

SELFY project: Realistic demonstrations show new cybersecurity tools for autonomous and connected vehicles

- **The SELFY toolbox solution aims to detect safety violations that go beyond a single vehicle's own field of view (FOV).**
- **First validations in urban areas on the ADAS/CAV test track at Applus+ IDIADA in Catalonia, where real-life situations in large cities were simulated.**
- **Live traffic demonstration in the city center of Vienna, where camera sensors and roadside units were distributed throughout the city.**
- **VIRTUAL VEHICLE provides expertise and automated test vehicles and develops new functions for data exchange**
- **SELFY offers car manufacturers, traffic managers, fleet operators and drivers a comprehensive solution to detect, respond to and mitigate cyberattacks.**

Graz/ Austria, June 17, 2025 - The [European consortium SELFY](#), coordinated by the Eurecat Technology Center, has demonstrated the effectiveness of new self-assessment and self-protection tools to increase the resilience and cybersecurity of autonomous and connected vehicles in smart cities through pilot tests in the Catalonia region and the city of Vienna. The SELFY solution identifies more than 95% of vulnerable vehicles and more than 90% of security breaches.

After three years of research and development, "SELFY offers automotive manufacturers, traffic managers, fleet operators and drivers with a comprehensive solution to detect, respond to and mitigate cyberattacks while fully preserving the privacy and integrity of autonomous mobility systems," explains *Fanny Breuil, project coordinator and European program manager at Eurecat*.

With this solution, "it is possible to identify vulnerable vehicles, reduce the risk of security breaches and enable the vehicles themselves to protect and self-recover, ensuring trust and secure data exchange", adds *SELFY's technical coordinator, Víctor Jiménez, researcher in Eurecat's IT&OT Security Unit at Eurecat*.

The first validation took place in the urban area of the ADAS/CAV test track at Applus+ IDIADA in Catalonia (Spain), with a layout that replicates intersections, traffic circles, pedestrian crossings and driving lanes to faithfully reproduce real traffic conditions in large cities.

The tests recreated scenarios such as detecting a vulnerable road user while a hacked vehicle was transmitting misleading information, detecting sensor failures by fusing infrastructure data, filtering unreliable cooperative messages and safely aborting an overtaking maneuver during an active cyberattack. An anonymization algorithm has also been verified to protect sensitive data such as pedestrian faces and vehicle license plates in real time.

"At the Applus+ IDIADA facilities, we used dummies, real vehicles and targeted attacks to simulate traffic-related maneuvers. The results confirm that the SELFY tools improve awareness and response to security incidents without compromising privacy," explains *Manel Rodríguez, Expert Engineer in Cybersecurity at Applus+ IDIADA*.

In parallel, a demonstration was conducted in Vienna, Austria, in the city center under live traffic conditions with camera sensors and roadside units installed throughout the city. After mounting a high-resolution camera and a roadside unit on the infrastructure, the SELFY system monitored the coherence between images and CAM messages and accurately detected artificially induced deviations, confirming the infrastructure's ability to identify misaligned or tampered sensors.

"The urban pilot confirms that the same tools that work on closed routes are also effective in real traffic. This is an important step for their introduction at European level," explains *Gernot Lenz, Coordinator for Traffic Management Systems at the City of Vienna*.

VIRTUAL VEHICLE provides expertise and automated test vehicles

As part of SELFY, the VIRTUAL VEHICLE research center developed basic functions to enable data exchange between two or more vehicles and the infrastructure. The VIRTUAL VEHICLE research vehicles used in the project can thus exchange data on road users such as pedestrians or vehicles that they detect with their sensors. This extended field of vision makes it possible to prevent accidents in particular, as information about the traffic situation and potential hazards is available at an early stage.

Another contribution of the VIRTUAL VEHICLE is a basic methodology for integrating such shared data. However, sharing precise location information is not always 100% accurate -

because the accuracy depends in particular on the sensor precision and the time interval. For example, a person can abruptly change their direction of movement in a fraction of a second.

Finally, the VIRTUAL VEHICLE also used one of its automated vehicles as a demonstrator. This automated L4 vehicle has an open architecture that allowed the SELFY project partners to load and test their self-developed functions on the vehicle. These functions were then tested both in simulations and under real conditions on a test track.

