AWARD

Scaling autonomous logistics

D4.6 – Public safety Documents including Safety plan, Hazard Analysis and Risk Assessment, Functional and technical safety concepts

Lead: Michael Gimeno

Due date: April 2022

Actual delivery date: 18/10/2022

Dissemination level: PU

The project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 101006817.

Document information

Project	
Project Acronym	AWARD
Project Full Title	All Weather Autonomous Real logistics operations and Demonstrations
Grant Agreement No.	101006817 - H2020-DT-ART-2020
Project Coordinator	EasyMile
Website	www.award-h2020.eu
Starting Date	January 1st, 2021
Duration	36 months

Deliverable	
Deliverable No. – Title	D4.6 Safety documents
Dissemination Level	Public
Deliverable Type	Report
Work Package No. – Title	WP4
Deliverable Leader	EasyMile
Responsible Author(s)	Michael Gimeno (EasyMile)
Responsible Co-Author(s)	NA
Technical Peer Review	Sylvain Rheme (CertX)
Quality Peer Review	Stéphane Potiron, Magali Cottevieille (EasyMile)
Submission date	30/04/2022 (initial version) 18/10/2022 (updated version)

LEGAL DISCLAIMER

This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

ACKNOWLEDGMENT OF EU FUNDING

The project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 101006817.

CONTACT

Ms. Magali Cottevieille
Project Coordinator
EasyMile
21 Boulevard de la Marquette
31000 Toulouse
France

Email: magali.cottevieille@easymile.com
www.award-h2020.eu

Revision history

Revision Number	Date	Author	Company	Changes
V0.1	09/04/2022	Michael Gimeno	EasyMile	Initial version
V0.2	19/04/2022	Sylvain Rhème	CertX	Technical version
V0.3	29/04/2022	Stephane Potiron	EasyMile	Quality review
V0.4	29/04/2022	Michael Gimeno	EasyMile	Final version
V1.0	29/04/2022	Magali Cottevieille	EasyMile	Last corrections
V1.1	16/09/2022	Michael Gimeno	EasyMile	Chapter updated according to project officer review: 1) Executive summary 6) Conclusion 4.3.2) 4.4.2) 4.5.2)

Table of contents

List of figures

List of tables

List of acronyms

ADS	Autonomous Driving System
ADV	Autonomous Driving Vehicle
ASIL	Automotive Safety Integrity Level
ATS	Autonomous Transport System
E/E	Electric / Electronic
FHE	Functional Hazardous Event
FSC	Functional Safety Concept
FSR	Functional Safety Requirement
HARA	Hazard Analysis and Risk Assessment
HDV	Heavy-Duty Vehicles
OBU	On Board Unit
OS	Operational Situation
RSU	Road Side Unit
SG	Safety Goals
SOTIF	Safety Of The Intended Functionality
UC	Use Case
VRU	Vulnerable Road User

1. Executive Summary

This deliverable “D4.6 – Public Safety Documents” presents the different safety activities that have been performed to determine and mitigate the safety risk related to the AWARD autonomous driving system project.

It is the public document that presents and summarizes the different activities related to task T4.1 which is part of “WP4 – Integration in heavy duty vehicle”.

Task “T4.1– Definition of safety and technical specification for each autonomous heavy-duty vehicle” – uses the overall scope of the targeted system and subsystem as defined in the “D3.1 – Architecture design report” and the operational situation and use cases defined in the “D2.3 – Use cases specification”.

The first part of this document deals with the scope of the safety studies and the different activities that have been performed within AWARD project. The purpose of this part is to introduce the methodology used in the AWARD project for the safety activities.

The second part presents the methodology and the outcome of the hazard analysis and risk assessment. The purpose of this part is to identify all the risks related to the different AWARD use cases.

The third part presents the methodology and the outcome of the functional safety concept activities. The purpose of this part is to determine the main principle to mitigate each safety risk identified in the previous part.

The last part describes the different safety concepts from a technical perspective. The purpose of this task is to present in detail each safety concept introduced in the previous part.

2. Safety plan

2.1. Scope

2.1.1. Scope of the safety plan

This safety plan presents the structure put in place, the organization and the safety documents produced which, together, shall guarantee the demonstration of safety management.

The scope of this document is limited to the scope of the WP4 of AWARD project. This document covers safety and SOTIF activities limited to the automated transport system level including:

- EasyMile systems
- All-weather sensor set
- Vehicle Platform
- Infrastructure (if needed).

2.1.2. Scope of the project

2.1.2.1. Scope

In order to demonstrate and evaluate the technical improvements for all-weather operations of automated vehicles, the AWARD project includes specific real world use cases. The use cases address vehicle tasks in different settings, from industrial areas to public roadways as well as with different automated vehicles and users.

The AWARD project aims at demonstrating the automated vehicles working in all weather conditions and addressing challenges related to the deployment of these vehicles in real logistics operations through several strategic use cases that meet market needs, from the factory to logistics hubs.

