

March 12, 2021

A coordinated framework for cyber resilient supply chain systems

On September 1st, the FISHY project was successfully launched. FISHY is a 36-month Research Innovation Action (RIA) project funded by the European Union within the H2020 research program.

Why FISHY

The main aim of FISHY, fishy-project.eu, is the development of a framework for the provision of cyber resilience that guarantees trust in supply chains of ICT systems. This framework should consider 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.

In actual words of José Francisco Ruiz, coordinator of the project: “FISHY aims at integrating cybersecurity naturally in supply chain systems in order to increase their protection at design and run-time while fulfilling their specific needs. This is for us a very important aspect as nowadays trust and resilience are the basis for any organization.”

In this sense, FISHY proposes a comprehensive validation and demonstration strategy, built upon three use cases covering diverse supply chains and ICT systems, to show diversity and heterogeneity. These use cases come from different sectors, including agriculture, manufacturing, and transportation, and turn into three different validation pilots, located in Greece, Portugal and Spain respectively.

The objective of FISHY in the use case from farm to fork (F2F) is to establish, in an agricultural supply chain, a decentralized reliable process aimed at facilitating all

FISHY Consortium



Project details

Coordinator: José Francisco Ruiz, Atos Spain

Funding: Grant agreement No 952644

Start date: September 1st. 2020

Duration of the Project: 36 months

More info

 fishy-project.eu/

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

 www.linkedin.com/groups/8979556/

 FISHY H2020





interested parties to receive information on the conditions in which the products have been grown, stored and transported throughout its useful life.

In the use case Wood-based Panels Trusted Value Chain (WBP TRUST), FISHY must guarantee safety, integrity and reliability in a Plant 4.0 scenario, which brings together different machinery from different suppliers together with many connected IoT devices.

Finally, in the Securing Autonomous Driving Function at the Edge (SADE) use case, FISHY must define where the resilience functions have to be implemented to adequately adapt to the expected demands, in a scenario where cloud and edge computing are combined in an autonomous car context.

The deployment of the FISHY solution in these pilots will also clearly highlight the impact FISHY will have on real scenarios and how complex ICT systems may benefit from FISHY.

Consortium

The consortium is led by Atos and built by 12 partners from 7 European countries, namely Germany, Greece, Italia, Portugal, Slovenia, Spain and Switzerland. From the partners, four of them are large companies, four are SMEs and four are Universities, with a joint expertise encompassing cybersecurity, IoT, Artificial Intelligence, Networking, Automotive Industry, Intent-based resilience, Integration verification, Blockchain and Security Assurance, to name a few.