Intelligent systems for autonomous and connected driving

The SELFY project has developed three macro solutions focusing on situational awareness and collaborative perception, a cooperative resilience and recovery system, and a trust and data management system.

The situational awareness and collaborative perception system combines vehicle perception with infrastructure information to create a unified view of the environment. Its tools continuously analyze the coherence of sensors and collaborative messages to detect discrepancies and assess the reliability of each source before using it to make driving decisions.

The Cooperative Resilience and Recovery tools are designed to protect Cooperative, Connected and Automated Mobility (CCAM) environments from cyber-attacks and security breaches. Managed by a Vehicle Security Operations Center (VSOC), the system improves resilience, robustness and system confidence and provides a secure degraded mode for vehicles when needed.

The trust and secure data management tools ensure the protection of information and privacy. They include algorithms to detect malicious behavior in both vehicles and roadside units, apply AI-based anonymization techniques and use software update mechanisms with post-quantum cryptography to ensure the integrity and traceability of each new version.

The SELFY project was funded with 6 million euros as part of the Horizon Europe program. The consortium, led by the Eurecat Technology Center, 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 the [Stadt Wien](#), the Netherlands with [Eindhoven University of Technology](#), Japan with [Okayama University](#), Australia with [RMIT University](#) and Turkey with [FEV](#).

About VIRTUAL VEHICLE

With 300 employees, Virtual Vehicle Research GmbH is Europe's largest research center for virtual vehicle development. Research focuses on the close linking of numerical simulations and hardware tests in the automotive and rail industries. This enables the design and automation of test and validation procedures at a defined quality level and the continuous development and validation of complex hardware-software systems. The focus on industry-oriented research makes VIRTUAL VEHICLE an innovation catalyst for vehicle technologies of the future.

VIRTUAL VEHICLE cooperates nationally and internationally with over 180 industrial partners (OEMs, Tier 1 and Tier 2 suppliers and software providers) and with more than 80 scientific partners.

Virtual Vehicle Research GmbH, a COMET Competence Center for Excellent Technologies, is funded by the Federal Ministry for Climate Protection, the Federal Ministry of Labor and Economy, the Province of Styria (Dept. 12) and the Styrian Business Promotion Agency (SFG).

www.virtual-vehicle.at

Contact & Information:

Virtual Vehicle Research GmbH

Dr. Christoph Pilz

Senior Researcher | Project Leader

Tel: +43 316 873 9715

E-Mail: christoph.pilz@v2c2.at

EURECAT

Marina Presas Quintana

Departamento de comunicación

Tel.: +34 932 381 400 (Ext. 1250)

E-Mail: marina.presas@eurecat.org

Pictures:



SELFY-Project-Testing_VIRTUAL-VEHICLE-ADD_DSC06875 FINAL-2500.jpg
 VIRTUAL VEHICLE Automated Drive Demonstrator during test drives for the SELFY Research Project.

[Download Link](#)

© Jan Latussek / VIRTUAL VEHICLE



SELFY-Project-Testing_VIRTUAL-VEHICLE-ADD_DSC06920 FINAL-2500.jpg
 VIRTUAL VEHICLE Automated Drive Demonstrator during test drives for the SELFY Research Project.

[Download Link](#)

© Jan Latussek / VIRTUAL VEHICLE



SELFY-Project-Testing_VIRTUAL-VEHICLE-ADD_DSC06924 FINAL-2500.jpg
 VIRTUAL VEHICLE Automated Drive Demonstrator during test drives for the SELFY Research Project.

[Download Link](#)

© Jan Latussek / VIRTUAL VEHICLE



SELFY-Project-Testing_VIRTUAL-VEHICLE-ADD_DSC06978 FINAL-2500.jpg
 VIRTUAL VEHICLE Automated Drive Demonstrator during test drives for the SELFY Research Project.

[Download Link](#)

© Jan Latussek / VIRTUAL VEHICLE



SELFY-Project-Testing_VIRTUAL-VEHICLE-ADD_DSC07059 FINAL-2500.jpg
 VIRTUAL VEHICLE Automated Drive Demonstrator during test drives for the SELFY Research Project.

[Download Link](#)

© Jan Latussek / VIRTUAL VEHICLE