The following use cases are included in the AWARD project:

- Use Case 1 (UC1): Loading and transport with automated forklift.
- Use Case 2 (UC2): Hub-to-hub shuttle service from warehouse/production site to logistics hubs.
- Use Case 3 (UC3): Automated baggage tractor on airside in Avinor OSL Gardermoen airport.
- Use Case 4 (UC4): Container transfer operations and automated boat loading in Rotterdam port.

2.1.2.2. System and component responsibilities

The workflow below (figure 1) describes the interaction between activities and delivery of the different work packages regarding the safety activities.

At the safety measures allocated to the infrastructure shall be defined at ATS level and the safety measure allocated to the platform shall be defined at vehicle level.

Both measures are included in the list of FSR exported to D3.1 Architecture design report.

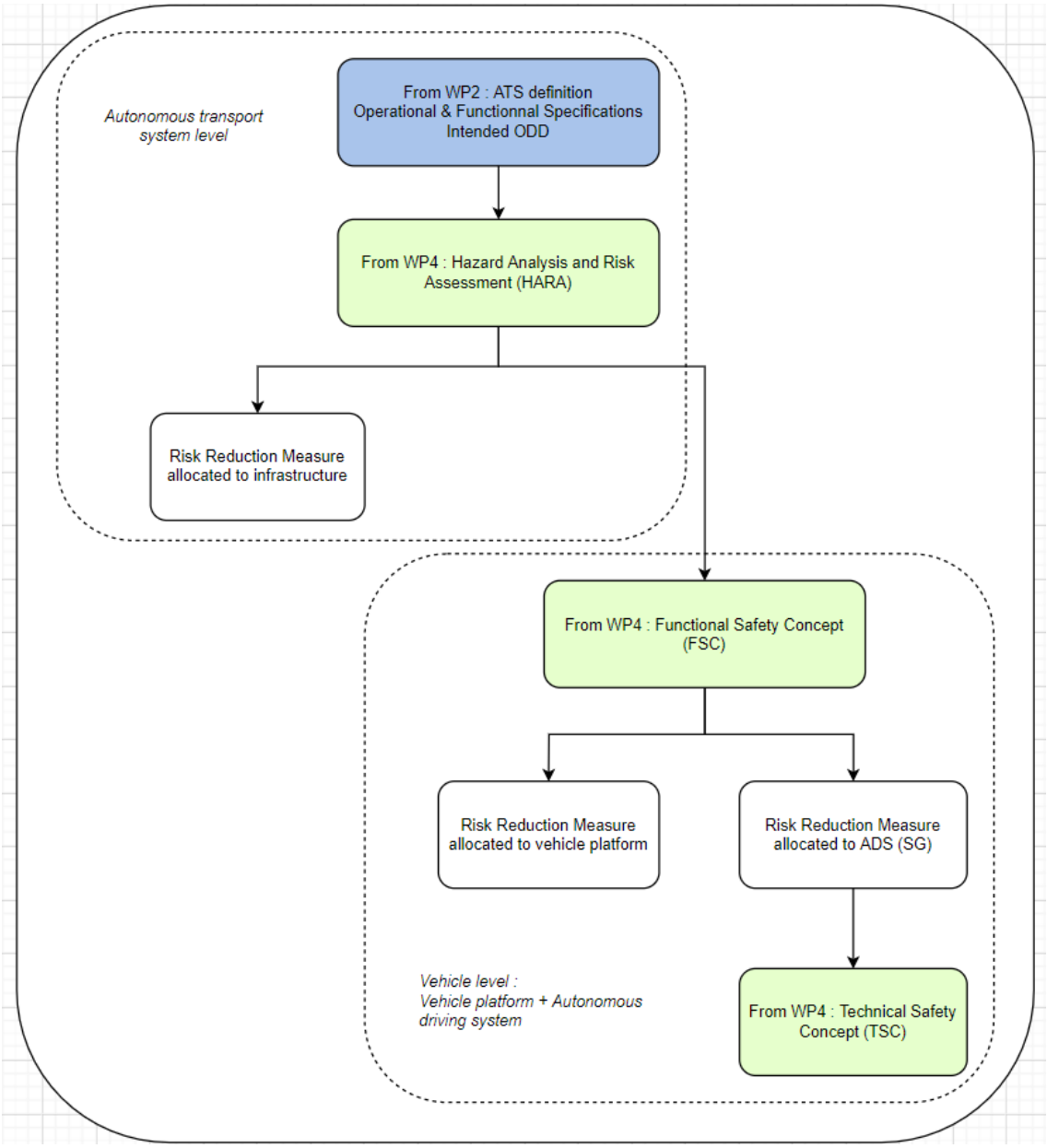


Figure 1: system and component responsibilities

2.2. Management of safety

2.2.1. Management of functional safety

2.2.1.1. Organization specific rules and processes for functional safety

– The organigram is described in figure 2.

