



# A Fail-Safe Decision Architecture for CCAM Applications

Mario Rodríguez-Arozamena<sup>1,4(✉)</sup>, Jose Matute<sup>1</sup>, Joshué Pérez<sup>1</sup>,  
Burcu Ozbay<sup>2</sup>, Deryanur Tezcan<sup>2</sup>, Enes Begecarslan<sup>2</sup>, Irem Mutlukaya<sup>2</sup>,  
Kevin Gomez Buquerin<sup>3,5</sup>, Tina Volkersdorfer<sup>3,6</sup>, and Hans-Joachim Hof<sup>3</sup>

<sup>1</sup> TECNALIA Research and Innovation, Basque Research and Technology Alliance,  
Derio, Spain

{mario.rodriguez,joseangel.matute,joshue.perez}@tecnalia.com

<sup>2</sup> FEV Türkiye, Istanbul, Türkiye

{oezbay,tezcan,begecarslan,mutlukaya}@fev.com

<sup>3</sup> Technische Hochschule Ingolstadt, CARISSMA Institute of Electric, Connected and  
Secure Mobility (C-ECOS), Ingolstadt, Germany

{kevin.gomez,tina.volksdorfer}@carissma.eu, hans-joachim.hof@thi.de

<sup>4</sup> University of the Basque Country (UPV/EHU), Bilbao, Spain

<sup>5</sup> Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen, Germany

<sup>6</sup> Universität Passau, Passau, Germany

**Abstract.** In the context of Connected, Cooperative, and Automated Mobility (CCAM), precise ego-vehicle positioning and environmental status assessment are crucial. However, these tasks can be susceptible to sensor failures, misuse, and cyberattacks. Automation disengagements and system redundancy are common strategies to achieve Minimum Risk Conditions when failures occur. This paper presents a Fail-Safe decision architecture formulated within the framework of the SELFY project (<https://selfy-project.eu/>). The main aim is to reduce inaccuracies in GNSS-derived positioning through the incorporation of sensor fusion, AI-guided situational assessment, trajectory planning, and mode decision components. Additionally, the architecture has been designed to enable real-time updates and communication with external entities, including the Vehicle Security Operations Centre.

**Keywords:** CCAM · Fail-Safe · Fallback Strategy · Situational Awareness · Decision · Urban Scenarios

## 1 Introduction

Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS) have enhanced commercial vehicle safety in recent years. However, accurate localisation remains a critical challenge for Automated Vehicles (AVs) in urban environments, necessitating further research. Most systems rely on redundancy or disengagement in case of failures for risk mitigation [1].

The latest European Commission reports emphasize key developments in communication, cyber-security, onboard sensors, infrastructure, mobility concepts, and city contexts for urban transportation [2, 3]. ADAS and ADS employ various sensors, including cameras, Global Positioning System (GPS), and Light and Radio Detection and Ranging (LiDAR and RaDAR), for environmental perception. Perception tasks are critical for increasing automation in AVs developments, as environment recognition must be assured in any scenario. Moreover, their failure-tolerant operation during automated mode is crucial to ensure passenger safety, particularly in emergencies [4].

Some authors have considered sensor data fusion to enhance performance robustness in different contexts, including the perception of the environment [5], localization [6, 7], and traffic sign detection and recognition [8]. A detailed description of the most popular methods and techniques for performing data fusion has been explored. The authors conclude that the appropriate technique to be implemented depends on environmental conditions [9]. For example, the most widely used global localization approaches involve global navigation satellite systems. However, these systems have limitations in urban environments due to signal blockage or multipath effects. As a result, alternative localization techniques have been evaluated to address these limitations and improve performance in urban environments.

Research and development efforts are underway to determine when a vehicle should switch to fault-tolerant operation. The SELFY project [10] focuses on initiating this process, either through external commands (e.g., Vehicle Security Operations Centre) or by processing vehicle and infrastructure data (e.g., Vehicle-to-Everything messages). The next step involves selecting a suitable fallback strategy, considering potential failures caused by malfunctioning systems (e.g., electric or electronic devices), performance limitations, and misuse (e.g., sensor limitations, algorithm failures, user errors due to overload or confusion). Ultimately, the resulting fault-tolerant mode defines the system's capabilities [11].

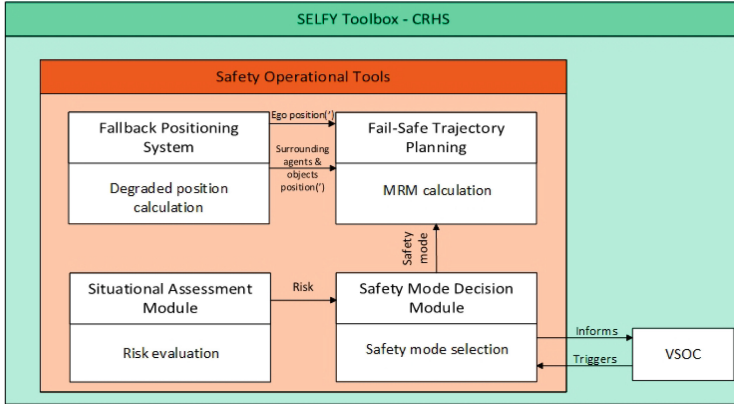
This work presents a fail-safe decision architecture for positioning failures of automated vehicles in urban scenarios. This architecture is based on the framework of the EU-SELFY project, which aims to increase AVs safety, security, robustness, and resilience.

