EVENTS

ReliablE in-Vehicle pErception and decisioN-making in complex environmenTal conditionS

Grant Agreement Number: 101069614

D4.4 Fail-safe Vehicle Control

Document Identification			
Status	Final	Due Date	31/08/2024
Version	1.0	Submission Date	18/12/2024
Related WP	WP4	Document Reference	D4.4
Related Deliverable(s)	D4.1, D4.2 & D4.3	Dissemination Level	PU
Lead Participant	CRF	Document Type:	Other
Contributors	All WP4 partners	Lead Authors	Fabio Tango (CRF)
		Reviewers	Leonardo Gonzalez (TECN)
			Barys Shyrokau (TUD)

Funded by the European Union

This project has received funding under grant agreement No 101069614. It is funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Document Information

Author(s)		
First Name	**Last Name**	**Partner**
Asier	Arizala	TECN
Oscar	de Groot	TUD
Alberto	Bertipaglia	TUD

Document History			
Version	**Date**	**Modified by**	**Modification reason**
0.1	15/07/2024	CRF	Empty document with section structure
0.2	01/12/2024	TUD	Received and incorporated contributions from TUD
0.3	02/12/2024	TECN	Received and incorporated contributions from TECN
0.4	04/12/2023	CRF	Version ready for review
0.5	13/12/2024	TECN	Review received from TECN
0.6	14/12/2024	TUD	Review received from TUD
0.7	17/12/2024	CRF	Merging reviews and preparing final document
1.0	18/12/2024	ICCS	Final submission

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	Leonardo Gonzalez (TECN)	10/12/2024
Quality manager	Panagiotis Lytrivis (ICCS)	17/12/2024
Project Coordinator	Angelos Amditis (ICCS)	18/12/2024

Executive Summary

This report includes the outcome of WP4/T4.3, that is the respective control commands for the subject vehicle based on the results of motion planning, taking especially into account the minimum risk manoeuvre in critical situations (e.g., fails of perception system, wrong decision of the CAV, no response within the due time of driver to a take-over request, and so on). In more detail, the outcomes of Task 4.1 and Task 4.2 are integrated with the concept of fail-safe control commands for the CAV. Based on the output of the perception self-assessment component (T3.5) and the estimated risk bounds for planned trajectories (T4.1), an automated emergency action can be performed (fall-back strategy).

Fail-safe control in AD refers to mechanisms and strategies designed to ensure that a vehicle remains safe in the event of system failures, errors, or unexpected situations. Thus, these systems must prioritize safety above all, in order to prevent accidents or to reduce the impact of hazardous situations. It is worth to noting that it may be difficult to find a fail-safe plan that works in all cases. For example, braking can work in many cases, but can also lead to collisions or dangerous situations when performed at the wrong time. Therefore, the idea followed in this report is to decrease the complexity of the possible solution to assure the robustness and the efficacy (even if this can imply a minor number of covered scenarios).

Table of Contents

List of Tables

List of Figures

Abbreviations & Acronyms

Abbreviation / acronym	Description
ACC	Adaptive Cruise Control
AD(F)	Autonomous Driving (Function)
AI	Artificial Intelligence
AL	Alert Limit
AV	Automated Vehicle
BP	Behavioural Planner
CA	Consortium Agreement
CAM	Cooperative Awareness Message
CAV	Connected Automated Vehicle
CPM	Collective Perception Messages
DDT	Dynamic Driving Task
DENM	Decentralized Environmental Notification Message
DM	Decision Making
EC	European Commission
EXPs	Experiments
FIS	Fuzzy Inference System
FoV	Field of View
FTP	Fail-degraded Trajectory Planning
GA	Grant Agreement
IR	Integrity Risk
ISO	International Organization for Standardization
I/O	Input(s) / Output(s)
LiDAR	Light Detection and Ranging
MDP	Markov Decision Process
MPC	Model Predictive Control
MRM	Minimum Risk Manoeuvre
MOP	Moving Object Prediction
MOT	Multi-Object Tracking

Abbreviation / acronym	Description
ODD	Operational Design Domain
PE	Position Error
PL	Protection Level
PP	Perception Platform
RADAR	RAdio Detecting And Ranging
REQs	Requirements
RL	Reinforcement Learning
SAE	Society of Automotive Engineers
SMD	Safety-mode Decision
SoTA	State of the art
SPaT message	Signal Phase and Timing message
SPECs	Specifications
TOR	Take Over Request
TP	Trajectory Planner
TSs	Target Scenarios
UCs	Use Cases
VRU	Vulnerable Road User
WP	Work Package

1. Introduction

This document follows the structure of all the other deliverables, namely, an introduction with the aim of the project and scope of the document; then follows the main body, with the specific topic of the document. The content is divided by experiments (EXPs), even if, in this case, the focus is only on EXP1, EXP2 and EXP4/5 due to the limited efforts and the number of partners involved.