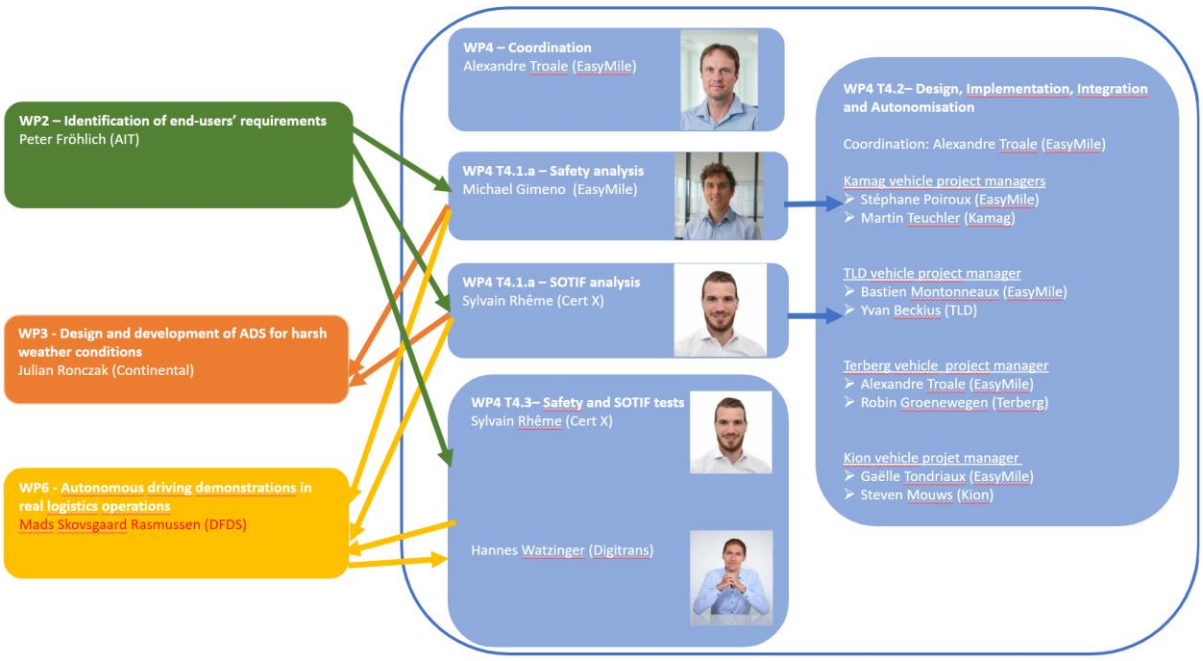


Figure 2: WP4 Organigram

– A project plan has been defined (deliverables, milestones etc.).

2.2.1.2. Competence management

The role of some of key actors of the project is presented below:

– The Project Manager is responsible for the coordination and monitoring of the entire project at ADS Level, which includes the Safety activities.

– The AWARD Safety Engineer is responsible for the implementation of the safety activities.

This includes:

– Ensuring the definition of this Safety Plan.
– Ensuring the update of this Safety Plan in relation to potential changes in the contract related to the project.
– Coordinating and performing the functional safety activities (described in this Safety Plan).
– Ensuring that the safety objectives and requirements of the ADS contract will be met.
– Collaborating with the AWARD SOTIF Engineer.

2.2.2. Project related safety management

The document review process is the following (figure 3):

1. Review using « track changes » in the Word document
2. PR Feedback form
3. Peer review document.

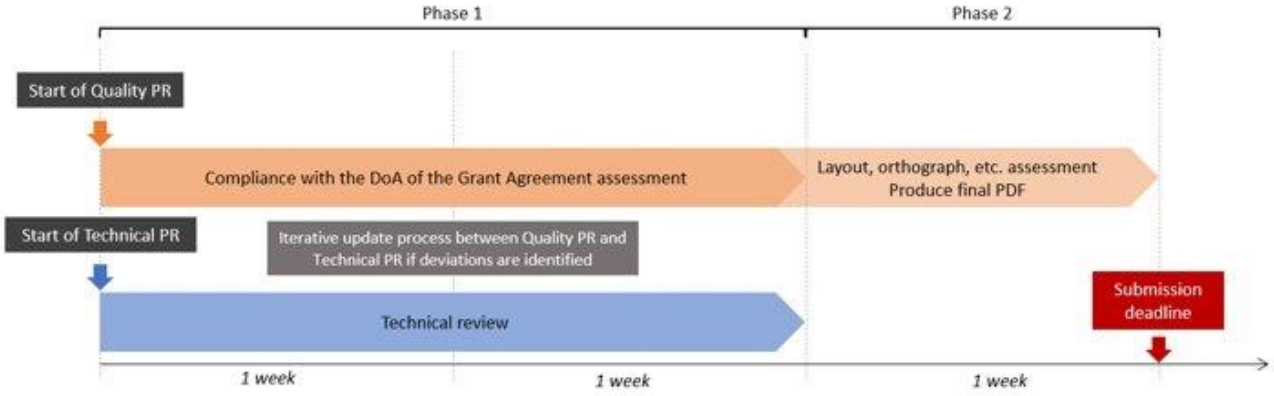


Figure 3: Project related safety management

2.2.3. Safety plan process

AWARD safety activities will follow the ISO 26262 recommendations. Even if ISO 26262 is a standard applicable to road vehicles, its scope has been extended for the AWARD project to the other AWARD use cases and platforms. Indeed, for the open road use cases, ISO 26262 is the more relevant standard.

