CONSORTIUM

Atos Capgemini engineering Technische Universität Braunschweig

Telefónica Universidade do Minho UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

POLITECNICO DI TORINO Sphynx Technology Solutions XLAB

optimum SONAE SYNELIXIS

www.fishy-project.eu

@H2020Fishy

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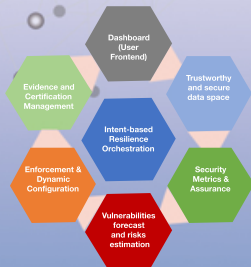
FISHY

What is FISHY?

FiSHY

FRAMEWORK
The FISHY framework takes into account 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.

ARCHITECTURE
FISHY aims at delivering a coordinated cyber resilient platform that would provide the appropriate set of tools and methods towards establishing trusted supply chains of ICT systems through novel evidence-base security assurance methodologies and metrics, innovative strategies for risk estimation and vulnerabilities forecasting, leveraging state-of-the-art solutions, leading to resilient complex ICT systems

Dashboard (User Frontend)

Evidence and Certification Management

Trustworthy and secure data space

Intent-based Resilience Orchestration

Enforcement & Dynamic Configuration

Security Metrics & Assurance

Vulnerabilities forecast and risks estimation

Expected Impacts

European Businesses
The project is seeking new market opportunities in the security/privacy/IoT/network/edge sectors, demonstrated by the use cases proposed, thus paving the way to innovative opportunities for project partners, i.e., ATOS (integrator, solution provider), TID (network operator), ALTRAN (Multi Vertical ER&D Services). SMEs (SYN, OPT, XLAB, STS, SONAE) will also benefit from FISHY by fuelling the deployment of their products and solutions in new verticals and the global market.

Dissemination
The project will follow an intense outreach strategy aiming at spreading the FISHY ideas to the industrial, research and business communities. Highly energetic actions are considered in the specific dissemination and exploitation WP.

Technology Provider
The project will start from the architecture and will evolve while fine-tuning the different functional blocks, components and technologies. The system components are integrated in the subsequent phase and tested at lab premises. Finally, the overall system is validated in a PoC and in three different use cases.

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 3: Develop a 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 2: Develop an evidence-based security assurance and certification methodology identifying security claims and metrics.

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.