SELFY: building cyber-resilient, self-healing connected vehicles for Europe

How a Horizon Europe project raised the cybersecurity bar for the Cooperative, Connected and Automated Mobility (CCAM).

Image: SELFY self-assessment, protection and healing tools validation in a closed track recreating manoeuvres close to everyday traffic using dummies, real vehicles and targeted attacks.

Europe is moving decisively toward CCAM—a reality in which vehicles are more than just machines. They generate data, make decisions and interact within complex ecosystems. Every additional layer of connectivity creates another door for cyberattacks. A hacked sensor or forged message could jam a bus corridor, paralyse a logistics hub or even cause accidents.

Over the last three years, the European research project SELFY, coordinated by the Eurecat Technology Center, has established trust in the CCAM ecosystem and validated a self-assessment and self-protection toolbox that enables CCAM to detect security breaches, mitigate attacks and heal without compromising privacy or interoperability.

Working collaboratively, a consortium of 16 partners in eight countries developed three macro-tools focusing on situational awareness and collaborative perception, cooperative resilience and healing, trust and data management. The tools are designed to increase the resilience and cybersecurity of autonomous and connected vehicles in smart cities.

The maturity of the solution has been confirmed by real-world demonstrations on Applus+ IDIADA's ADAS and CAV Urban Area track proving ground in Catalonia, as well as on Vienna's public roads.

> "SELFY offers automotive manufacturers, traffic managers, fleet operators and drivers a comprehensive solution to detect, respond to and mitigate cyberattacks, while fully preserving the privacy and integrity of autonomous mobility systems."

Fanny Breuil
SELFY coordinator,
European Programme Manager,
Eurecat Technology Center

Image: SELFY vehicle demonstrator with LIDAR during real-world demonstrations.

The SELFY solution identifies over 95% of vulnerable vehicles and more than 90% of security breaches, while also enabling the vehicles themselves to protect and self-recover, ensuring trust and secure data exchange.

Situational awareness and collaborative perception: obtaining a comprehensive understanding of the environment

At the core of autonomous decision-making lies awareness of the surrounding environment. SELFY's Situational Awareness and Collaborative Perception framework was created to ensure awareness with shared, yet trustworthy, perception.

The system fuses vehicle perception with infrastructure information to build a unified view of the environment. Its tools continuously analyse the coherence of sensors and cooperative messages to detect discrepancies and assess the reliability of each source before relying on it for driving decisions.

It comprises three primary categories of tools: vehicle-centred tools, which enable vehicles to perceive and interpret their surroundings accurately; RSU-centred tools, which combine advanced hardware and software within roadside units (RSUs) to gather and analyse environmental data; and tools for data fusion and situational awareness, aimed at aggregating shared perception data.

Cooperative resilience and healing system: an immune layer for connected mobility

The tools for the Cooperative Resilience and Healing System are designed to protect CCAM environments against cyberattacks and security breaches. Managed by a Vehicle Security Operations Centre (VSOC), the system enhances resilience, robustness and system trust levels, and provides a secure degraded mode for vehicles when necessary.

The Cooperative Resilience and Healing System consists of seven integrated tools. Beginning with the VSOC, which orchestrates primary cybersecurity in the SELFY solution, the system also includes tools that detect anomalies or raise an alarm if the execution of an application or a communication flow deviates from the expected one. Additionally, tools are installed in a roadside unit that audits all vehicles passing nearby. It also provides algorithms to increase robustness in cooperative driving.