1.1 Project aim

Driving is a challenging task. In our everyday life as drivers, we are facing unexpected situations we need to handle in a safe and efficient way. The same is valid for Connected and Automated Vehicles (CAVs), which also need to handle these situations, to a certain extent, depending on their automation level. The higher the automation level is, the higher the expectations for the system to cope with these situations are.

In the context of this project, these unexpected situations where the normal operation of the CAV is close to be disrupted (e.g., ODD limit is reached due to traffic changes, harsh weather/light conditions, imperfect data, sensor/communication failures, etc.), are called “events”. EVENTS is also the acronym of this project.

Today, CAVs are facing several challenges (e.g., perception in complex urban environments, Vulnerable Road Users (VRUs) detection, perception in adverse weather and low visibility conditions) that should be overcome to be able to drive through these events in a safe and reliable way.

Within our scope, and, to cover a wide area of scenarios, these kinds of events are clustered under three main use cases: a) Interaction with VRUs, b) Non-Standard and Unstructured Road Conditions and c) Low Visibility and Adverse Weather Conditions.

Our vision in EVENTS is to create a robust and self-resilient perception and decision-making system for AVs to manage different kinds of “events” on the horizon. These events result in reaching the AV ODD limitations due to the dynamically changing road environment (VRUs, obstacles) and/or due to imperfect data (e.g., sensor and communication failures). The AV should continue and operate safely no matter what. When the system cannot handle the situation, an improved minimum risk manoeuvre should be put in place.

1.2 Deliverable scope and content of the Document

In the EVENTS project, WP4’s main goals are to design and implement the on-board decision-making and control algorithms of EVENTS use cases, considering complex traffic and environmental conditions, especially around critical zones, where potential contradictions to existing traffic rules can emerge, or the environment is unstructured

[1]. In particular, this deliverable – referred to task T4.3 – translates the outcomes of Tasks T4.1 and T4.2, which are the motion planning and the behavioural decision-making, into fail-safe control commands for the CAV. Based on the output of the perception self-assessment component (T3.5) and the estimated risk bounds for planned trajectories (T4.1), an automated emergency action will be performed (fall-back strategy). This one can become a minimum risk manoeuvre (MRM), in case of critical situations, such as failure of the perception system, wrong / dangerous decision-making from the automation, no answer or too late answer to a take-over request (TOR) from the CAV, and so forth. Based on the state of the art, the method used will be a model-based controller, which considers a prediction horizon (MPC), which could be tuned by a more sophisticated state of the art (SOTA) algorithm, such as reinforcement learning.

The document is structured as follows. After this introduction, Section 2 describes the implementations on the prototype vehicles, for the selected experiments. Finally, Section 3 presents the conclusions of the progress mentioned previously, including a summary of the document and possible lessons learnt.

2. Fail-safe Control for the selected EXPs

In the context of WP4, T4.3 deals with the "fail-safe control" of the prototype vehicles. First, it is important to define what a fail-safe control is. Fail-safe control in autonomous driving refers to mechanisms and strategies designed to ensure that a vehicle remains safe in the event of system failures, errors, or unexpected situations. These systems prioritize safety above all else, aiming to prevent accidents or reduce the impact of hazardous situations, an approach also described in deliverable D2.3 (Vehicle System Hazard Analysis & Risk Assessment) [10]. Some of these situations can be, sensor malfunctions, actor failures, software errors, power loss or communication breakdowns. Note that fail-safe strategies can be proposed at different levels in the autonomous vehicle architecture. Sensor fusion fallback provides redundancy to deal with sensor malfunctions, brake-by-wire systems ensure mechanical braking in case of electronic control failure and fallback localization uses odometry when GPS or high-definition maps are unavailable.