According to the remaining time, a gap analysis could be performed between ISO 26262 and ISO 3691-4 to identify the remaining work to cover ISO 3691-4 if any.

Note: This gap analysis is not including in the scope of T4.1, but this activity may be performed later in the T4.3 and the outcome described in D4.3.

2.2.4. Safety document

The following documents are part of the scope of the safety activities for the AWARD project. Each document will be applicable for the four platforms included in the AWARD project:

- Safety plan
- Hazard Analysis and Risk Assessment (§3)
- Functional Safety Concept (§4)
- Technical Safety Concept (§5).

2.3. Concept phase

2.3.1. Item definition

ISO 26262-3:2018 (5.4.)

The AWARD project includes four item definitions for each platform of the project and are defined in the WP2.

2.3.2. Hazard Analysis and Risk Assessment

2.3.2.1. HARA report

ISO 26262-3:2018 (6.4.1 – 6.4.5.)

Hazard Analysis and Risk Assessment (HARA) is an inductive approach in which the starting point is the list of malfunctions that may occur at the item's functions level, due to potential failures of the related elements (E/E elements).

Starting from the main functions of the four platforms described in the item definition and the associated malfunctions (potential failures of the function), the HARA identifies the potential effects (= Functional Hazardous Event or FHE).

Then, for each identified FHE, the HARA allows to define Safety goals and their assigned ASILs (as defined in the ISO 26262 standard) related to the prevention or mitigation of the associated FHE.

In order to identify the Safety Goals (SG), the analysis considers the following top-level safety needs:

- Ensure the safety of the passengers, other road participants and the safety operator.
- Identify, detect, monitor, limit... any malfunctioning behavior that can occur.
- And then put the ADV into a Safe mode.

The Safety Goals should cover all the use cases of the four platforms that are in the scope of AWARD project.

2.3.2.2. Verification report of the HARA

This activity is described in section 4.2 HARA coverage report. This report determines how each safety goal determined in the HARA is covered by a FSC.

2.3.3. Functional Safety Concept

2.3.3.1. Functional Safety Report

ISO 26262-3 (7.4.1-3)

Starting from the Safety Goals, the Functional Safety Concepts aim to specify the Functional Safety Requirements (FSR).

FSC should refine, decompose the associated ASIL attributes and allocate to every element of the ATS's subsystem the FSR that are necessary to achieve the SG.

ASIL tailoring and decomposition follows the ISO26262 rules and requirements.

2.3.3.2. Verification report of the Functional Safety Concept

FSR are exported in the AWARD D3.1 – Architecture-design-report and the verification report will be done in the "D4.5 – Safety Evaluation report: Compliance report".

2.4. Product development at system level

2.4.1. Technical Safety Concept

2.4.1.1. Technical safety requirement specification

ISO 26262-4:2018 (6.4.1 & 6.4.2.)

The Technical Safety Requirement will be described in the Technical Safety Concept document. TSR will be derived from the FSC and will be allocated to ADS system elements for implementation by the system design.

Due to the maturity of the project, no TSR will be provided but only technical detail about the different concepts.

2.4.1.2. System Architectural Design Specification

ISO 26262-4:2018 (6.4.3 - 6.4.6.)

The system architectural design specification has been performed through an iterative process in collaboration with the safety activities.

The outcome of this task can be found in the deliverable AWARD-D3.1-Architecture-Design-Report.

3. Hazard Analysis and Risk Assessment

3.1. Template and methodology

3.1.1. Inputs

To identify the risk related to the different AWARD use cases, the list of the operational situation was analyzed.

This list of operational situations was defined in the WP2.3 and summarized in table 4.1 of the document AWARD-D2.3-Use-cases-specification_1.0.docx.

- Columns A “OS ID”: ID of the operational situation
- Columns F “Operational situation”: Description of the operational situation.

Each operational situation is applicable to one or more use cases.

- Columns B “UC1 Automated forklift”: There is a cross in the cell if the OS is applicable.
- Columns C “UC2 Hub to hub”: There is a cross in the cell if the OS is applicable.
- Columns D “UC3 Baggage tractor”: There is a cross in the cell if the OS is applicable.
- Columns E “UC4 Container transfer”: There is a cross in the cell if the OS is applicable.

For each operational situation and use case, the different interactions that could have an impact on the safety are defined.

- Column H “Interaction”: Description of the possible interaction with the autonomous heavy truck and the surrounding environment.

