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

Grant Agreement Number: 101069614

D.2.3 Vehicle System Hazard Analysis & Risk Assessment

Document Identification			
Status	Final	**Due Date**	31/08/2023
Version	1.0	**Submission Date**	31/08/2023
Related WP	WP2	**Document Reference**	D2.3
Related Deliverable(s)	D.2.1, D2.2	**Dissemination Level**	PU
Lead Participant	APTIV	**Document Type:**	R
Contributors	All Task 2.4 partners	**Lead Authors**	Yogesh Ganesh, APTIV
		Reviewers	Anastasia Bolovinou, ICCS
			Siddartha Kashgir, WMG

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.

Author(s)		
First Name	**Last Name**	**Partner**
Yogesh	Ganesh	APTIV
Mariat	James Elizebeth	WMG
Bill	Roungas	ICCS
Anthony	Ohazulike	HIT-FR
Alireza	Ahrabian	HIT-UK
Dariu	Gavrila	TUD

Document History			
Version	**Date**	**Modified by**	**Modification reason**
0.1	14/03/2023	APTIV	Initial version.
0.2	02/05/2023	APTIV	Added control structure
0.3	17/07/2023	APTIV	Finalizing HARA report
0.4	09/08/2023	APTIV	Complete D2.3 report
0.5	25/08/2023	APTIV	Integrating review comments
1.0	31/08/2023	ICCS	Final Approval

Quality Control		
Role	**Who (Partner's short name)**	**Approval Date**
Deliverable Leader	Yogesh Ganesh (APTIV)	30/08/2023
Quality manager	Panagiotis Lytrivis (ICCS)	31/08/2023
Project Coordinator	Angelos Amditis (ICCS)	31/08/2023

Executive Summary

The “D2.3: Vehicle system hazard analysis & risk assessment” deliverable is a public report of the EVENTS project, dealing with the risks and potential hazards associated with each use case by performing a Risk Assessment and Hazard Analysis (HARA) process. The approach taken in this work proposes a hybrid scheme that integrates STPA analysis with classical HARA.

The safety analysis findings are then used to formulate safety goals that are required to be met, in order for each vehicle system to operate safely within its ODD.

Work on Task 2.4 is based on the use case specification including ODD definition (mainly level of automation, road types and required infrastructure), the expected use-case exposure as well as the system architecture provided by the previous tasks.

Acceptance criteria, which are used to measure/assure safety of the intended function (SOTIF) of an autonomous vehicle or advanced driver assistance system (ADAS), are provided for the European roads. These initial performance goals will feed the development work of WP3 (Perception and self-assessment) and WP4 (On-board decision-making for fail-safe automated vehicle motion), where a list of reasonably quantified SOTIF events will be provided based on simulation testing, which in turn will feed the work on vehicle system safety compliance verification on Task T5.3.

Table of Contents

List of Tables

List of Figures

Abbreviations & Acronyms

Abbreviation / acronym	Description
ACC	Adaptive Cruise Control
AD(F)	Autonomous Driving (Function)
ADS	Autonomous Driving System
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
FSC	Functional Safety Concept
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

Abbreviation / acronym	Description
MOP	Moving Object Prediction
MOT	Multi-Object Tracking
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
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

Assuring safety is important in autonomous vehicles. The safety related to autonomous vehicles can be primarily viewed from two perspectives [6]: the functional safety (FuSa) and the safety of the intended functionality (SOTIF). While FuSa ensures the system has an acceptable risk with respect to malfunctions of electrical and electronic components, SOTIF ensures the system has an acceptable risk with respect to functional insufficiencies and performance limitations. SOTIF also considers expected system misuse, touching on cybersecurity aspects; however, such aspects are considered out of the project focus and will not be covered by this work.

With the growing complexity of automotive systems and the integration of advanced technologies, ensuring functional safety is of utmost importance. ISO 26262 [1], the international standard for functional safety in the automotive industry, provides a structured framework to address these safety challenges. In ISO 26262, the concept of *HARA* (Hazard Analysis and Risk Assessment) is introduced for system safety assessment during the concept phase of the system. HARA is an integral part of the functional safety process since it serves as the foundation for identifying potential hazards and assessing their associated risks. It involves a rigorous examination of potential failure modes, their causes, and the severity of their consequences on vehicle occupants, other road users, and the environment. Once HARA is completed, functional safety requirements are created and all the findings are aggregated into a functional safety concept. Works that augment HARA with scenario-based analysis or replace HARA with alternatives more suitable for AD systems have recently appeared [7].

2. Methodology

This project combines two analysis methods, namely HAZOP and STPA to generate a list of hazards and based on this, the safety analysis results.

2.1 Method 1: Hazard and Operability Study

HAZOP (Hazard and Operability Study) is a systematic and structured approach used in industries such as chemical, petrochemical, and manufacturing to identify potential hazards and operability issues in processes, systems, and equipment. The classical HAZOP approach has several advantages:

1. Comprehensive Hazard Identification
2. Structured and Systematic
3. Team Collaboration
4. Risk Assessment
5. Early Identification of Hazards

Figure 1 illustrates the analytical steps of the HAZOP study.

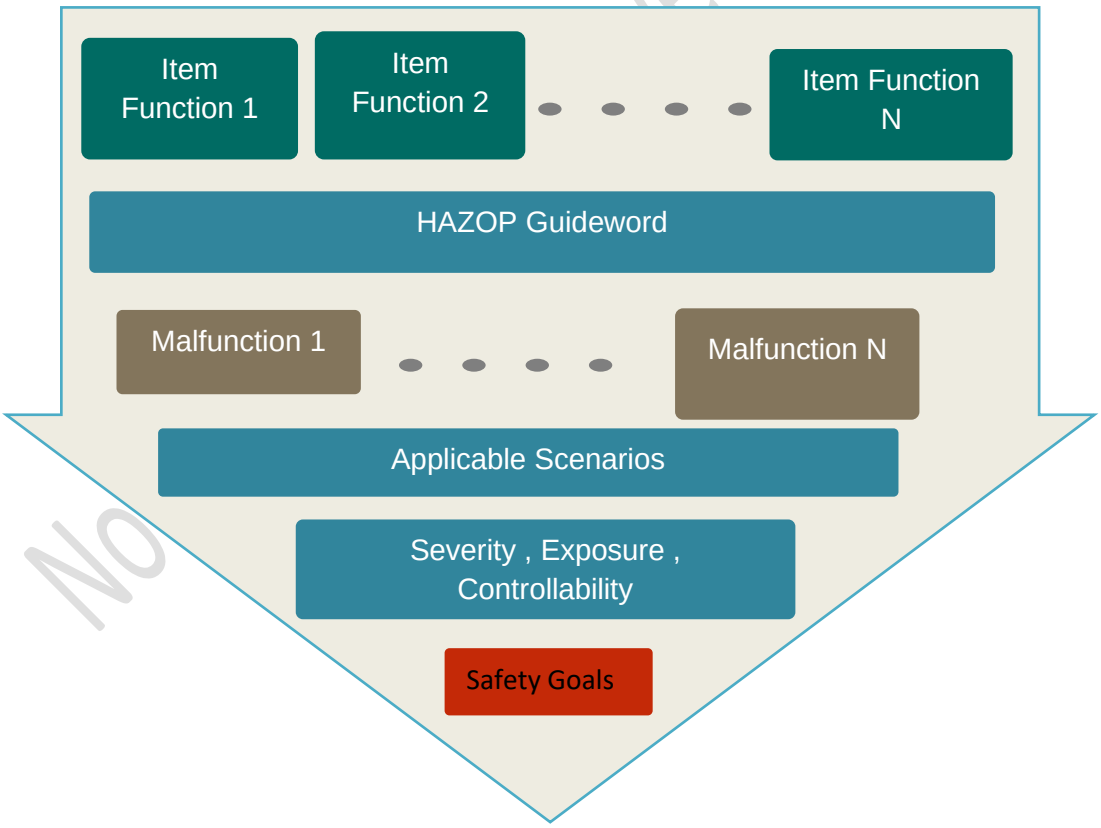

Figure 1: HAZOP Steps

This study applies the HAZOP study steps shown in Figure 1 as follows:

1. Define the system of study and the scope of the analysis.
2. List all the functions that the system components are designed to perform.
3. For each of the identified functions, apply a set of guidewords [8] that describe the various ways in which the function may deviate from its design intent.
4. Identified malfunctions from relevant guideword for each function is then analyzed with applicable scenarios to document the context of malfunction.
5. Severity, Exposure, Controllability [9] is then analyzed for step 4.
6. Top level Safety goals are derived to be fulfilled by the system design.

2.2 Method 2: Systems-Theoretic Process Analysis (STPA)

The STPA is a top-down system engineering approach to system safety that guides safety managers and analysts in the identification of a migration toward states of higher *risk [11]* and addresses more types of hazards and treats safety as a dynamic control problem rather than an individual component failure. STPA also addresses types of hazardous causes in the absence of failure [12]. In STPA, the system is modelled as a dynamic control structure, where proper controls and communications in the system ensure the desired outcome for emergent properties, such as safety. In the STPA framework, a system will not enter a hazardous state unless an unsafe control action is issued by a controller, or a control action needed to maintain safety is not issued. The STPA steps are shown in Figure 2.

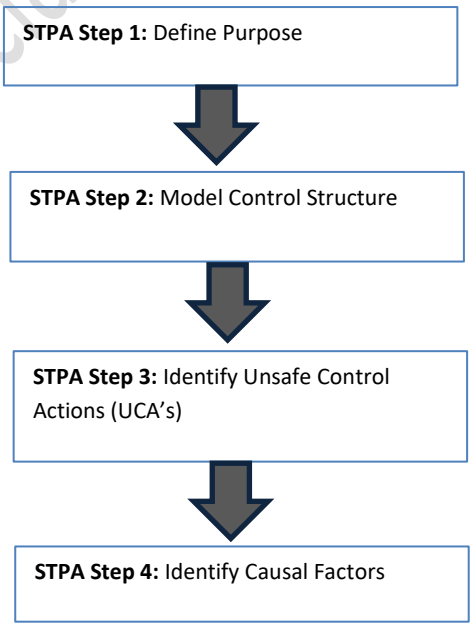

Figure 2: STPA Steps

2.3 Integrating STPA steps into ISO26262

The absence of a risk assessment phase in the STPA analysis method represents a notable omission, as this step plays a crucial role in determining the safety integrity allocation on system elements. In Figure 3, the procedures for incorporating STPA into the ISO26262 [REF ISO] process methodology are presented.

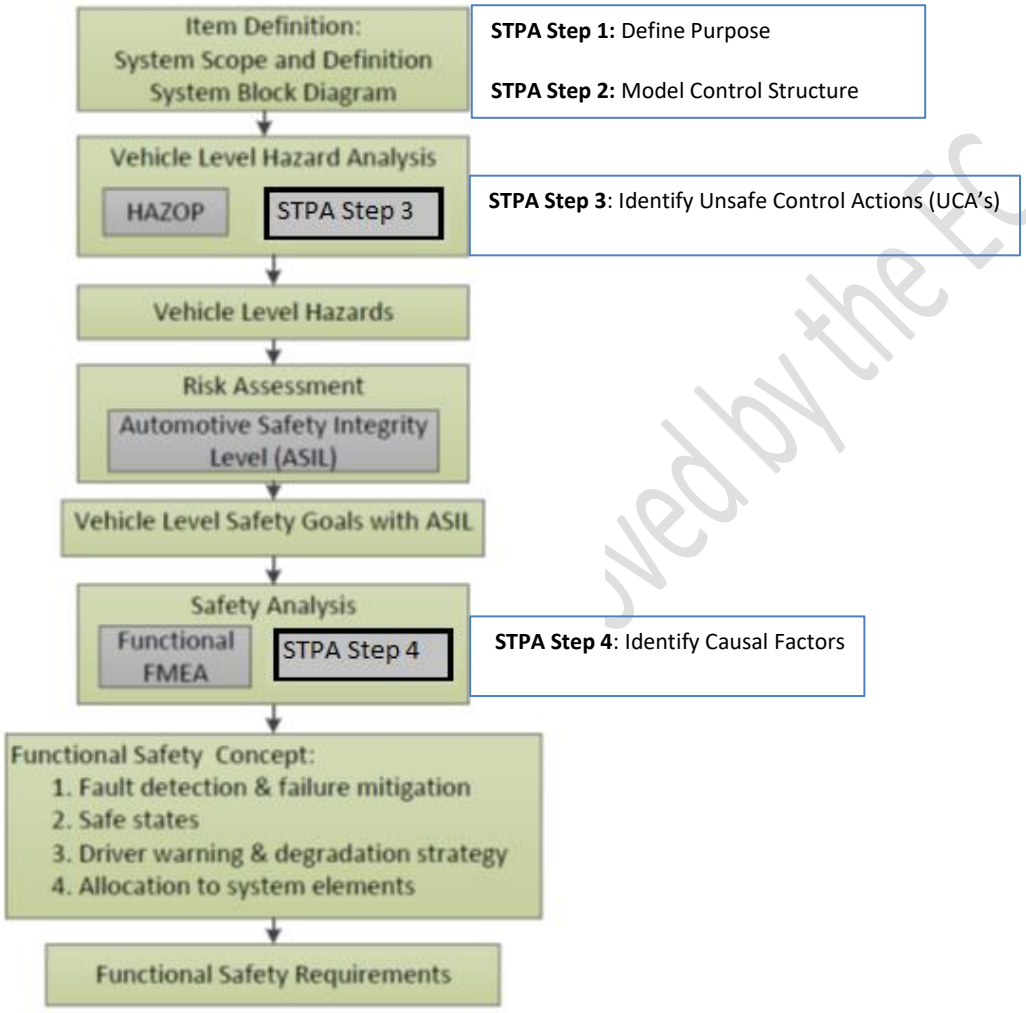

Figure 3: STPA in ISO26262 Context

By merging the traditional HAZOP process with STPA, we have enhanced our safety analysis approach, making it more tailored for Connected and Autonomous Vehicles (CAVs).

3. Item Definition: System scope and definition.

The System Scope refers to defining the boundaries and extent of the automotive safety system under consideration. This involves specifying the components, functions, and interfaces that are within the scope of the safety assessment.