Thanks to the inputs provided by WP3, the goal in this task is to generate a fail-safe trajectory, that is, the "minimum-risk manoeuvre" to perform (e.g., safe lane-change in the emergency lane, stop at a safe distance from the obstacle ahead etc.). Figure 1 shows the different connections among the tasks in WP4, pointing out the inputs and outputs for T4.3:

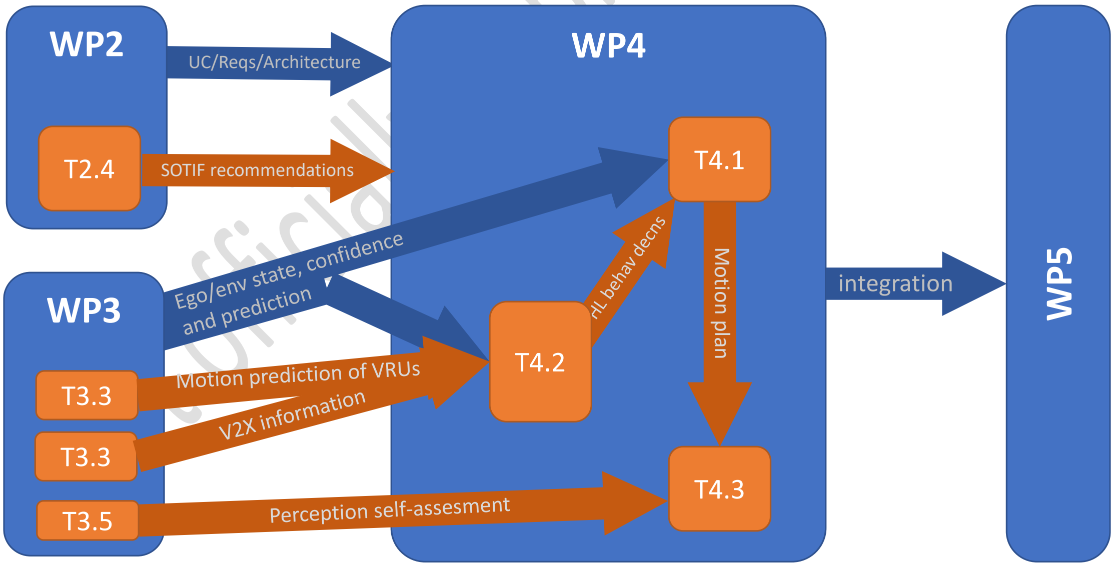

Figure 1: sketch of the WP4 interactions (in a graphical way).

The outputs of T4.3 "Fail-safe Vehicle Control" can be used by the automated system in case a (very) critical/dangerous situation occurs.

As mentioned in the previous section, based on the state of the art, the method used is a model-based controller, which considers a ***prediction horizon*** (MPC), which will be tuned by a more sophisticated SOTA algorithm, such as reinforcement learning.

In the following paragraphs, the developed algorithms are presented in detail for experiments EXP1, EXP2, EXP4 and EXP8.

2.1 EXP1

Experiment 1 (EXP1) "*Interaction with VRUs in complex urban environment*" is under the responsibility of Delft University of Technology. EXP1 is about safe, comfortable and time-efficient automated driving in complex urban environment while interacting with VRUs (e.g., pedestrians, cyclists).

This section describes the architecture of the fail-safe motion planner. In general, it is challenging to find a fail-safe plan that works in all cases. For example, braking may work in many cases but can lead to collisions when performed at the wrong time. The motion planner should, therefore, take obstacles into account when computing a fail-safe plan.

In Deliverable 4.3 [4], a topology-driven guidance planning strategy as well as a behavioural decision-making component have been introduced that were tightly coupled with motion planning. The guidance planner gives back trajectories that pass obstacles on different road sides, left or right overtaking. This strategy may not compute trajectories that brake for the obstacles, which in the context of fail-safe planning is desired. Hence, the guidance planner is enhanced with a topological measure that can distinguish between passing and non-passing trajectories, such as overtaking or brake scenarios. The main idea is that one or more trajectories are concurrently optimized that are braking to stop before obstacles so that if the other behaviours are not feasible, then one of the fail-safe trajectories is executed. If other behaviours are feasible, then fail-safe trajectories will be ignored because they are relatively slow, leading to a higher cost.