The following object, pedestrian or other road users has been considered in the HARA:

- massive static object;
- pedestrian and workers;
- truck;
- Forklift;
- baggage tractor;
- passenger car;
- bicycle and motorcycle.

3.1.2. Hazard analysis

Before assessing the risk, all the hazard related to the different operational situation and use cases shall be identified.

The hazard identification is done by combination of:

- Column I “Function / Expected behavior”: Description of the autonomous driving system feature.
- Column J “Functional failure mode”: Description the failure mode related to the function.
- Column K “Exposed persons”: Description of the people concerned by the hazard.

The result of this analysis is:

- Column L “Hazard”: Description of the hazard related to the functional failure more combined with the operational situation.
- Column M “Potential effect”: Description of the potential effects of the hazard.

3.1.3. Hazard assessment

The last step consists in evaluating the risk according the ISO26262 criteria:

- Column N and O “Severity” and “Severity Comment”: Severity ASIL quotation and related comment about the delta speed between the autonomous heavy truck and the related interaction.
- Because the scope of the ISO26262 is not the same as the AWARD project, a severity matrix was defined to assess the risk severity related to each ADV platform.
- These severity matrixes took into account each platform characteristic regarding the risk of collision with different obstacles (other road users or pedestrian).
- Column P and Q “Exposure and Exposure Comment”: Exposure ASIL quotation and the related comment.
- Column R and S “Controllability and Controllability Comment”: Controllability ASIL quotation and the related comment.

According to the ASIL matrix definition in the ISO26262, the result of the severity, exposure and controllability was defined in:

- Column T “ASIL”: Related integrity level.

To mitigate the risk related to the hazard a safety goal was defined:

- Column U “Safety Goal” Requirement at system level to mitigate the hazard.

3.2. Safety goals

Table 1 describes all the safety goals that have been identified during the HARA. For each safety goal the related integrity level and the list of the applicable use cases are defined.

Table 1: Safety goal list

ID	*ASIL*	*Safety Goal*	*UC*
	Collision with massive and static object		
SG01-1	A	ADV shall avoid collision with massive and static object on the trajectory when driving at 20 km/h on a company site	2/4
SG01-2	B	ADV shall avoid collision with passenger car stop on the trajectory when driving on a public road at 20 km/h	2/4
SG01-3	C	ADV shall avoid collision with passenger car stop on the trajectory when driving on a public road at 40 km/h	2/4
SG01-4	A	ADV shall avoid collision with other road users stop on the trajectory when driving at 10 km/h on a private road	1/2/3/4
SG01-5	B	ADV shall avoid collision with passenger car stop on the trajectory when driving through a tunnel at 20 km/h	2/3
	Collision with pedestrian		
SG02-1	C	ADV shall avoid collision with pedestrian on the trajectory when driving at 10 km/h on a company site	2/4

SG02-2	C	ADV shall avoid collision with pedestrian crossing a public road when driving at 20 km/h or 40 km/h	2/4
SG02-3	C	ADV shall avoid collision with pedestrian crossing a private road when driving at 10 km/h	1/2/3/4
	Collision with another vehicle		
SG03-1	QM	ADV shall avoid collision with another truck stop on the trajectory when driving at 10 km/h on a company site	2/4
SG03-2	A	ADV shall avoid collision with passenger car stop on the trajectory when driving at 10 km/h on a company site	2/4
SG03-3	A	ADV shall avoid collision with forklift on the trajectory stop on the trajectory when driving on a company site	2/4
SG03-4	C	ADV shall avoid collision with other road user stop on the trajectory when driving on a public at 40 km/h	2/4
SG03-5	A	ADV shall avoid collision with other road user stop on the trajectory when driving at 10 km/h on a private road	1/3
	Lateral deviation leading to collision		
SG04-1	D	ADV shall avoid lateral deviation from the navigation lane when driving on a company site at 10 km/h	2/4
SG04-2	D	ADV shall avoid lateral deviation from the navigation lane when driving at 20 km/h on a public road	2/4
SG04-3	C	ADV shall avoid lateral deviation from the navigation lane when driving at 10 km/h on a private road	1/2/3/4
	Crossing intersection		
SG05-1	D	ADV shall decelerate and reach standstill before intersection with public road and other road users driving at 50 km/h	2/4
SG05-2	D	ADV shall not cross intersection with public road if there is oncoming vehicle on the path and other road users driving at 50 km/h	2/4
SG05-3	D	ADV shall decelerate and reach standstill before intersection when the connected traffic light is red and other road users driving at 50 km/h	2
SG05-4	D	ADV shall not cross intersection if the connected traffic light is red and other road users driving at 50 km/h	2
SG05-5	A	ADV shall decelerate and reach standstill before intersection with private road	3
SG05-6	A	ADV shall not cross intersection with private road if there is oncoming vehicle on the path	3
SG05-7	C	ADV shall decelerate and reach standstill before intersection with priority given on a public road	2
SG05-8	C	ADV shall not cross intersection with public road if there is oncoming vehicle on the path	2
SG05-9	A	ADV shall decelerate and reach standstill before intersection with priority given on a private road	3
SG05-10	A	ADV shall not cross intersection with private road if there is oncoming vehicle on the path	3
	Unexpected braking leading to rear collision		
SG06-1	C	ADV shall avoid unexpected deceleration when driving at 20 km/h on a public road	2/4