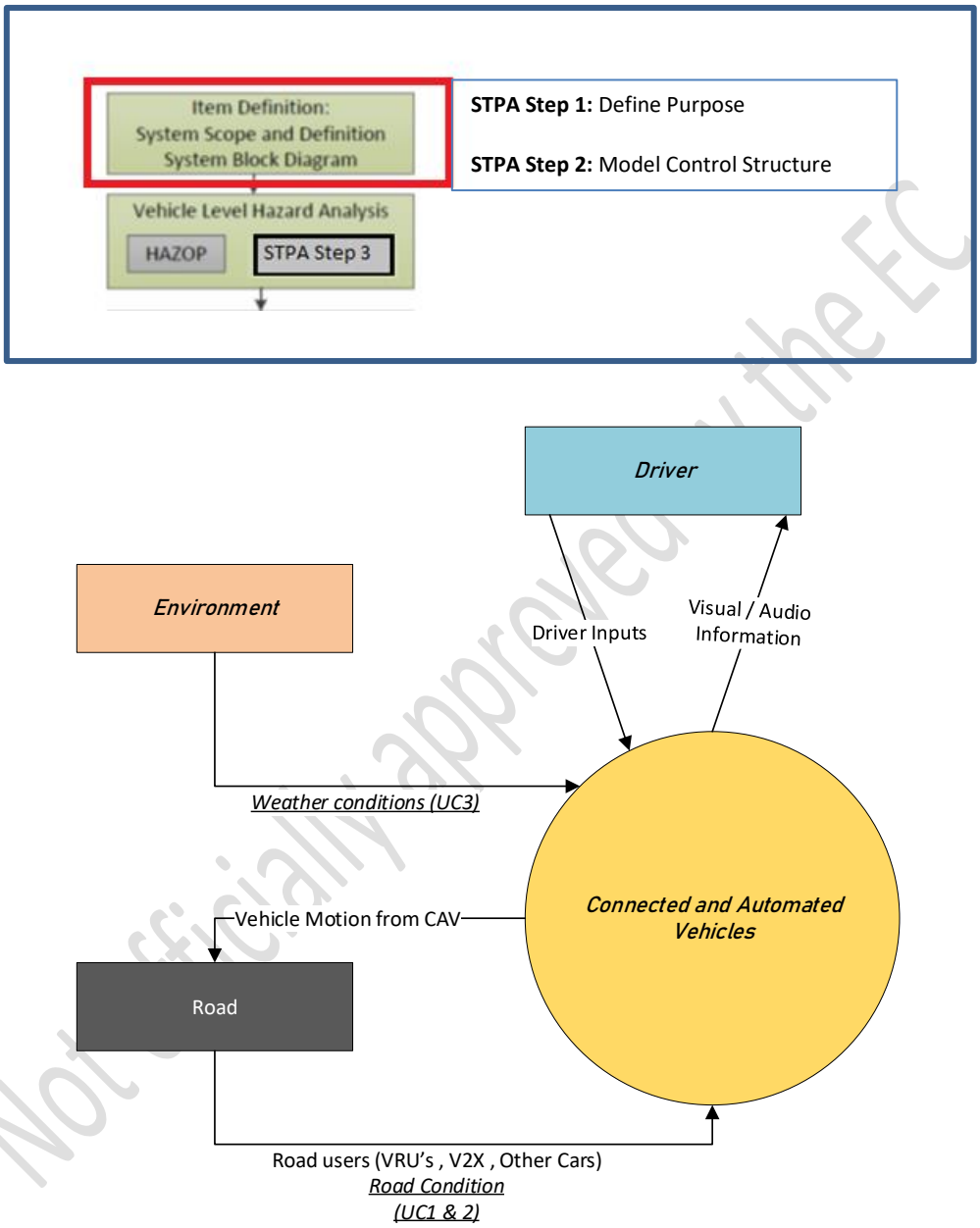

Figure 4: Item Context Diagram

3.1 Initial Inputs for HARA

Analysis Assumptions on CAV

- Autonomy vehicle level – L3 system (Driver hands off).
- ODD as defined to include all experiments for the EVENTS Use Cases 1, 2 & 3 [14] [15].

- Vehicle equipped with automatic gear, wiper and headlights.
- Autonomous mode intended for forward motion only.

Analysis Assumptions on Driver

- Driver with valid driving license.
- Driver shall remain attentive and able to take back control in time when requested by the Autonomy Function.

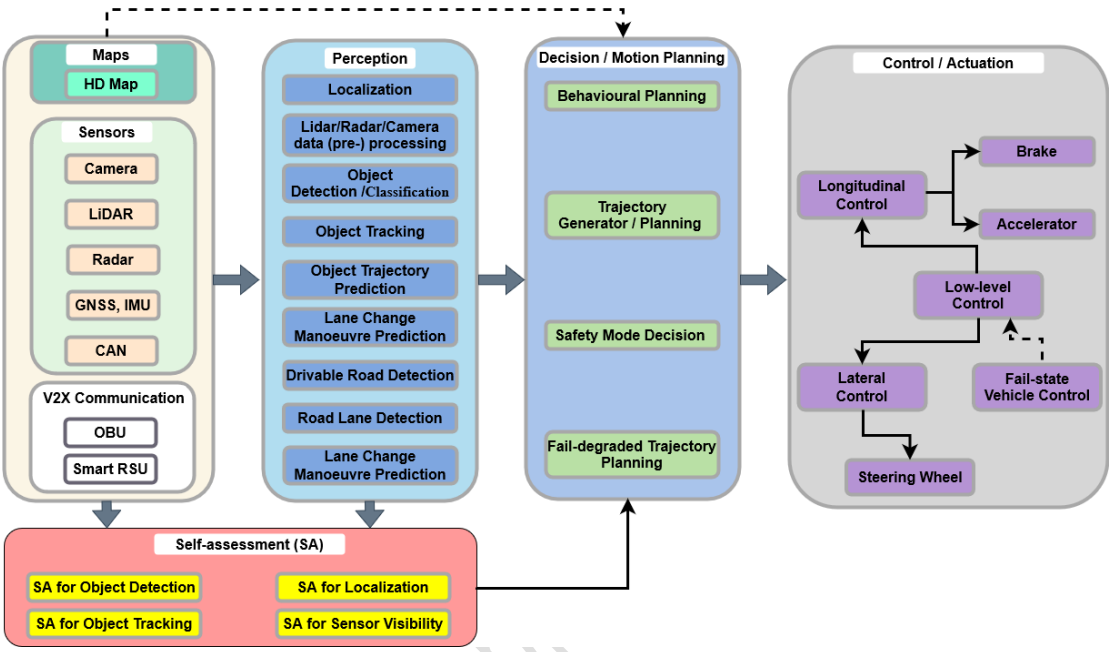

Figure 5: EVENTS system architecture diagram

3.2 STPA Step 1: Define Purpose

Purpose: Identify Losses

An approach to identifying losses involves:

1. Identify the stakeholders, e.g. Users, producers, customers, operators, etc.
2. Stakeholders identify their “stake” in the system. What do they value? For example, human life, fleet of useable aircraft, electrical power generation, transportation, etc. What are their goals? For example, maintain a fleet of useable aircraft, provide transportation, provide medical treatment, provide electrical power generation, etc.
3. Translate each value or goal into a loss.

Identified list of losses:

L-1: Loss of life or injury to people

L-2: Loss or damage to vehicle

L-3: Loss or damage to objects outside the vehicle

**The focus of this safety analysis will be to cover loss of life or injury to driver, passenger or pedestrians and other losses have been excluded.*

Losses	
L-1	Loss of life or injury to driver, passengers, or pedestrians

Table 1: Identified Losses

A hazard is a system state or set of conditions that, together with a set of worst-case environmental conditions, will lead to a loss.

