

Key Innovations in Supply Chain Cybersecurity and Resilience that Make Sense in Today's Industry

FISHY Press Release #3

The pertinence of runtime security is rapidly engaging companies and institutions worldwide, that are becoming more aware of their vulnerabilities and consequences of attacks, in the age of digital transformation affecting workflows across industries. With the different skillsets and expertise of the FISHY Consortium partners, the impact of the novelty developed in this project is already affecting highly relevant domains in the context of supply-chain cybersecurity and resilience, such as vulnerability management and risk/integrity assessment; security assurance & certification management; and intrusion and detection or cloud-native networking.






(free image, credit: j-mel - stock.adobe.com)

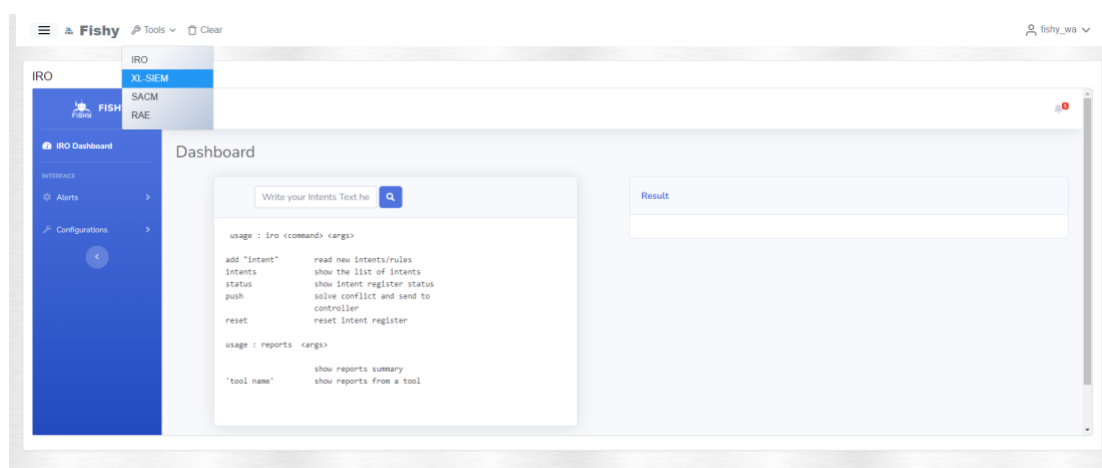
The FISHY Framework considers all the **supply chain** components, from the **IoT ecosystem** to the **infrastructure** connecting them, addressing **security and privacy** functionalities related to **risks** and **vulnerabilities** management, accountability, and **mitigation strategies** as well as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



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.

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. It also makes available 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.



FISHY is a platform that is not vendor-specific, with a modular approach to ensuring cybersecurity that offers **monitoring, and security and resilience enforcement all-in-one** tool (these functionalities are typically separate and vendor-specific). FISHY's **vulnerability forecast and risk estimation** toolkit enables users to set up custom scans based on any user-provided script or by using the integrated vulnerability scanners to run the scanning tasks on-demand immediately or set up automatic repeated schedules, being alerted to new vulnerabilities discovered.

The novel **Intent-based Resilience Orchestration** technology is translating high level intents into configured policies, and interact with the system response using AI techniques. It is mostly open source, offering AI/ML-based intent-based resilience orchestration responsible for mapping high-level intents given by a user into configured policies that can run by a lower-level system controller. With its **Enforcement & Dynamic Configuration** engine FISHY, it can focus

especially on regulatory obligations and automated configuration of security controls, avoiding configuration errors in modern SDN-based infrastructures, and ensuring the fast implementation of sophisticated remediations to cybersecurity attacks.

To enhance security in supply chains, FISHY includes also (i) a **Security Assurance and Certification Manager**, focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements, tailored to supply chain needs; and (ii) a **Security & Privacy Dataspace Infrastructure** able to help supply chain managers to analyse security metrics and translate high-level intents into configured policies related to Access Control, providing a common event format to facilitate security event analysis. Moreover, FISHY's **Secure Infrastructure Abstraction** is fully open source and its functionality includes standardised API for network infrastructure abstraction supporting a consistent connectivity framework, based on a virtual distributed switch.

The importance of Open Source Software and of the Communities associated with it highly contributes to the excellence of European research and development, and for the health and prosperity of the European industrial landscape. In line with the European Commission's Open Source Software Strategy, FISHY contributes to the innovation and autonomy of Europe's digital infrastructure, particularly in the security and resilience of supply chains. To guide these contributions, we defined the five pillars of open research - (1) a FISHY public repository, (2) the upstreaming of specific components of the FISHY KERs to open source repositories of FISHY Consortium member institutions, (3) community engagement, (4) contribution to standards and (5) open research - that promotes the collaboration between researchers, the dissemination and reuse of innovation, and the sustainability of the technology developed in this project.

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. FISHY's early adopters are present in the food industry, the connected cars sector and in the smart factories domain. The Farm-to-Fork use case of SYNELIXIS obtained the reduction in downtime, given that 62% of supply chain attacks exploit the trust of client to their supplier and that 58% of attacks aim at accessing data. The FISHY technology allowed CAPGEMINI for a significant improvement regarding

safety in the car thanks to logs and certification monitoring, with 80% achievement FISHY integration on premises and edge. On the other hand, the automated identification of rogue IoT devices in the smart factories of SONAE helps reduce cybersecurity effort by detecting unauthorized and potentially malicious devices within the network.

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.

Communication manager

Eva Marin, UPC

[*eva.marin@upc.edu*](mailto:eva.marin@upc.edu)

Innovation manager

Joao Costa, XLAB

[*joao.pitacosta@xlab.si*](mailto:joao.pitacosta@xlab.si)

Project coordinator

Antonio Alvarez Romero, Eviden

[*antonio.alvarez@eviden.com*](mailto:antonio.alvarez@eviden.com)

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

LinkedIn: <https://www.linkedin.com/in/fishy-project-16342920a/>

Twitter: <https://twitter.com/H2020Fishy>

Youtube: <https://www.youtube.com/channel/UCSDpfCPvFNjRS3RemG0iNQQ/>

GitHub: <https://github.com/H2020-FISHY>

Zenodo: <https://zenodo.org/communities/fishy/?page=1&size=20>