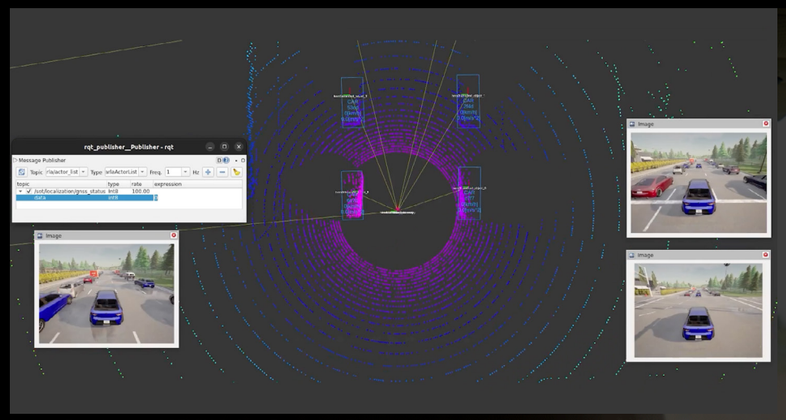

Image: Dashboard of SELFY Safety Operation Tool, ensuring the vehicle can enter a safe mode based on risk assessments.

Trust data management system: privacy and integrity by design

Connected mobility cannot thrive if every camera frame and sensor log threatens personal privacy. SELFY's Trust Data Management System combines tools that address trust and secure data management to ensure information protection and privacy.

They incorporate algorithms to detect malicious behaviour in both vehicles and roadside units, apply AI-based anonymisation techniques to sensitive data in video feeds, add noise to existing data to protect privacy, and use software update mechanisms with post-quantum cryptography to ensure the integrity and traceability of each new version.

Real-world demonstrations in Catalonia and Vienna

The solutions developed by the project were first validated in the lab and in simulation. After that, tools were also evaluated in real scenarios.

The first large-scale evaluation of the SELFY toolbox took place at the Applus+ IDIADA ADAS/CAV Urban Area proving ground, southwest of Barcelona, where engineers configured the urban section to mimic roundabouts, bus lanes, intersections and pedestrian crossings.

The tests recreated scenarios such as detecting a vulnerable road user while a hacked vehicle was transmitting misleading information, identifying sensor failures through infrastructure data fusion, filtering unreliable cooperative messages and safely aborting an overtaking manoeuvre during an active cyberattack. An anonymisation algorithm was also verified, protecting sensitive data in real time, such as pedestrian faces and vehicle licence plates.

In parallel, a demonstration was held in the city centre of Vienna, Austria, under live-traffic conditions, with camera sensors and roadside units installed across the city. The SELFY system monitored the coherence between images and cooperative awareness messages (CAM), accurately detecting artificially induced mismatches and validating the infrastructure's capability to identify misaligned or tampered sensors.

The successful live-traffic validation demonstrated that the SELFY solution, which performs well in a closed circuit, can withstand the unpredictability of a historic city centre.

Impact on Europe's CCAM landscape

SELFY strengthens Europe's claim to leadership in connected and automated mobility by proving that the sector's most daunting risk, cyber insecurity, can be managed with transparent, interoperable and privacy-preserving technology. In doing so, it underpins long-term industrial growth, safeguards jobs and, above all, fosters public confidence that the road to automated transport is not only smart and green but also secure by design.

These results matter because CCAM's promises—fewer crashes, lower emissions, better access—hinge on trust. SELFY's toolbox solution provides original equipment manufacturers (OEMs), their key suppliers (Tier 1) and regulators with a trustworthy solution that increases the cybersecurity of the vehicle network and makes connected driving environments more reliable.

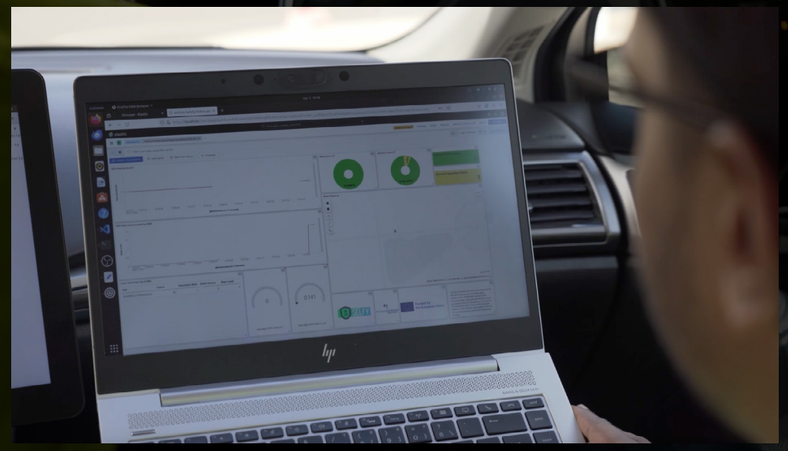

Image: View of SELFY's Vehicle Security Operations Center (VSOC) for holistic monitoring and control of vehicle fleets in CCAM systems.