## 2 Fail-Safe Decision Architecture in the SELFY Project

The proposed architecture, depicted in Fig. 1, is part of the Cooperative Resilience and Healing System (CRHS) Toolbox, which includes tools that elicit self-protection actions whenever a compromised situation is detected in relation to assets, vehicles, operations, or the system itself. These actions can be taken locally, or in cooperation with other tools in their environment so that decisions can be taken at the global Connected, Cooperative, and Automated Mobility (CCAM) level.

Overall, the architecture consists of four separate components, including positioning, situation assessment, safety mode decision, and path planning. The

architecture runs in parallel with the normal perception and decision modules and overwrites the path computed by the normal path planner when a localisation failure occurs. It can also receive and send status information to external entities.



**Fig. 1.** Fail-Safe Decision Architecture in the SELFY Project

## 2.1 Fallback Positioning System

This component in the global architecture provides an alternative solution to localization when the primary source, typically the Global Navigation Satellite System (GNSS), fails. It offers pose and twist estimations with covariance but is less precise. This solution is considered degraded but reliable enough for secure vehicle operation for several seconds.

The module relies on the Extended Kalman Filter (EKF), which blends the kinematic bicycle model of the vehicle with external localization sources, including the degraded GNSS signal with Inertial Measurement Unit (IMU) compensation, cooperative perception via Vehicle-to-X (V2X), and landmark-based localization methods. Mahalanobis gates are employed to reject the sensor and external localization sources that are more distant than the Mahalanobis distance with the kinematic bicycle model. The positioning system is an adaptation of the Autoware EKF localizer [12], which involves amendments to the vehicle model and the localization sources.

## 2.2 Situational Assessment Module

The Situational Assessment Module compares the environment model (fused from RSU and on-board vehicle sensor data), CAN messages from the ego vehicle, Cooperative Awareness Messages (CAM), analyses these data by using Artificial Intelligence-based methods to detect anomalies, misuse, malfunctions, etc.,

and decides the risk level of the current situation. The risk information is provided to the Safety Mode Decision Module.

A method based on distance estimation was developed to prevent GNSS loss or GNSS spoofing. For this method, latitude and longitude data from GNSS, speed and steering data from CAN, and forward acceleration data from IMU were used. These data were obtained by simulation driving in Carla and to calculate the distance between the two time intervals, the Haversine great circle formula, which calculates with latitude and longitude information, was used.

A Long Short-Term Memory (LSTM) model, which is a type of RNN, was used to estimate the distance. Since our algorithm is a sequence prediction problem, a LSTM is a proper model because of its capability of learning long-term dependencies. Speed, steering angle and forward acceleration were used as input data to train the LSTM. The output is the distance between two time intervals. After completing the training on the LSTM model, a fine-tuning operation was performed to enhance its performance and achieve higher accuracy. In pursuit of obtaining closer predictions and improving its capabilities, additional 2 hidden layers were added to the model architecture. By implementing these measures, the aim is to enhance the system's accuracy and performance by improving its capacity to capture intricate relationships. Following the fine-tuning operation, it was observed that the predicted distance values converged towards the actual values and an enhancement in accuracy was achieved. After the distance estimation is completed, a threshold distance value is set according to the vehicle's capacity and the error values in the GNSS signal. When the estimated value exceeds this threshold value, GNSS loss or spoofing is detected.

In addition to the LSTM model development, an innovative approach involving data manipulation techniques was used to further improve the model's robustness and anomaly detection capabilities. To simulate various anomaly scenarios, a custom function that introduces anomalies into the dataset by perturbing the GNSS latitude and longitude coordinates, creating inconsistent speed or acceleration values, and generating outliers in steering angle and speed was developed. These anomalies cover possible GNSS hacking, spoofing, or signal degradation scenarios.

A preliminary NN model was trained and designed as a binary classifier that aims to predict whether a given sample is normal or manipulated according to the provided features. While the simplicity of the neural network may limit its predictive capabilities, it still provides valuable insight into the overall impact of the data manipulation techniques. The successful differentiation of the NN model between normal and manipulated data encourages us to use it to refine and fine-tune the LSTM model for advanced anomaly detection, ultimately leading to a more sophisticated and accurate GNSS anomaly detection solution.

### 2.3 Safety Mode Decision Module

The Safety Mode Decision Module selects the most suitable operation mode according to the environmental circumstances and the ego-vehicle status. The algorithm is capable of switching between three modes of operation, including

*Normal Operation*, *Fail-Safe Operation*, and *Total Failure - Stop*. When engaged, the *Fail-Safe Operation* guides the vehicle towards a safe state, which may not always require an immediate stop. Depending on the situation and the availability of a suitable stop location nearby, the vehicle might have to continue driving for a brief period.