This implementation uses a topological measure to distinguish high-level trajectories. It filters out trajectories with identical behaviours so that its outputs are distinct. For fail-safe behaviour, angles with winding numbers are implemented [2] as a topological measure. Such angles measure how far and in which direction the vehicle rotates around obstacles. With the relative position of an obstacle j (with position $\boldsymbol{o}_k^j$ at time step k) and the vehicle (with position $\boldsymbol{p}_k$ at time step k) given by $\boldsymbol{d}_k^j = \boldsymbol{p}_k - \boldsymbol{o}_k^j$. The angle θ_k^j can be computed and the change in this angle as $\Delta\theta_k^j = \theta_{k+1}^j - \theta_k^j$,

The angle is then computed as:

$$\lambda^j = \frac{1}{2\pi}\sum_{k=1}^{N}\Delta\theta_k^j$$

The absolute value of the angle $|\lambda^j|$ determines how far the vehicle has overtaken the obstacle. The sign indicates in which orientation the obstacle has been overtaken. With the sign of the angle (i.e., to distinguish between left and right overtaken trajectories), the absolute value can be used to determine whether a trajectory overtakes the obstacle or not.

The implementation considers high-level trajectories distinct if they result in left or right overtake manoeuvres or if no overtake opinion is available and there is a need for a fail-safe strategy. The two distinct trajectories (blue lines) and the fail-safe trajectory (red line) are shown in Figure 3. Each distinct trajectory returned by the behavioural decision-making component, up to a limit, is optimized by the motion planner as described previously. The fail-safe trajectory results in a braking scenario to avoid collision with the obstacle, whereas the other two trajectories steer around the obstacle.

Figure 2: example of overtaking and fail-safe braking scenarios.

The fail-safe trajectory brakes to avoid collision with the obstacle, whereas the other two trajectories steer around the obstacle.

To verify the fail-safe strategy, an environment consisting of a two-lane road, where four pedestrians are crossing, was used. The pedestrians are randomly spawned in each scenario, but the same for different planners. The simulation environment uses the Autoware Planning Simulation [3] adapted for EXP1 real-world map and vehicle.

In this environment, the planner with and without fail-safe topological measure has been compared, using the task duration (time for the vehicle to reach the goal), number of collisions, timeouts (how often the vehicle did not reach the goal) and average velocity. The results of 25 experiments per planner are shown in Table 1 showing the comparison between T-MPC++ with and without fail-safe in a scenario with four crossing pedestrians. The metrics used in Table 1 are the duration of the task [mean (std)], collisions, timeouts and average velocity of both methods.

Pedestrians	Method	Dur. [s]	Collisions	Timeouts	Avg. Velocity [m/s]
4	T-MPC++ (no fail-safe)	24.2 (4.8)	3	1	1.56
	T-MPC++	**21.0 (1.7)**	**0**	**0**	**1.78**

Table 1: simulation results.

The results indicate that the fail-safe strategy reduces the number of collisions and, therefore, allows the task to be completed faster.

2.2 EXP2

EXP2, called “*Re-establish platoon formation after split due to roundabout*”, led by TECNALIA partner makes use of via V2X information for a successful integration. In this experiment a platoon can be split because of traffic when approaching and crossing a roundabout[1]; then, the followers must be able to reach the leading vehicles while also ensuring string stability under curved trajectories.

2.2.1 Architecture

When it comes to software level fail safe motion planning strategies there are several approaches in the state of the art. Some works propose generating safe trajectories that fully stop the vehicle without entering the probabilistic occupancy set of a leading vehicle in case a feasible trajectory does not exist [5][6]. Others consider the possibility of the trajectory generator problem being too demanding to get a valid trajectory in real-time. In[7] a nonlinear MPC with several constraints is proposed for lateral control, prioritizing optimality above efficiency in the control, thus they make use of a relaxed MPC solution as backup. In [8] the authors address the dependency of lateral and longitudinal controllers to IMU readings, specially angular velocity, so a control switch is designed to choose between a yaw-rate dependent nonlinear control law and a yaw-rate independent controller with slightly lower control performance.

In this work a control switch combining approaches in [7] and [8] is proposed where a switch is used to address an MPC lateral controller possible delays. The less optimal control strategy adopted in this case is a feedback proportional control acting upon lateral and angular error of the vehicle against the centre of the lane, a.k.a. a PID-like controller.

[1] Driving rules in the roundabout are assumed to prioritize the vehicles inside the roundabout.

The figure represents the idea behind this work, where control switch receives both steer outputs from the MPC and the PID-like controller.