Vehicle-Level Hazards:	**Hazard Description**	**Link to Losses**
H-1	CAV fails to maintain minimum separation with or collides with vulnerable road users.	L-1
H-2	CAV fails to maintain minimum separation with or collides laterally with static/dynamic objects.	L-1
H-3	CAV fails to maintain minimum separation with or collides longitudinally with static/dynamic objects.	L-1
H-4	CAV fails to follow traffic signs / rules.	L-1
H-5	CAV enters an uncontrolled state.	L-1
	Note: Vulnerable road users can include pedestrians, cyclists, horse riders, motorcyclists and people using mobility scooters.	

Table 2: Vehicle level hazard table.

3.1 STPA Step 2: Model Control Structure

The control structure represents how the system is controlled or managed. It includes the controllers, operators, and automated control elements that influence the system's behavior. In Figure 6, the RED downward arrows represent the control actions and the BLUE upward arrows indicate the feedback signals. The UCA (unsafe control action) Guideword is applied to each control action and relevant hazard is documented in STPA Step 3.

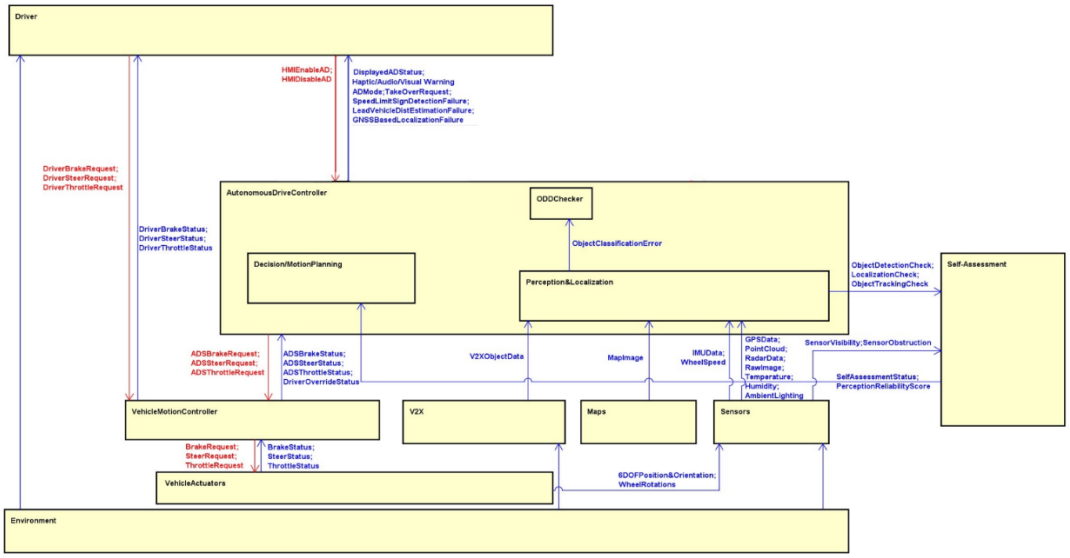

Figure 6: Model Control Structure (a larger image is shown in Annex 1)

4. Vehicle Level Hazard analysis

Vehicle Level Hazard Analysis involves systematically identifying potential safety risks in a vehicle's design and operation, assessing the severity and probability of these hazards, and implementing measures to mitigate them. This process helps ensure that vehicles are engineered with a strong focus on safety, reducing the risk of accidents and enhancing overall road safety. This activity is performed at a vehicle level and the top-level safety goals are derived. The subsystems will inherit the relevant safety goals and ASIL targets.

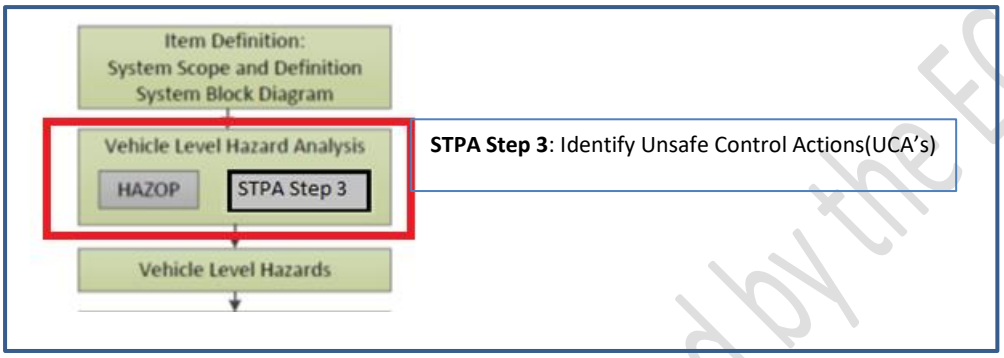

Figure 7: The STPA Step 3

4.1 Functional Decomposition of CAV.

Functional decomposition of a Level 3 (CAV) autonomous system involves breaking down the system's capabilities and functions into distinct components that work together to enable the vehicle to operate autonomously.

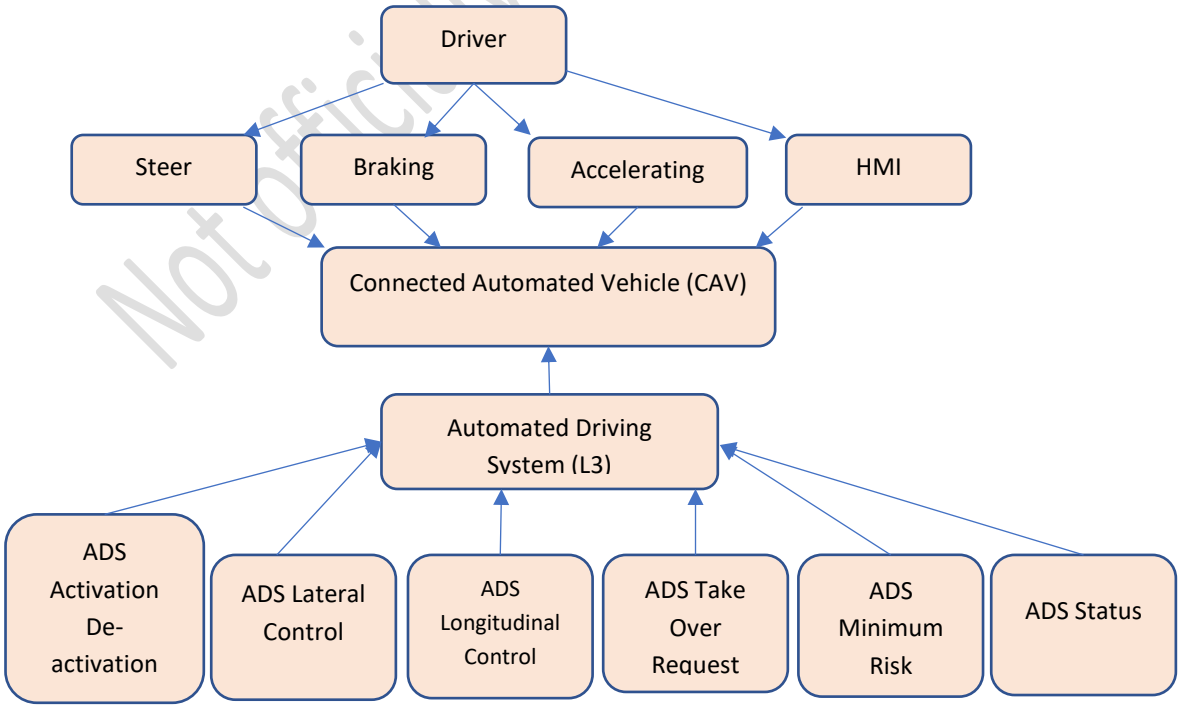

Figure 8: CAV Functional Decomposition

4.2 Functions list with applicable HAZOP Guidewords

		HAZOP Guide Word			
	ADS Function List	***No /Loss /Missing***	***Incorrect***	***Unintended***	***Insufficient***
1	ADS Activation	x	x	x	Not Applicable
2	ADS De-activation	x	x	x	Not Applicable
3	ADS Lateral Control	x	x	x	x
4	ADS Longitudinal Control (Acceleration & Braking)	x	x	x	x
5	ADS Take Over Request (CAV initiated)	x	x	x	Not Applicable
6	ADS Minimum Risk Maneuver	x	x	x	Not Applicable
7	ADS Status (Active/Inactive)	x	x	Not Applicable	Not Applicable

ADS – Autonomous Driving System

Table 3: Applicable HAZOP Guidewords for ADS functions.