SG06-2	A	ADV shall avoid unexpected deceleration when driving at 10 km/h on a private road	1/2/3/4
SG06-3	A	ADV shall avoid unexpected deceleration when driving at 10 km/h on a compound site	2/4
	Uncoupling trailer		
SG07-1	B	ADV shall not uncoupling trailer when driving on a private road	3
SG07-2	D	ADV shall not uncoupling trailer when driving on a public road	3
	Approaching the ramp		
SG08-1	C	ADV shall avoid lateral deviation when approaching the ramp	2/3/4
SG08-2	C	ADV shall avoid collision with pedestrian when approaching the ramp	2/3/4
	Passing an obstacle		
SG09-1	A	ADV shall determine correct path and correct timing to pass an obstacle on a private road	1/2/3/4
SG09-2	C	ADV shall determine correct path and correct timing to pass an obstacle on a public road	2/4
	Active status emergency		
SG10-1	A	ADV shall abort the mission and stop in case of Active status emergency safe	1/2/3/4
SG10-2	A	ADV shall abort the mission and drive to a safe zone in case of Active status emergency safe	1/2/3/4

Due to the operational situation and the use cases modification, the following safety goals are not applicable anymore to the AWARD project:

- uncoupling trailer (SG07-1/SG07-2);
- passing an obstacle (SG09-1/SG09-2);
- active status emergency (SG10-1/SG10-2).

4. Functional Safety Concept

4.1. Methodology

Functional safety concepts are performed through an iterative process in collaboration with task T3.1.

The preliminary architecture provided in T3.1 is used as an input to describe each concept to mitigate each risk identified in the hazard analysis and risk assessment.

Each safety goal shall be covered by a safety concept, but a safety concept can mitigate several safety goals.

Then the functional safety concept is achieved through the following steps:

- functional fault tree analysis and minimal cut set determination based on the preliminary architecture;
- ASIL allocation to ADS subsystem ;
- determination of the functional safety requirements.

So, the output of the functional safety concepts is a list of functional safety requirements allocated to the different ADS subsystems.

4.2. HARA coverage report

Table 2: HARA coverage table

Safety Goal	SG ID	FSC
Collision with massive and static object	SG01-1/SG01-2/SG01-3/SG01-4/SG01-5	Collision avoidance
Collision with pedestrian	SG02-1/SG02-2/SG02-3/SG02-4	Collision avoidance
Collision with another vehicle	SG03-1/SG03-2/SG03-3/SG03-4/SG03-5	Collision avoidance
Lateral deviation leading to collision	SG04-1/SG04-2/SG04-3	Trajectory following
Crossing intersection	SG05-1/SG05-2/SG05-3/ SG05-4/ SG05-5/ SG05-6/ SG05-7/ SG05-8/ SG05-9/ SG05-10	Crossing intersection with traffic light
Unexpected braking leading to rear collision	SG06-1/SG06-2/SG06-3	Collision avoidance
Uncoupling trailer	SG07-1/SG07-2	Non Applicable
Approaching the ramp	SG08-1	Trajectory following
Approaching the ramp	SG08-2	Collision avoidance
Passing an obstacle	SG09-1/SG09-2	Non Applicable
Active status emergency	SG10-1/SG10-2	Non Applicable

4.3. Collision avoidance

4.3.1. Safety goal

The FSC: Collision avoidance allow to mitigate all the situation related to the risk of collision and cover the following safety goals:

- Collision with massive and static object (SG01-1/SG01-2/SG01-3/SG01-4/SG01-5)
- Collision with pedestrian (SG02-1/SG02-2/SG02-3/SG02-4)
- Collision with another vehicle (SG03-1/SG03-2/SG03-3/SG03-4/SG03-5)
- Unexpected braking leading to rear collision (SG06-1/SG06-2/SG06-3)
- Approaching the ramp (SG08-2).

According to the risk analysis, the collision avoidance feature shall be compliant with the higher ASIL of the above safety goals list.

The ADV shall avoid collision with an obstacle – ASIL C.

4.3.2. ASIL allocation

Based on the preliminary architecture defined in D3.1 chapter 4.2.3.2 “Collision avoidance”, a fault tree analysis was performed to define the ASIL allocation to the different ADV subsystems. The top event is the risk of collision and then the fault tree was broken down to the different component failures that could lead to a collision with an obstacle. The outcome of the fault tree analysis is the following cut set (figure 4).