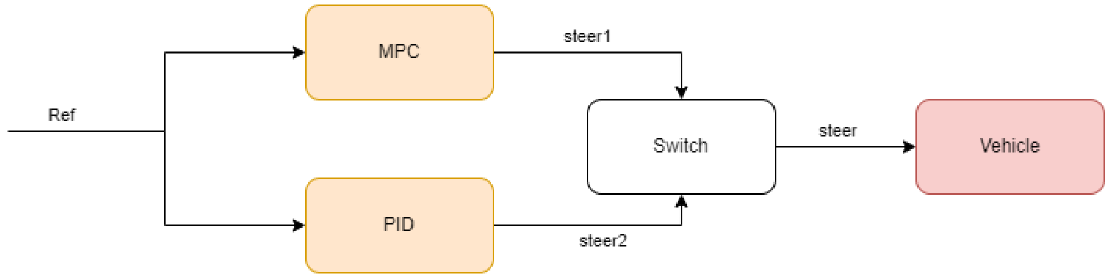

Figure 3: EXP2 control switch.

2.2.2 Algorithmic approach

The next two paragraphs will show the control switch and model, with the details on the related algorithms.

Control Switch

The short period of time after a switch is crucial since the discontinuity in the control signal can lead to undesired transients in the system. In [8] a bump function is proposed to smooth the control switch using the steer values of both controllers. In our case, however, one of the control values will not be available during the control switching. Therefore, the smoothing function proposed uses the previous steering information:

$$\delta = (1 - \kappa(\alpha))\delta(k-1) + \kappa(\alpha)\delta(k)$$

where the bump function is:

$$\kappa(\alpha) = 1 - e^{-\frac{\alpha^2}{1-\alpha^2}}$$

and α is a time dependent function where:

$$\alpha(t) = \frac{t}{T_{shift}}, \qquad if\ \alpha > 1\ then\ \alpha = 1$$

T_{shift} is the transition time from one controller to another. The condition to use the MPC controller back is set to receive a number n of steering messages at an admissible maximum rate of f_{mpc} frequency.

Control Models

As mentioned before, two controllers are being used for this experiment. The MPC controller uses a simple kinematic vehicle model composed by three state variables and two input variables:

$$X = \{x, y, \theta\}^T, U = \{\delta, v\}^T$$

The position of the vehicle in cartesian coordinates framed to the initial state of the vehicle $P = (x, y)$ and the orientation θ. Inputs of the model are the steering of the wheels δ and vehicle longitudinal speed v. The state derivative is given in the following equation:

$$\dot{x} = \begin{cases} v\cos(\theta + \beta) \\ v\sin(\theta + \beta) \\ v\cos(\beta)\dfrac{\tan(\delta)}{L} \end{cases}$$

, where β is the sliding angle of the control point:

$$\beta = \operatorname{atan}\left(\frac{l_r tan(\delta)}{L}\right)$$

l_r being the distance between the rear axle and the control point and L the wheelbase of the vehicle.

The minimization function can be written as:

$$\min(J(\mathrm{X}, U)) = \int_{i=0}^{H} w_{dist} d_{ref}^2 + w_{orient}\theta_{dif} + w_{steer}\delta^2 + w_{acc}v^2$$

$$\text{s.t.} \qquad \begin{gathered} \delta_{min} < \delta < \delta_{max} \\ 0 < v < v_{max} \end{gathered}$$

Minimizing the distance to the reference path d_{ref}, the orientation difference δ_{dif} and control variations. No further constraints are considered due to wanting to boost control efficiency.

The second controller uses a simple gain based weighted sum of lateral and orientation error from a control point to the reference.

$$\delta = w_{lat}e_{lat} + w_{orient}e_{orient}.$$

2.3 EXP4

EXP4 is carried out by TECNALIA and University of Warwick partners and its title is “Decision making for motion planning when faced with roadworks, unmarked lanes and narrow roads with assistance from perception self-assessment”. The objective of the EXP4 is to navigate in an unstructured road wide enough for at least two vehicles driving in parallel and with occasional disturbances, like roadworks. The challenge regarding behavioural planning is the selection of a collision free path within the boundaries of the roads in real time.

In this case, a similar analysis of the fail-safe control in the EXP2 can be applied. Nonetheless, a different approach is considered due to the specific conditions that roadworks impose to the scenario. Unstructured roads do not usually have a representative map of lanes. Therefore, a coherent and feasible reference needs to be computed beforehand as the control input. This applies to situations where maps are no longer reliable due to roadworks, since the trajectory generation becomes highly dependent on the perception module.