4.3 Experiments for hazard analysis.

The list of experiments provides Locations, Road & Weather conditions and Traffic and people considerations [14] and its relevant combinations, which are included in the HARA analysis. Namely, the EVENTS experiments are:

EXP1: Interaction with VRUs under complex urban environment. *(HARA Analysis on Urban roads with VRU's and adverse weather conditions)*

EXP2: Re-establish platoon formation after splitting due to roundabout. *(HARA Analysis on Urban roads)*

EXP3: Self-assessment and reliability of perception data with complementary V2X data in complex urban environments. *(HARA Analysis on Urban roads)*

EXP4: Decision making for motion planning when faced with roadworks, unmarked lanes and narrow roads with assistance from perception self-assessment. *(HARA Analysis on Urban roads & Highway with Missing lane information and Construction zone)*

EXP5: Decision making for motion planning when entering a jammed highway. *(HARA Analysis on Highways with varying traffic conditions)*

EXP6: Small object detection at a far range in adverse weather conditions. *(HARA Analysis on Highways with Static Objects in lane)*

EXP7: Localization/perception self-assessment and other vehicles' behaviour prediction under adverse weather or adverse road conditions. *(HARA Analysis on Urban and highway roads with adverse weather conditions)*

The consolidated list to perform HARA for all experiments is tabulated below.

Location		Surface Condition
Road type	**Road layout**	
Highway (max- 130kmph)	Two way driving non-divided with VRU's	Normal road condition (Mu > 0.8)
Urban roads (max- 50kmph)	Highway with several lanes	Low Mu (<0.4)
	Missing lanes	
	Construction zone	

Table 4: Location and surface condition table

Weather Conditions	Traffic and people	
	Traffic Condition	Static Objects
Normal condition	No Traffic - Free Drive	No Obstruction in Lane
Rain	Slow moving traffic < 10kmph	Obstruction in Lane
Snow	Traffic Standstill	
Dense Fog		

Table 5: Weather and traffic condition table

4.4 Vehicle Operating Modes

CAV Mode	Description	Driving Authority
Manual Mode	Driver performing dynamic driving task.	Driver
Autonomy Active ADS	CAV performing dynamic driving task.	CAV
Take Over Request	CAV performs dynamic driving for short duration until driver takes over.	CAV -> Driver
Minimum Risk Maneuver	CAV performs stop in lane maneuver with gradual deceleration in the absence of driver take over.	CAV

Table 6: Vehicle operating mode table

4.5 STPA Step 3: Identify Unsafe Control Actions (UCA's)

From the control structure each down arrow coloured in RED is a control action. The UCAs (Unsafe Control Actions) which are control actions that, in a particular context and worst-case environment, will lead to a hazard are documented in STPA Step-3.

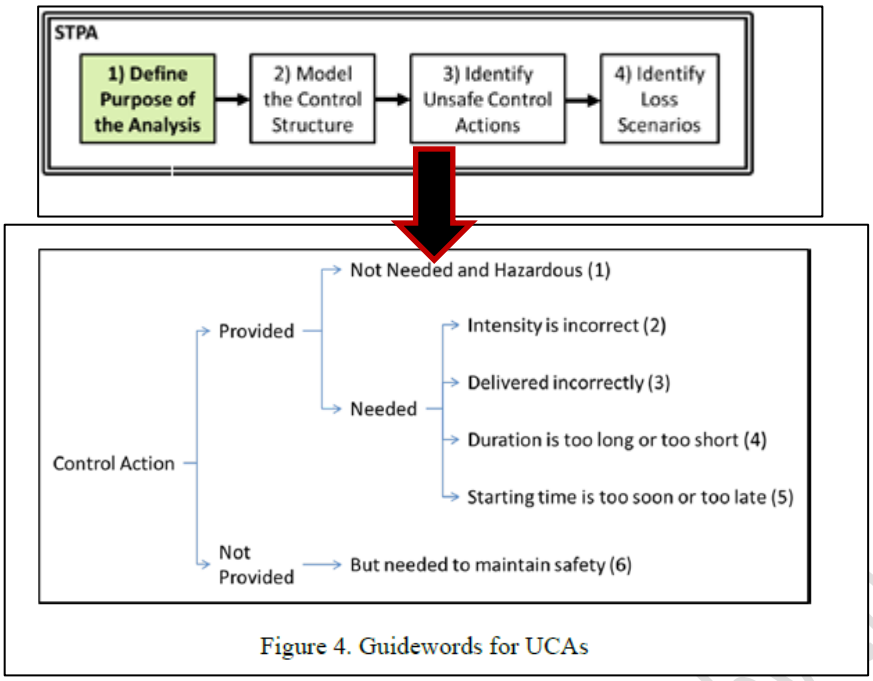

Figure 9: UCA Guideword

The detailed STPA Step 3 can be found in Annex 2.

5. Risk Assessment – ASIL Rating

Risk Assessment is a quantitative assessment of the risk associated with each hazard. Risk is typically calculated as the product of the likelihood (probability) of an event and the severity (consequences) of that event. ISO 26262 [1] defines a specific Automotive Safety Integrity Level (ASIL) scale (ASIL A, B, C, or D) to categorize the risk level.

Figure 10: The Automotive Safety Integrity Level (ASIL)

The detailed HAZOP-based HARA can be found in Annex 3.

5.1 Safety goals derived from HARA

No	Safety Goal	ASIL	Responsible Function
1	Ensure ADS status is correctly reported to the driver	D	ADS Status (Active/Inactive)
2	Prevent control not given back to the driver when requested	D	ADS Take Over Request (Driver Take Over)
3	Prevent ADS use outside of ODD	D	ADS Activation / De-ADS Activation
4	Prevent insufficient/ unintended steering.	D	ADS Lateral Control
5	Prevent unintended braking.	C	ADS Longitudinal Control (Acceleration & Braking)
6	Prevent loss or insufficient braking.	D	ADS Longitudinal Control (Acceleration & Braking)
7	Prevent unintended acceleration.	D	ADS Longitudinal Control (Acceleration & Braking)
8	Always activate brake lights when brakes are activated.	C	Vehicle Body/Chassis domain
9	Ensure safe stop in case of no driver take over	D	ADS Minimum Risk Maneuver

Table 7: Safety goal summary

5.2 Assigning Control Actions to ADS Functions

Control Action	From	To	Responsible Function
HMIEnableAD	Driver	AutonomousDrive Controller	ADS Status
HMIDisableAD			
DriverBrakeRequest	Driver	VehicleMotion Controller	ADS Take Over Request (Manual Drive / Driver Override)
DriverSteerRequest			
DriverThrottleRequest			
ADSBrakeRequest	AutonomousDrive Controller	VehicleMotion Controller	ADS Longitudnal Control (Acceleration & Braking)
ADSSteerRequest			ADS Lateral Control
ADSThrottleRequest			ADS Longitudnal Control (Acceleration & Braking)
BrakeRequest	VehicleMotion Controller	VehicleActuators	- General Body domain
SteerRequest			
ThrottleRequest			

Table 8: Mapping Control Actions to ADS Functions table

6. Safety Analysis

After the unsafe control actions have been identified, the next step is to identify loss scenarios. Two types of loss scenarios must be considered:

a. Why would Unsafe Control Actions occur?

b. Why would control actions be improperly executed or not executed, leading to hazards?