Executive Summary | Importance | Minimal cuts set | Probabilities | Sensitivity

N°	Quantity	Probability	Percent	Events			
1	1	0	0	Speed fdbk failure			
2	2	0	0	EM sensors failure	Mapping failure		
3	2	0	0	Mapping failure	Steering fdbk failure		
4	3	0	0	Conti Sen failure	EM sensors failure	Foresight Sen failure	
5	3	0	0	Adasky camera	EM sensors failure	Foresight Sen failure	
6	3	0	0	Adasky camera	Conti Sen failure	EM sensors failure	
7	4	0	0	Adasky camera	Conti Sen failure	Foresight Sen failure	Steering fdbk failure
8	1	0	0	ADS Act failure			
9	1	0	0	ADV Platform failure			

Figure 4: Collision avoidance minimal cut set

According to the fault tree analysis related to collision avoidance feature, these cut sets have been identified:

- Platform speed feedback failure
- ADS Act failure
- ADV platform braking failure.

Each cut set is related to a subsystem failure.

Based on this analysis and the identification of the minimal cut set, the ASIL allocation to the subsystem has been performed and is described in the below block diagram (figure 5).

If a minimal cut set has been identified as a potential subsystem failure, the consequence is that there is not ASIL decomposition allowed for this subsystem.

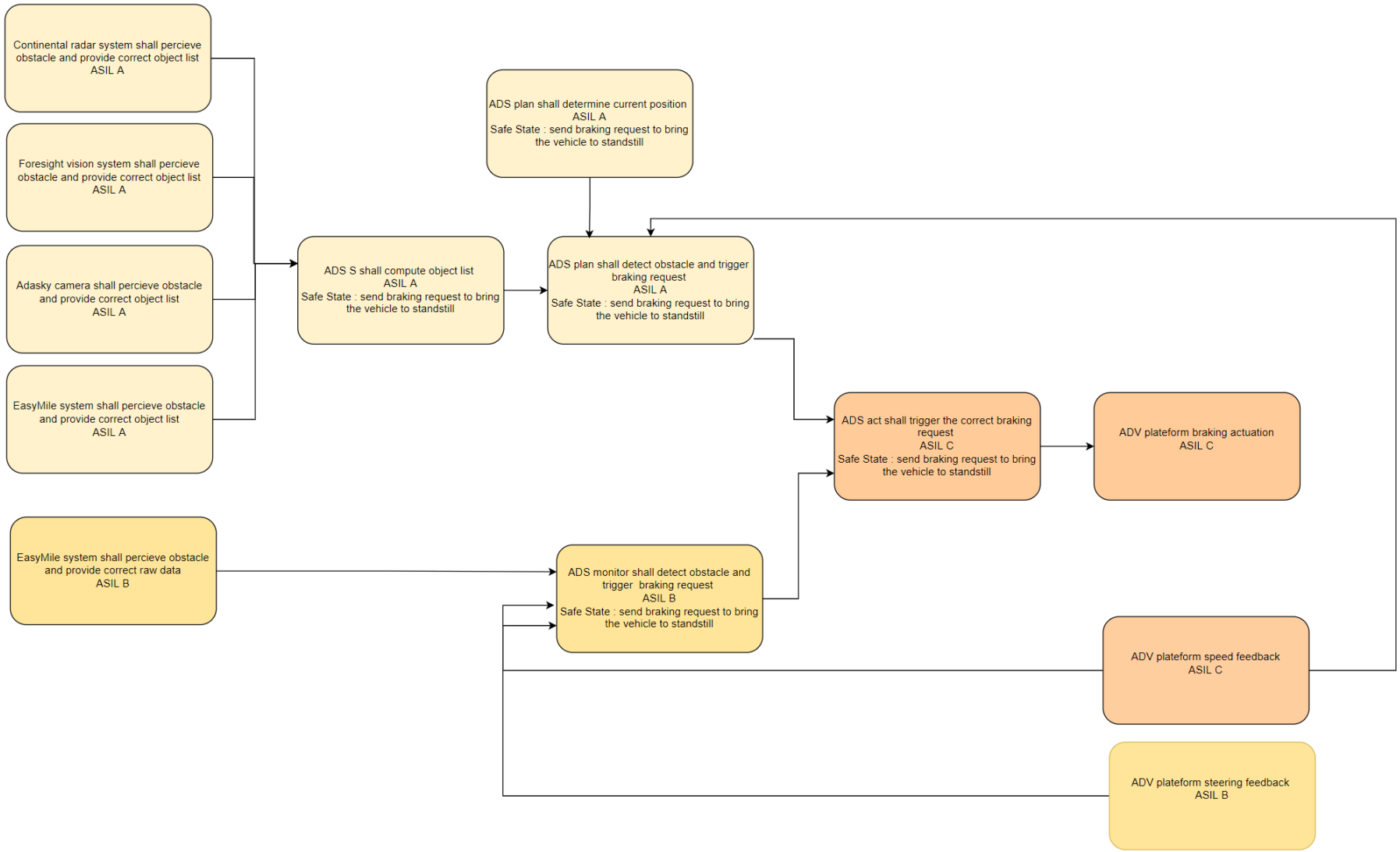


Figure 5: Collision avoidance ASIL allocation

4.3.3. Functional safety requirement

Based on the ASIL allocation and the preliminary architecture, a list of functional safety requirements was defined (table 3). Each functional safety requirement is allocated to an ADV subsystem and shall be compliant with a level of integrity (ASIL).