In this case we leverage the redundancy of systems, since a fail-save behaviour is managed in the control module. Therefore, no path modification for Minimum Risk Manoeuvres (MRM) are considered. Instead, system fails are handled through control redundancies and emergency MRM.

2.3.1 Algorithmic approach

The possibility of the trajectory generation NMPC failing is considered in the lateral control by allowing the use of the suboptimal B-spline as backup. This way a reference for the control is ensured in real time (Figure 4).

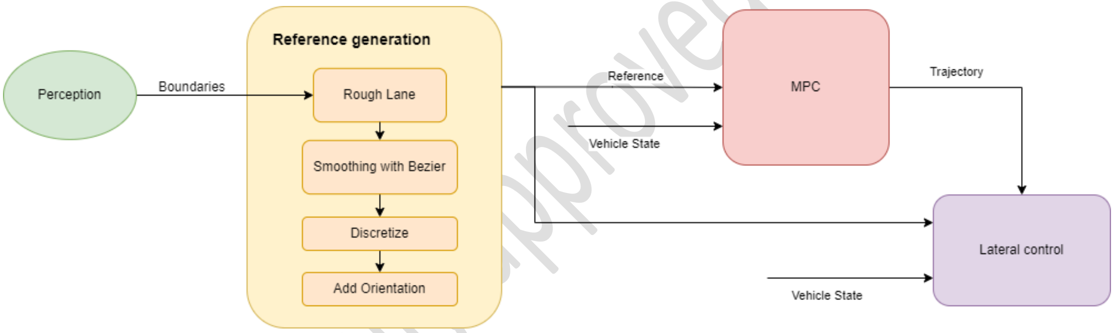

Figure 4: EXP4 Lateral control fail-safe design.

If borders are no longer detected, the control enters in a degraded state and stops the vehicle within a maximum deceleration value, maintaining straight steering. The longitudinal control is calculated from:

$$v_{ref} = v - a_{decel}\, t, if\ v_{ref} < v_{traj}$$

v_{traj}, being the speed assigned to the last trajectory received.

Other system errors make the vehicle perform an MRM as close to the last reading of the border as possible.

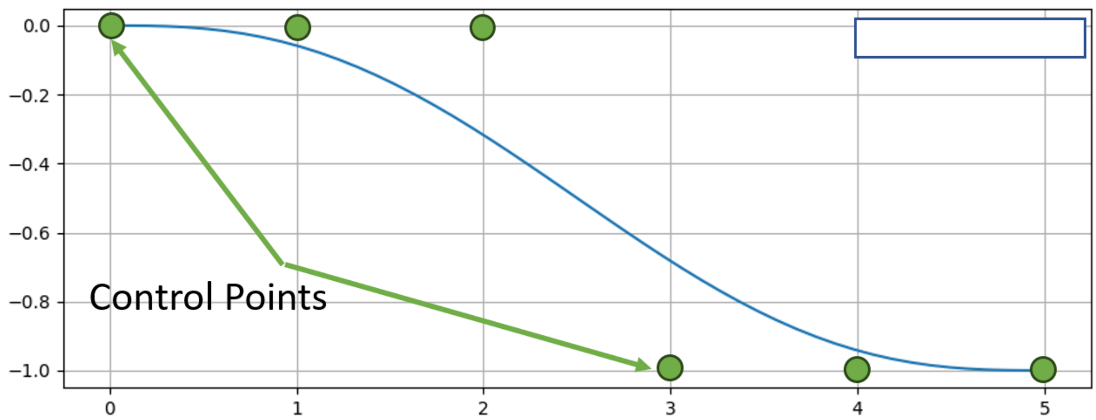

Figure 5: EXP4 MRM trajectory.

The trajectory for that manoeuvre is generated in the control module with a quintic Bezier curve using the control points configuration presented in the 4.1 task (see the related figure above). Thus, ensuring feasibility through continuous curvature along the path.

2.4 EXP8

Experiment 8 (EXP8) is "*Emergency evasion manoeuvre on the slippery roads under rain conditions*". The objective is to perform collision avoidance (e.g. pedestrian, cyclist or vehicle) in poor weather conditions on slippery roads. EXP8 is under the responsibility of the TUD.