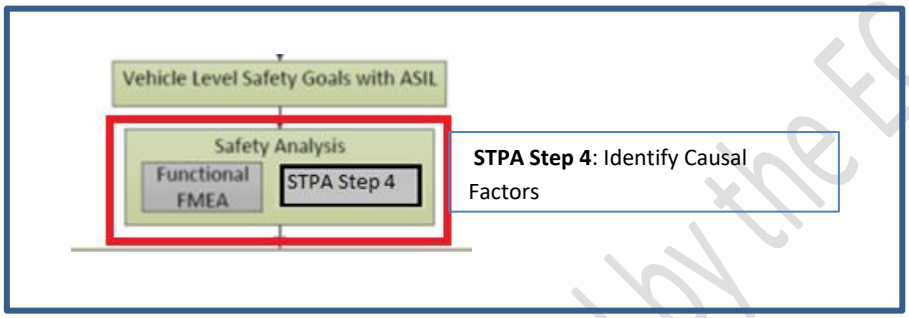

Figure 11: The STPA Step 4

There are four general reasons why a controller might provide (or not provide) a control action that is unsafe:

- Failures involving the controller (for physical controllers).
- Inadequate control algorithm.
- Unsafe control input (from another controller).
- Inadequate process model.
- Hazards can be caused by UCAs, but they can also be caused without a UCA if control actions are improperly executed or not executed. To create these scenarios, we must consider factors that affect the control path as well as factors that affect the controlled process.

The identification of Causal Factor type, Requirements to Prevent & Detect the Causal Factors is documented below.

6.1 STPA Step 4: Identify Causal Factors

The STPA Step 4 can be found in Annex 4.

6.2 Requirements derived from STPA Analysis

STPA being a systematic approach considers safety as an emergent problem and analyses the complex interactions within the social–technical systems. This kind of approach is suitable for SOTIF issues **Error! Reference source not found.**.

In STPA Step 4, we have analyzed known limitations of system components to derive causal scenarios from those limitations that could potentially result in vehicle-level hazards. The Causal Factor analysis which also contains SOTIF triggering events has been grouped into ODD, Driver, Sensors, V2X, Self-Assessment, HMI, AutomousDriveController, MAPS, VehicleMotionController and can be found in Annex 5.

Also, in Annex 5, the Mitigation strategies for these triggering events such as design decision (mechanism for the detection of incorrect/erroneous inputs) and functional limitation (notification to the driver) have been identified.

7. Functional Safety Concept & Requirements

The Functional Safety Concept (FSC) is a crucial aspect of ISO 26262 [1]. The FSC provides a high-level overview of how functional safety will be achieved in a particular system or component. Six FSCs are considered in this report and are analyzed through a simplified system diagram and a list of safety requirements.

Figure 12: The Functional Safety Concept & Requirements

7.1 Activation / Deactivation Functional Safety Concepts

The Activation / Deactivation Functional Safety Concept addresses SG-03 (Prevent ADS use outside of ODD). When ADS is in Available Mode, it keeps evaluating constantly the ODD and ego vehicle condition and road type. With the help of Figure 13, a list of requirements has been defined as follows:

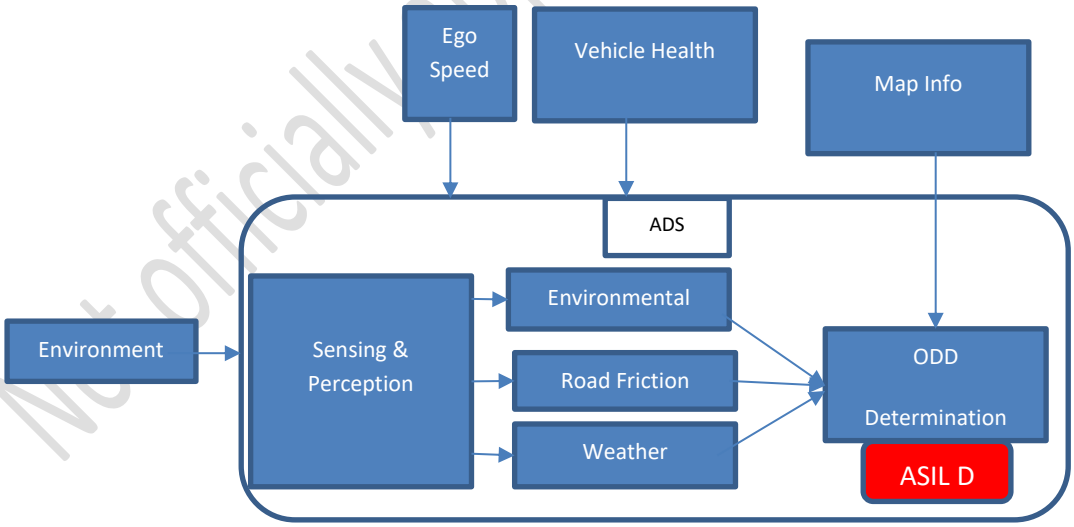

Figure 13: Activation/Deactivation Safety Concept.

- The ODD Determination block shall prevent the operation of ADS outside its ODD by using information provided by various vehicle sub-systems.
- Map info shall provide Country and Road type information.

- Sensing and Perception shall provide Traffic Signs, Lane situations, Road Situations, Traffic Situations and Extreme Weather conditions.

7.2 HMI Status Functional Safety Concept

The Activation/HMI Status Functional Safety Concept addresses SG-01 (Ensure ADS status is correctly reported to the driver). With the help of Figure 14, a list of requirements has been defined as follows:

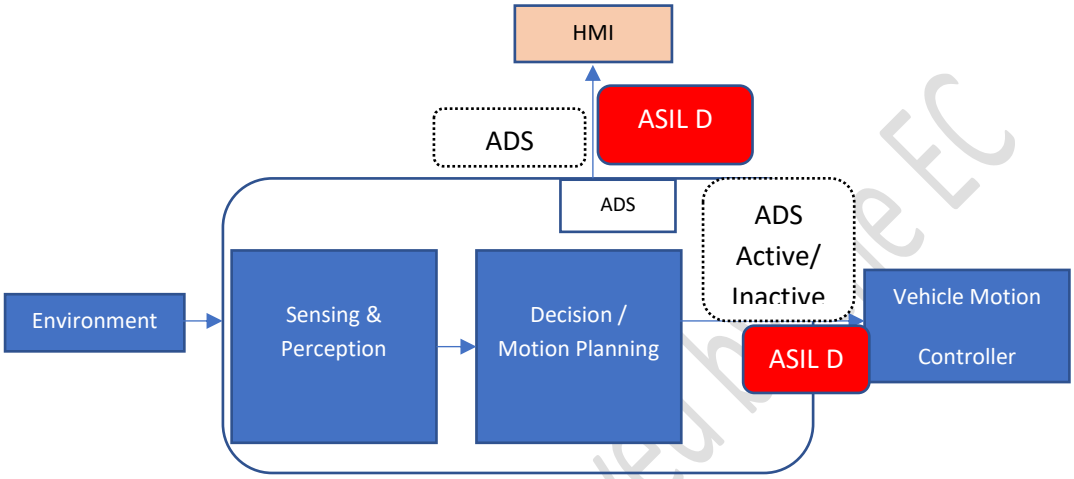

Figure 14: HMI Safety concept

- ADS shall compute the correct ADS activation status.
- Failure: avoid setting ADS active when ADS is not active.
- HMI & Infotainment shall indicate to the driver ADS active only when "ADS ACTIVE" is set by ADS System.
- Recommend to use a graphical visualization and / or a textual description

7.3 Longitudinal Control Functional Safety Concept

The Longitudinal Control Functional Safety Concept addresses SG-5, SG-6, SG-7 covering unintended braking on system limit, loss or insufficient braking, and unintended acceleration while ADS is operating.

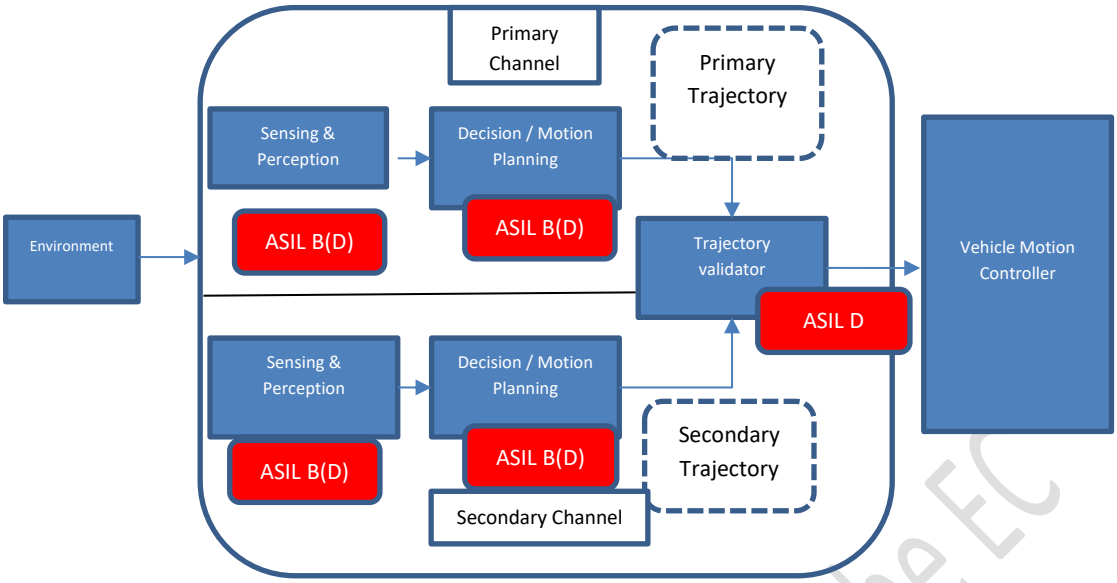

Figure 15: Longitudinal & Lateral Control Functional Safety Concept

The safety integrity of the longitudinal control request is provided by ADS System with 2 independent channels (Primary and Secondary Trajectory generation). Two operational modes are considered:

1. **Nominal Mode**

- Primary longitudinal Request is ASIL B(D).
- Secondary longitudinal Request is ASIL B(D).
- Sufficient independence between Primary trajectory generation and Secondary. trajectory generation shall be demonstrated.
- Trajectory Validator and selection (between both) is ASIL D.When ADS is Active Control, it shall detect safety relevant obstacle and provide its correct attributes (Position, Long/Lat Speed, Long/Lat Accel,).
- In case of conflict between both trajectory, Initiate TOR apply predefined deceleration profile and maintain the lateral control. Where conflict is assumed to be:
    - One trajectory requesting deceleration and second requesting acceleration.
    - Both trajectories requesting different deceleration values. The conflict thresholds need to be tuned.

2. **Fault Handling Mode**

- On detection of fault impacting the Primary Longitudinal Control Request Integrity with respect to No/insufficient deceleration, Primary channel shall initiate a Take Over Request.
- On detection of fault impacting the Secondary Longitudinal Control Request Integrity with respect to No/insufficient deceleration, Secondary channel shall initiate a Take Over Request.

7.4 Lateral Control Functional Safety Concept

The Lateral Control Functional Safety Concept addresses SG-04 (Prevent insufficient/ unintended steering). The safety integrity of the lateral control request is provided by ADS System with 2 independent channel trajectories. To ensure the sufficient independence between both trajectories, 2 different sources are used for the perception of Ego Lanes:

- Source 1: Camera.
- Source 2: LIDAR / Surround Camera AND Predicted trajectory Lane based on Surrounding Object as lead Vehicle, Adjacent Vehicles, Road Boundaries (Barriers, Edges).

ASIL D: Deviation of more than 50 cm with high yaw rate change (In Annex 3 - ADS Lateral Control).

ASIL B: Deviation of more than 50 cm with low yaw rate change (In Annex 3 - ADS Lateral Control).

In case of conflict between Primary and Secondary trajectories, Initiate TOR apply predefined deceleration profile and maintain the lateral control (Last known best values). Primary & Secondary Channel shall detect Lane markings with Source 1 (Camera) and Source 2 and provide its correct attributes.

Fault magnitude: inaccuracy of +/-50 cm.

7.5 Take Over Request & Safe Stop Functional Safety Concept

Take over request is initiated by the CAV when it can no longer perform the required DDT (Dynamic driving task). Take Over Request FSC addresses SG-2 (Prevent control not given back to the driver when requested) and SG-9 (Ensure safe stop in case of no driver take over). Driver actions on steering and braking has the highest priority over ADS request. Transition to safe stop shall be performed depending on failure category as described in *Table 9*.

Initial Operating Mode	Failure Categories	ADS capabilities after Failure	Transition to safe state
Available / Standby	Any Failure	-	Feature Disabled
Active Control	Low critical failures	Vehicle is able to maintain follow Lead vehicle/Lane (including collision mitigation)	Comfort Handover-Handover period of 30s and to stop the vehicle within 15sec.
Active Control	High critical failures	Vehicle is able to stop-in-Lane Only	Emergency Deceleration to stop in lane

Table 9: Failure criticality to safe state transition table

7.6 Usage of STPA derived requirements & FSC in EVENTS

This section explains, using an example, the methodology for usage of derived safety concept and the STPA requirements for the individual experiments.

EVENTS module owners shall select the applicable safety concept from Section 6 that is relevant for their experiment. For example, in EXP6 *(Small object detection at a far range in adverse weather conditions)*, as illustrated in Figure 11, the focus is only on Sensing & Perception and Decision/Motion Planning.

