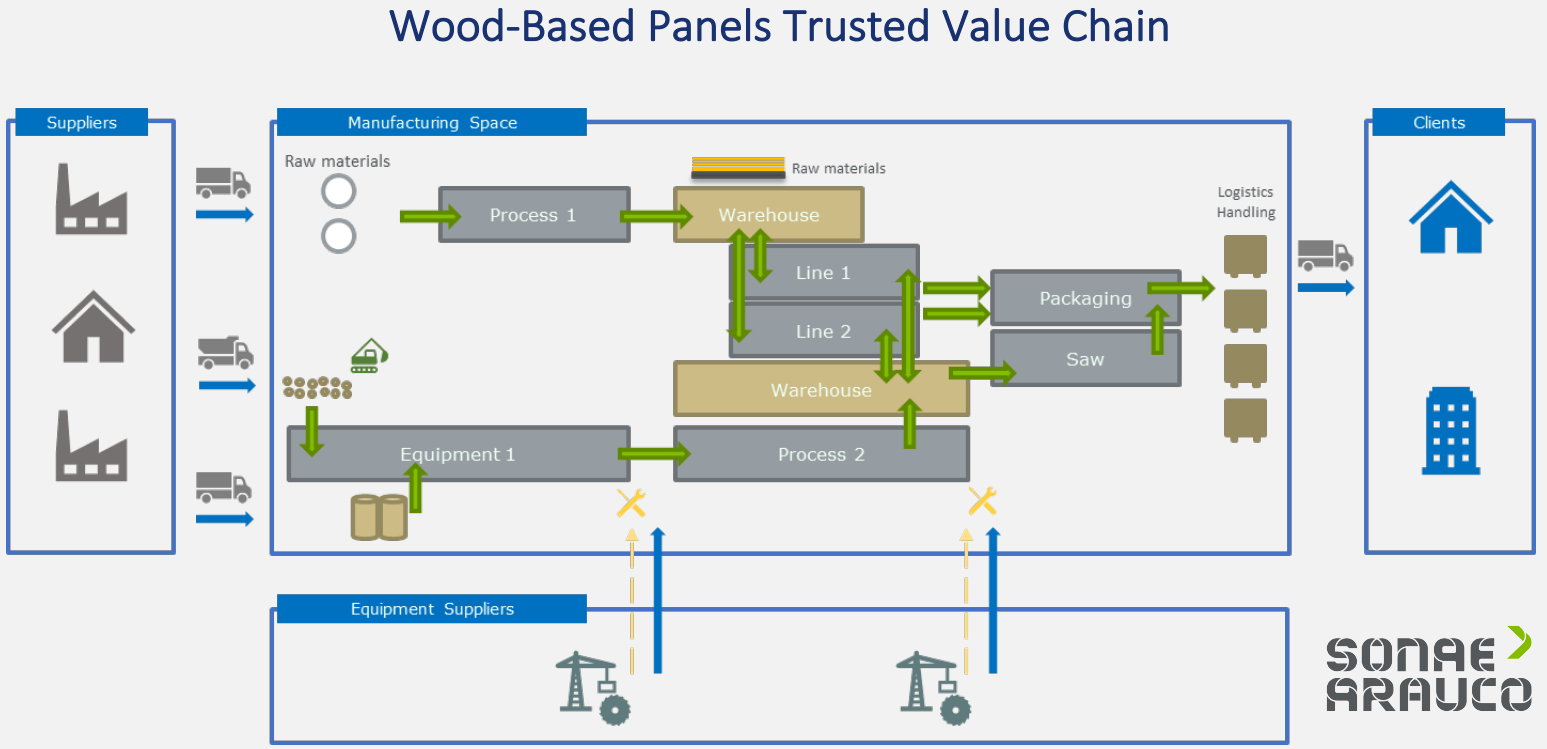
- Different actors use IT systems of different providers and technologies which makes difficult the protection of the whole IT chain
- Cybersecurity attacks to servers, databases, cloud environments and components
- Controlled access to actor-specific information is mandatory
- Need to shield from blockchain threats

The FISHY platform

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

FISHY Use Cases: Wood-Based Panels Trusted Value Chain

- The Wood-Based Panels Trusted Value Chain (**WBP TRUST**) use case consists of a real manufacturing scenario, fostering the principles of Industry 4.0, where ensuring security, integrity and reliability is very important.
- This use case aims to run a proof-of-concept to test and help validate the components of FISHY designed to facilitate trust guarantees and security assurance in that value-chain, using a real end-to-end business process as the main validation scenario.
- This use case will thus help set the basis to foster an ecosystem of services that take advantage of digitally connected manufacturing environments.