Similar fail-safe strategies to the ones used for the previous experiment (EXP1) can also be used for EXP8. However, the fail-safe control for EXP8 is tailored specifically for emergency evasion manoeuvres on slippery roads during rainy conditions. The complexity of this scenario lies in the heightened risk of losing stability under such adverse conditions. To address this, the fail-safe controller prioritizes acting on the longitudinal dynamics rather than the lateral dynamics of the vehicle. Therefore, the proposed fail-safe strategy focuses on hard braking to stop the vehicle as quickly as possible, thereby reducing the likelihood of collisions or instability.

2.4.1 Algorithmic approach

A key principle of fail-safe design is the incorporation of redundancy. The additional longitudinal dynamic controller has been introduced that activates if the proposed controller for EXP8 fails to converge in time or becomes infeasible. This fail-safe controller utilizes a PID-based approach to track a reference longitudinal velocity, calculated as the maximum longitudinal acceleration a vehicle can sustain under an assumed road friction coefficient of 0.5 (see Figure 8.1).

If the proposed MPC fails to converge or becomes infeasible, the reference velocity is recalculated based on the maximum achievable deceleration using the following equation:

$$v_{ref} = v_{veh} - a_{bra}\,\Delta t, if\ v_{veh} > 0$$

Where v_{ref} is the reference velocity that the fail-safe controller will track, v_{veh} is the current vehicle velocity, Δt is the control sampling time and the a_{bra} is the desired braking acceleration computed as follows:

$$a_{bra} = SF\ \mu\ g$$

Where SF is a safety coefficient, assumed equal to 0.9 that compensates for errors in road friction (μ) estimation and g is the gravitational acceleration.

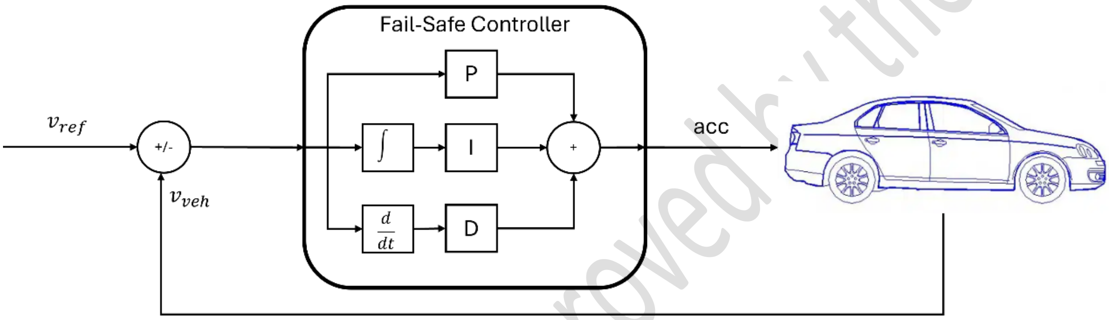

Figure 6: the scheme of the fail-safe controller.

The example of the vehicle decelerating in a braking manoeuvre with a road friction coefficient of 0.5 and a safety coefficient of 0.9 are shown in the following figures.

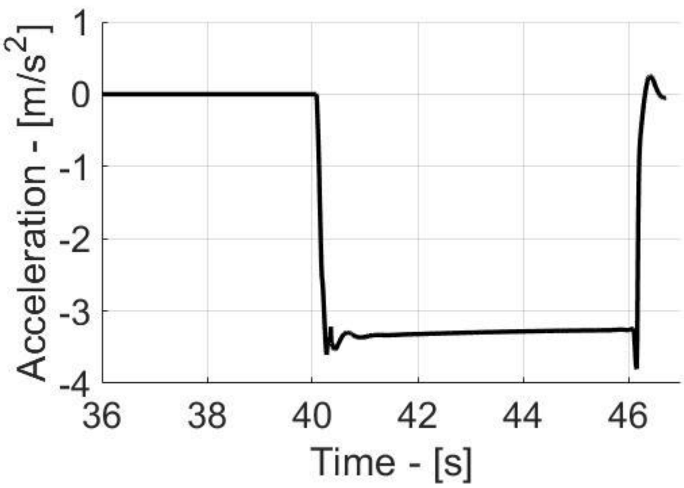

Figure 7: profile of vehicle deceleration.