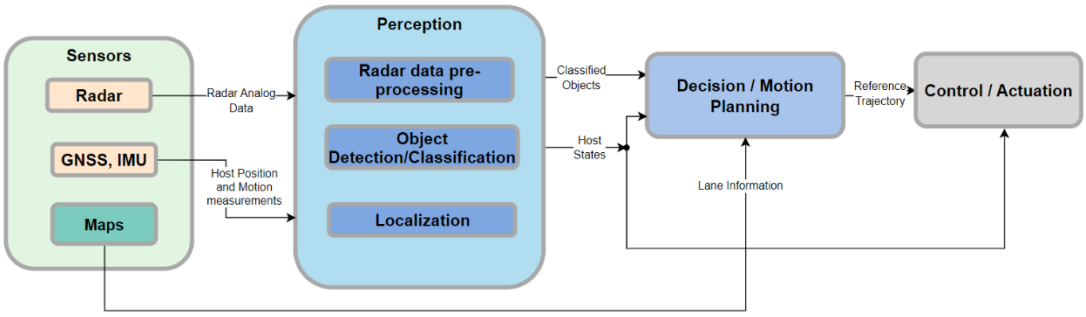

Figure 16: EXP6 high-level Full Stack Architecture and Interfaces

EXP6 shall apply the Longitudinal & Lateral Control Functional Safety Concepts and the requirements from STPA analysis (Section 6.2) from Sensors & Perception, AutomousDriveController, and MAPS.

8. Acceptance Criteria for SOTIF based on Mileage Strategy

Acceptance criteria are the most important metrics used to measure/assure safety of the intended function (SOTIF) of an autonomous vehicle or advanced driver assistance system (ADAS) [16]. Mileage refers to the distance a vehicle can cover using one gallon or liter of fuel or per one charge cycle. Considering a car's operating speed and mileage, there is a limited amount of time or distance it can travel in a given year. Within this mileage strategy [10], we utilize this time or distance to establish Acceptance Criteria values.

Factors to Consider for calculating Acceptance Criteria with Mileage Strategy:

Average Vehicle Speed: In the context of the mileage strategy, it is crucial to monitor the average speed of a vehicle during its Operation Design Domain (ODD). This is because urban, rural, and highway mileages can vary significantly for vehicles. Furthermore, when a vehicle operates at a low average speed within its ODD, there's a limit to the number of miles it can cover even with extended hours of operation. This information helps us assess whether we require more test fleet vehicles or simply need to adjust the planned timeline for mileage accumulation.

Crash Data: Similar to the operational lifetime strategy, obtaining crash data for the mileage strategy may not always be straightforward. Instead, we may need to estimate the number of crashes by considering the ODD or the expected average accidents per km within the ODD. This estimation is essential for calculating Acceptance Criteria (AC) [2][3][4][5].

ODD Factors: Just like in other strategies, ODD factors are significant in the context of the mileage strategy. Regardless of the total potential achievable mileage by the vehicles, insufficient coverage of the intended ODD factors could compromise Safety of the Intended Function (SOTIF) assurance.

Table 10 can be used to calculate the Acceptance criteria based on the mileage strategy.

Annual distance travelled by car for the EU (kms)	Total passenger car on road (EU)	Average Injuries + fatalities per year (EU 2017-2021)	Passenger cars Injuries + fatalities per year (EU)	VRU's Injuries + fatalities per year (EU) ***(Pedestrians + Motorcycle + Bicycle)***	Passenger cars (Injuries + fatalities) **Incidents/km**	VRU (Injuries + fatalities) **Incidents/km**
11.300	**246.000.000**					
	Number of Fatalities	21.500	9.589	9.245	3,45E-09	3,32578E-09
	Number of Injuries	1.200.000	535.200	516.000	1,92532E-07	1,85625E-07
	Total	1.221.500	544.789	525.245	1,96E-07	1,89E-07
	Rural roads accounted for 52.5 % of the fatalities			1,81E-09		
	Urban roads accounted for 38.7 % of the fatalities			1,33E-09		
	Motorways accounted for 8.8 % of the fatalities			3,04E-10		
Average number of kilometers between incidents	5.102.525,9	Kms				

Table 10: Acceptance Criteria Calculation

With the current crash data, the incident/km for Passenger cars is 1.96E-07 and Pedestrians is 1.89E-07. The L3 System developed shall be at least 10 times safer than human performance and the SOTIF acceptance Criteria shall be 1.96E-08.

Note: Applying acceptance criteria as defined above to the EVENTS experimental context (simulations and field tests) and subsystems will be investigated further during the evaluation phase (WP6).

9. Conclusions

In conclusion, the completion of the D2.3 deliverable represents a significant milestone in ensuring the safety and reliability of our autonomous driving system. By employing both classical Hazard and Operability (HAZOP) analysis and the System-Theoretic Process Analysis (STPA) approach, one of the notable achievements of this deliverable is the clear definition of safety goals and safety requirements. These are essential components for guiding the development and evaluation of our autonomous driving system.

The tabulation of safety requirements into distinct categories, including ODD (Operational Design Domain), Sensors, Driver Interaction, and AVstack (Autonomous Drive Controller), provides a structured framework for addressing specific safety concerns within each area. Furthermore, the Functional Safety Concept (FSC) outlined in this deliverable illustrates how we intend to achieve system-level safety, by outlining the strategies and measures to mitigate identified risks.

In the future, our steps will involve these safety concept and safety requirements to be accepted by experiment leaders and implemented during the implementation phase of the project (WP5).

References

[1] ISO. 26262-2:2018 Road vehicles — Functional safety — Part 2: Management of functional safety, 2018.

[2] *https://road-safety.transport.ec.europa.eu/system/files/2023-03/ERSO_annual_report_20220509.pdf*.

[3] *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Road_accident_fatalities_-_statistics_by_type_of_vehicle&oldid=583880*.

[4] *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Passenger_mobility_statistics#Urban_trips*.

[5] *https://www.odyssee-mure.eu/publications/efficiency-by-sector/transport/distance-travelled-by-car.html#:~:text=Sectoral%20Profile%20%2D%20Transport&text=Large%20discrepancy%20of%20the%20average,km%2Fyear%20for%20the%20EU*.

[6] *https://jsystemsafety.com/index.php/jss/article/view/6*.

[7] *https://warg.org/fredrik/publ/ssiv2020/QRN_Approach.pdf*.

[8] *https://pqri.org/wp-content/uploads/2015/08/pdf/HAZOP_Training_Guide.pdf*.

[9] *https://www.i-q.de/iso-26262/fusi-asil-klassifikationen*.

[10] *https://www.sae.org/publications/technical-papers/content/2023-01-0582/*.

[11] *https://dspace.mit.edu/handle/1721.1/124172*.

[12]*https://www.researchgate.net/publication/314797280_Using_STPA_in_Compliance_with_ISO_26262_for_Developing_a_Safe_Architecture_for_Fully_Automated_Vehicles*.

[13] Becker, C., Brewer, J. C., & Yount, L. (2020). Safety of the intended functionality of lane-centering and lane-changing maneuvers of a generic level 3 highway chauffeur system (No. DOT HS 812 879). United States. National Highway Traffic Safety Administration. Electronic System Safety Research Division.

[14] EVENTS Deliverable D2.1: User and system requirements for selected use cases (2023).

[15] EVENTS Deliverable D2.2: Full Stack Architecture & Interfaces (2023).

[16] Madala, K., Erdos, D., Krishnamoorthy, J., Wang, Z., Gonzalez, C. A., Shivkumar, A., & Chang, M. (2023). Strategies to Define Reasonable Acceptance Criteria and Validation Targets for SOTIF Assurance (No. 2023-01-0582). SAE Technical Paper.