> SELFY responds to emerging risks and threats requiring a global, distributed, decentralised and collaborative solution that works between static and mobile assets and CCAM ecosystem players.
>
> **Víctor Jiménez**
> SELFY technical coordinator,
> IT&OT researcher,
> Eurecat Technology Center

The project also strengthens Europe's position in the global mobility race. The SELFY solution provides manufacturers and suppliers with a ready-to-use framework for meeting new cybersecurity standards, enabling them to bring products to market faster.

Trust between all road users is another gain. Every piece of data moving between cars, trucks, roadside units and control centres is checked and authenticated. At the same time, faces and licence plates are anonymised, protecting privacy. For the public, the benefit is clear: transport that is seamless, affordable and easy to trust.

SELFY lowers barriers to acceptance and helps citizens understand both the advantages and limits of automated mobility by reducing service interruptions and protecting personal data.

Key takeaways

- **>95% detection rate** for vulnerable vehicles and **>90% of security breaches** thanks to an integrated solution.
- **Three macro-tools** for CCAM-enhanced perception, resilience and trusted data work together from vehicle level to the cloud.
- **Real-world pilots** in Catalonia and the city of Vienna proved the concept in both closed-track and live-traffic conditions.
- **Open-source Vehicle Security Operations Centre (VSOC).**
- **Immediate relevance for EU CCAM policy**: stronger user trust, smoother type-approval and a more resilient single market for automated mobility.

https://youtu.be/ElmD2DC5oGM?si=0_ck-9gBux3E_AGC

SELFY

SELF assessment, protection and healing tools for a trustworthy and resilient CCAM

PROJECT SUMMARY

The SELFY project has created a toolbox of collaborative tools to enhance the security, protection and resilience of the CCAM against cyberthreats. The tools developed have been validated in the lab, followed by real-world scenarios to demonstrate their effectiveness.

PROJECT PARTNERS

The consortium, led by the technology centre Eurecat, includes partners from eight countries, including Spain (Eurecat, Tecnalia, AEVAC, Ficosa and Applus+ IDIADA); France with CEA and Canon Research Centre; Germany with Technische Hochschule Ingolstadt and FEV.io; Austria with Virtual Vehicle Research and City of Vienna; the Netherlands with Eindoven University of Technology; Japan with Okayama University; Australia with RMIT University; and Turkey with FEV.

PROJECT LEAD PROFILE

Fanny Breuil: BA and Master's in Business Administration. Former Business Unit Manager at DHL Express. For over 15 years, Breuil has led EU R&I projects (e.g. SHIFT2ZERO, SELFY, FRONTIER) at CETEMAR, CETEMMSA and now Eurecat. As Head of Transport and Mobility Programmes, she oversees fundraising, project coordination and EU strategic positioning. Breuil is also an occasional expert evaluator for the European Commission.

Víctor Jiménez: Electronics Engineer. Over the last seven years, Jiménez has researched cybersecurity, focusing on hardware and system-level solutions in the automotive and industrial sectors at Eurecat. He has been coordinating the technical aspects of some European Projects and has also worked in the private sector. Previously, Jiménez was involved in hardware and system design in the automotive and railway sectors.

PROJECT CONTACTS

Fanny Breuil, **Project coordinator**
Av. Universitat Autònoma,
23. ParcTecnològic del Vallés, 08290
Cerdanyola del Vallès – Barcelona
info@selfy-project.eu
linkedin.com/company/selfy-project/
@Selfy_EUProject
@SELFY_EUProject

Funded by the European Union

FUNDING DISCLAIMER

This project has been funded by European Union's Horizon Europe research and innovation programme grant agreement no. 101069748.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.