FISHY Use Cases: Wood-based Panels Trusted Value Chain

The challenges

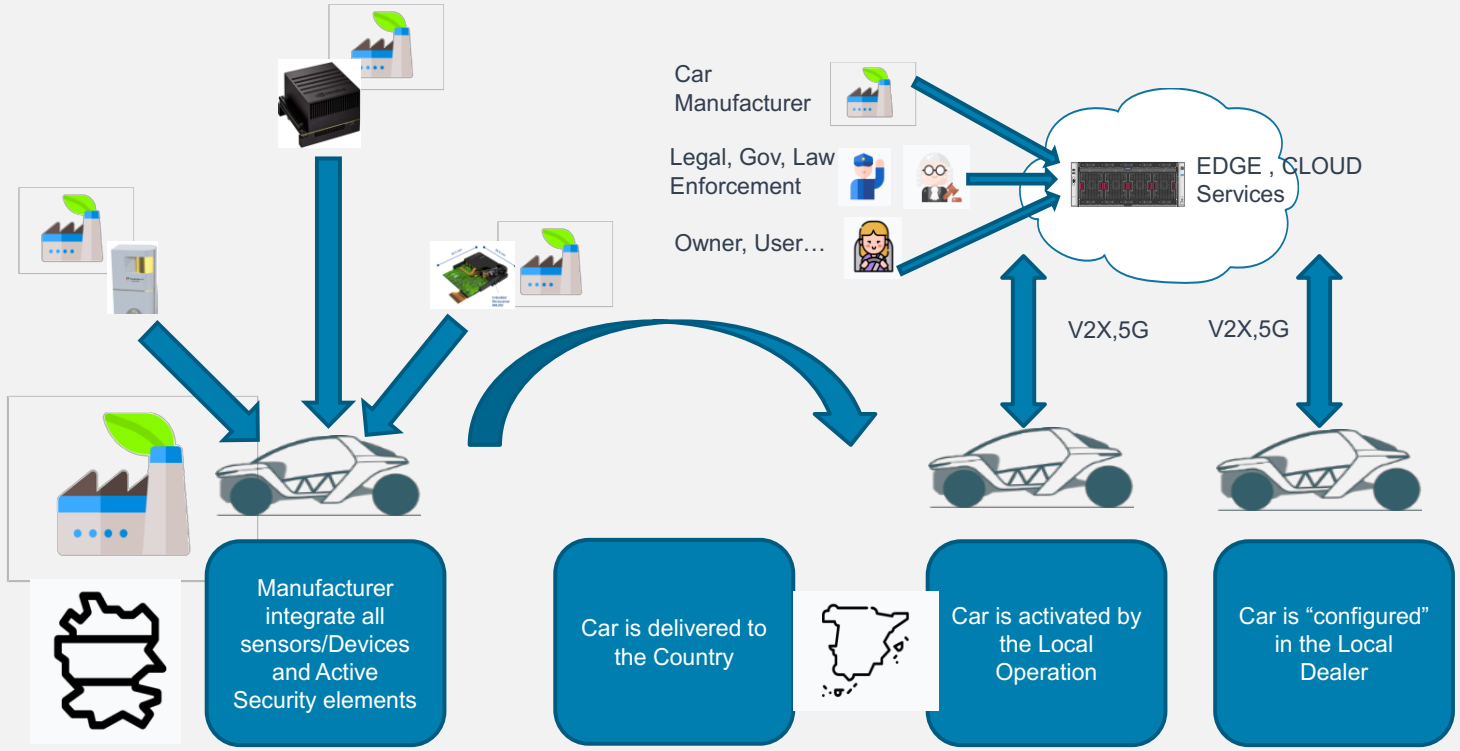
- Extractions and integration of data from a wide number of different machineries from different suppliers, some of them old and with outdated software
- Seamless connectivity through heterogeneous networks
- Cybersecurity of all connected devices and prevention of attacks and incidents to guarantee the availability (uptime) of the production plants

The FISHY platform

- offers trust guarantees and security assurance of individual IoT devices, the ecosystem of IoT devices and the edge and cloud infrastructures in place
- enables IoT security auditing
- is based on a mixture of traditional IoT security controls, gateways and virtualized network security functions to provide security-on-demand as need-based.

FISHY Use Case: Securing Autonomous Driving Function at the Edge

- Cars IOT Supply chain:
  - ✓ OEMs rely in hundreds of providers for many of the embedded systems, becoming more of a system integrator but with full accountability of the call during its entire life span and Location
  - ✓ Security patches and updates are a challenge: OEMs rely in hundreds of providers for many of the embedded systems.
  - ✓ Manufactures acts as Systems Integrators for these IOT devices.
- Connected CAR:
  - ✓ Automobile systems are now more exposed to the remote risks and tampering,
  - ✓ Connected CAR adds to above another level of complexity about identity and its management.
  - ✓ Local ton is needed and unknown



FISHY Use Case: Securing Autonomous Driving Function at the Edge

The challenges

For Cars IOT Supply chain:

- SW level verification, cybersecurity assets updates.
- Means to deploy: Wireless, OTA, procured SW and tools (Proprietary, vehicles recall)
- How to identify suspicious components or IOT Devices
- RISK of a car will be defined by the combination of the SW and Patching level of the CAR, and each of its components.

For the Connected CAR:

- How to manage sensitive data: Plates, Biometrics, Identification, Location, Speed and store it properly in the Edge / Cloud
- Who can access? How to manage it
- How to avoid to match it with the actual car

The FISHY platform

A holistic solution that

- **Ensures 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
- **Enables elaborate access management to Private Data ensuring anonymization and protection**
- **Enforces security policies to address threats** to Idenfiied security assets of the cars

Thank you

Atos

XLAB

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Telefónica I+D

SYNELIXIS

Technische Universität Braunschweig

SONAE ARAUCO
Taking wood further

SPHYNX Technology Solutions

POLITECNICO DI TORINO

Universidade do Minho

Capgemini engineering

optimum.

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