The algorithm is based on Fuzzy logic, considering various factors, including the risk evaluation from the Situational Assessment Module, median control errors, GNSS signal status, surrounding agent detection, and localization covariance. External entities can also trigger the available modes, and the module can provide periodic updates to these entities.

**Vehicle Security Operations Centre.** One entity that further utilizes the information from the fail-safe decision architecture is a Vehicle Security Operations Center (VSOC). Besides communication between cars and exchanging safety modes and risks, a VSOC can further utilize this data. A VSOC is responsible for collecting data from various sources within an environment. In the case of the SELFY project, the VSOC collects data from the CCAM, e.g., including all tools within the SELFY toolbox and OEMs or third-party services (e.g., threat intelligence providers and vulnerability databases). This overview allows the SELFY VSOC to picture the events within the SELFY ecosystem comprehensively. As a result, detecting vulnerabilities, anomalies, and cyber-security incidents becomes feasible. The VSOC utilizes the information from the safety operational tools to define risk values for the vehicle or a group of vehicles. Distributing the risk value can further increase knowledge between participants of the CCAM ecosystem. Implementing dedicated point-to-point communication methods is time-consuming and complex with all the technologies present in modern vehicles and their ecosystems. If the VSOC distributes this knowledge, a more open knowledge-sharing methodology is achieved. Only some participants need to implement a connection to other participants. Instead, a connection to the VSOC allows the tools to send relevant data to the VSOC and receive enriched information from it.

## 2.4 Fail-Safe Trajectory Planning

The last component in the architecture handles Minimum Risk Manoeuvre calculations. Utilizing emergency vehicle localization from the Fallback Positioning System, along with the positions of surrounding agents like vehicles and road users, as well as the initially planned trajectory and lane map data, it continuously computes the minimum risk manoeuvre. This new path is executed only when the *Fail-Safe Operation* is activated within the Safety Mode Decision Module. Under *Normal Operation*, the final path adheres to the originally planned trajectory.

The ultimate goal during *Fail-Safe Operation* is to perform a controlled stop at a suitable location, but this may not always be possible immediately. Longitudinally, the speed is reduced within the legal limits of the road. Laterally, the

calculated path is capable of lane changes, overtaking, and emergency stops, but larger safety margins are built-in and safety is given priority over comfort.

### Acknowledgements.



**Funded by  
the European Union**

This research has been funded by the European Union, through the Horizon Europe Transport programme, under grant agreement No. 101069748 - SELFY project. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

### References

1. Sari, B.: Fail-operational safety architecture for ADAS/AD systems. In: Fail-operational Safety Architecture for ADAS/AD Systems and a Model-driven Approach for Dependent Failure Analysis. WRFUS, pp. 31–75. Springer, Wiesbaden (2020). [https://doi.org/10.1007/978-3-658-29422-9\\_3](https://doi.org/10.1007/978-3-658-29422-9_3)
2. Eshetu, A.A., Valilai, O.F., Wicaksono, H.: European CCAM Outlook 2023: a review of CCAM advancements and applications in Europe's public transport sector (2023)
3. European Climate Infrastructure and Environment Executive Agency (CINEA). Towards cooperative, connected and automated mobility: Contributions of horizon Europe projects managed by CINEA (2023)
4. Thorn, E., Kimmel, S.C., Chaka, M.: A framework for automated driving system testable cases and scenarios (2018)
5. Fayyad, J., Jaradat, M.A., Gruyer, D., Najjaran, H.: Deep learning sensor fusion for autonomous vehicle perception and localization: a review. *Sensors* **20**(15), 4220 (2020)
6. Matute, J., Rodríguez-Arozamena, M., Perez, J., Karimoddini, A.: Sensor fusion-based localization framework for autonomous vehicles in rural forested environments. In: IEEE 26th International Conference on Intelligent Transportation Systems (ITSC) (2023)
7. Meng, X., Wang, H., Liu, B.: A robust vehicle localization approach based on GNSS/IMU/DMI/LIDAR sensor fusion for autonomous vehicles. *Sensors (Switzerland)* **17**(9), 2140 (2017)
8. Saadna, Y., Behloul, A.: An overview of traffic sign detection and classification methods. *Int. J. Multimedia Inf. Retrieval* **6**(3), 193–210 (2017). <https://doi.org/10.1007/s13735-017-0129-8>
9. Yeong, D.J., Velasco-Hernandez, G., Barry, J., Walsh, J.: Sensor and sensor fusion technology in autonomous vehicles: a review. *Sensors* **21**, 1–37 (2021)
10. SELFY EU Project: Self assessment, protection & healing tools for a trustworthy and resilient CCAM (2022). <https://selfy-project.eu/>
11. Stolte, T., et al.: Taxonomy to unify fault tolerance regimes for automotive systems: defining fail-operational, fail-degraded, and fail-safe. *IEEE Trans. Intell. Veh.* **7**(2), 251–262 (2021)
12. Autoware: Autoware universe (2023). <https://github.com/autowarefoundation/autoware.universe>. Accessed 23 Aug 2023

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