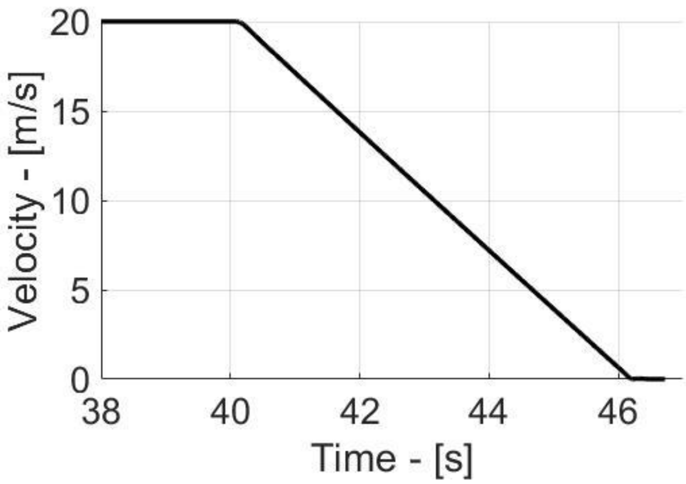

Figure 8: profile of vehicle velocity.

3. Conclusions

This section presents the final remarks of this document. Deliverable D4.4 aims at including the outcome of T4.3, which is the respective control commands for the subject vehicle, based on the results of motion planning. In particular, the outcomes of Task 4.1 and Task 4.2 are integrated with the concept of fail-safe control commands for the CAV [9]. Based on the output of the perception self-assessment component (T3.5) and the estimated risk bounds for planned trajectories (T4.1), an automated emergency action will be performed (fall-back strategy).

Talking about fail-safe control in autonomous driving refers to mechanisms and strategies designed to ensure that a vehicle remains safe in the event of system failures, errors, or unexpected situations. Thus, these systems must prioritize safety above all, in order to prevent accidents or to reduce the impact of hazardous situations (such as sensor malfunctions, actor failures, software errors, power loss or communication breakdowns). It is worth noting that it may be difficult to find a fail-safe plan that works in all cases. For example, braking can work in many cases, but can also lead to collisions or dangerous situations when performed at the wrong time.

In general, fail-safe strategies can be proposed at different levels in the autonomous vehicle architecture. Sensor fusion fallback provides redundancy to deal with sensor malfunctions, brake-by-wire systems ensure mechanical braking in case of electronic control failure and fallback localization uses odometry when GPS or high-definition maps are unavailable, the motion planner should take obstacles into account when computing a fail-safe plan, and so forth.

The idea followed in this report is to decrease the complexity of the possible solution (e.g., from using the MPC to adopting a simpler PID algorithm) to assure the robustness and the efficacy, even if this implies to cover fewer complex situations and a minor number of scenarios (but able to guarantee the safe operation of the ADF, also in edge conditions). Moreover, it is important to point out that some experiments have the fail-safe approach at the trajectory generation stage, in order to enhance again the robustness of the proposed solutions.

References

[1] *EVENTS Deliverable D2.1: User and system requirements for selected use cases,* 2023.

[2] *M. A. Berger, "Topological Invariants in Braid Theory," Letters in Mathematical Physics, vol. 55, no. 3, pp. 181–192, Mar. 2001, doi: 10.1023/A:1010979823190.*

[3] *https://autowarefoundation.github.io/autoware-documentation/main/tutorials/ad-hoc-simulation/planning-simulation.*

[4] *EVENTS Deliverable D4.3: Behavioural decision-making, 2024*.

[5] S. R. Venkita, B. Boulkroune, A. Mishra and E van Nunen. "*A fault tolerant lateral control strategy for an autonomous four wheel driven electric vehicle*". 2020 IEEE Intelligent Vehicles Symposium (IV).

[6] M. Ammour, R. Orjuela, M. Basset. "*A MPC combined decision making and trajectory planning for autonomous vehicle collision avoidance*". IEEE Transactions on Intelligent Transportation Systems, vol. 23, pp. 24805–24817, 2022.

[7] C: Pek and M. Althoff. "*Fail-safe motion planning for online verification of autonomous vehicles using convex optimization*". IEEE Transactions on Robotics, vol. 37z, pp. 798–814, 2020.

[8] S. Magdici and M. Althoff. "Fail-safe motion planning of autonomous vehicles". 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, pp. 452-458, 2016.

[9] Matute-Peaspan, J. A., Perez, J., & Zubizarreta, A. (2020). A Fail-Operational Control Architecture Approach and Dead-Reckoning Strategy in Case of Positioning Failures. Sensors, 20(2), 442.

[10] *EVENTS Deliverable D2.3: Vehicle System Hazard Analysis & Risk Assessment,* 2023.