The implementation of all these functional safety requirements with the correct level of integrity will allow the ADV system to mitigate the risk of collision identified in the hazard analysis and risk assessment.

Table 3: Collision avoidance functional safety requirements

Topic	Text	ASIL	Allocation
Collision Avoidance	Provide radar object list & attributes	A(C)	Continental radar System
	Provide vision object list & attributes	A(C)	Foresight vision System
	Provide thermal vision object list & attributes	A(C)	Adasky camera
	Provide object list & attributes	A(C)	EasyMile System
	Provide raw lidar data	B(C)	
	Compute consolidated object list	A(C)	ADS Sense
	Localize ADV	A(C)	
	Predict obstacle movement	A(C)	ADS Plan
	Evaluate collision risk with obstacle	A(C)	
	Compute optimal speed command	A(C)	
	Evaluate collision risk with obstacle	B(C)	ADS Monitor
	Trigger safe state request	B(C)	
	Get steering feedback	B(C)	ADS Act
	Get speed feedback	C(C)	
	Forward speed command to platform	A(C)	
	Decide to forward safe state request	B(C)	
	Apply requested speed command	C(C)	ADV platform
	Provide speed feedback	C(C)	
	Provide steering feedback	B(C)	

4.4. Trajectory following

4.4.1. Safety goal

The FSC: Trajectory following allow to mitigate all the situation related to the risk of trajectory deviation and cover the following safety goals:

- Lateral deviation leading to collision (SG04-1/SG04-2/SG04-3)

- Approaching the ramp (SG08-1)

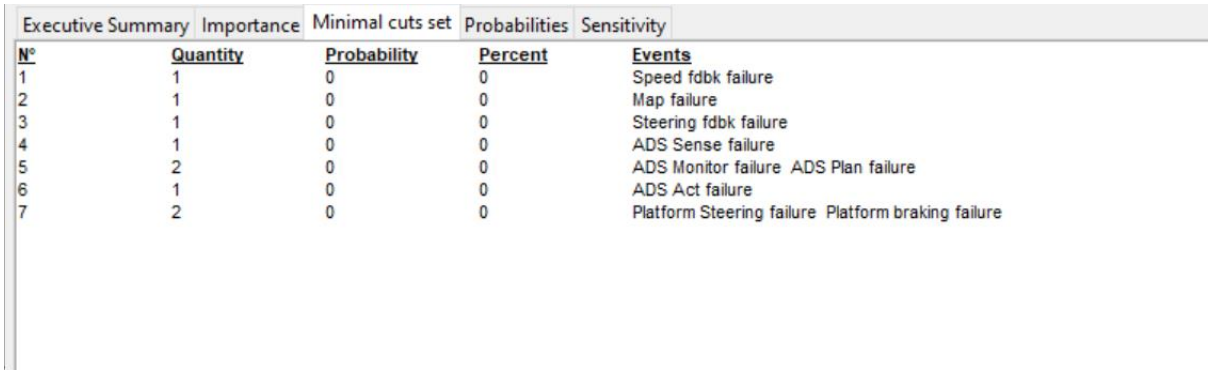
According to the risk analysis, the trajectory following feature shall be compliant with the higher ASIL of the above safety goals list:

AV truck shall avoid lateral deviation from the navigation lane - ASIL D.

4.4.2. ASIL allocation

Based on the preliminary architecture defined in D3.1 chapter 4.2.3.3 “Trajectory following”, a fault tree analysis was performed to define the ASIL allocation to the different ADV subsystems. The top event is the risk trajectory deviation, and then, the fault tree was broken down to the different component failures that could lead to a trajectory deviation.

The outcome of the fault tree analysis is the following cut set (figure 6):


Executive Summary | Importance | Minimal cuts set | Probabilities | Sensitivity

N°	Quantity	Probability	Percent	Events
1	1	0	0	Speed fdbk failure
2	1	0	0	Map failure
3	1	0	0	Steering fdbk failure
4	1	0	0	ADS Sense failure
5	2	0	0	ADS Monitor failure ADS Plan failure
6	1	0	0	ADS Act failure
7	2	0	0	Platform Steering failure Platform braking failure

Figure 6: Lateral deviation minimal cut set

According to the fault tree analysis related to collision avoidance feature, these cut sets have been identified:

- Platform speed feedback failure
- Platform steering feedback failure
- Map failure
- ADS Sense failure
- ADS Act failure
- ADV platform braking failure

Each cut set is related to a subsystem failure.

Based on this analysis and the identification of the minimal cut set, the ASIL allocation to the subsystem has been performed and is described in the below block diagram (figure 7). If a minimal cut set has been identified as a potential subsystem failure, the consequence is that there is not ASIL decomposition allowed for this subsystem.

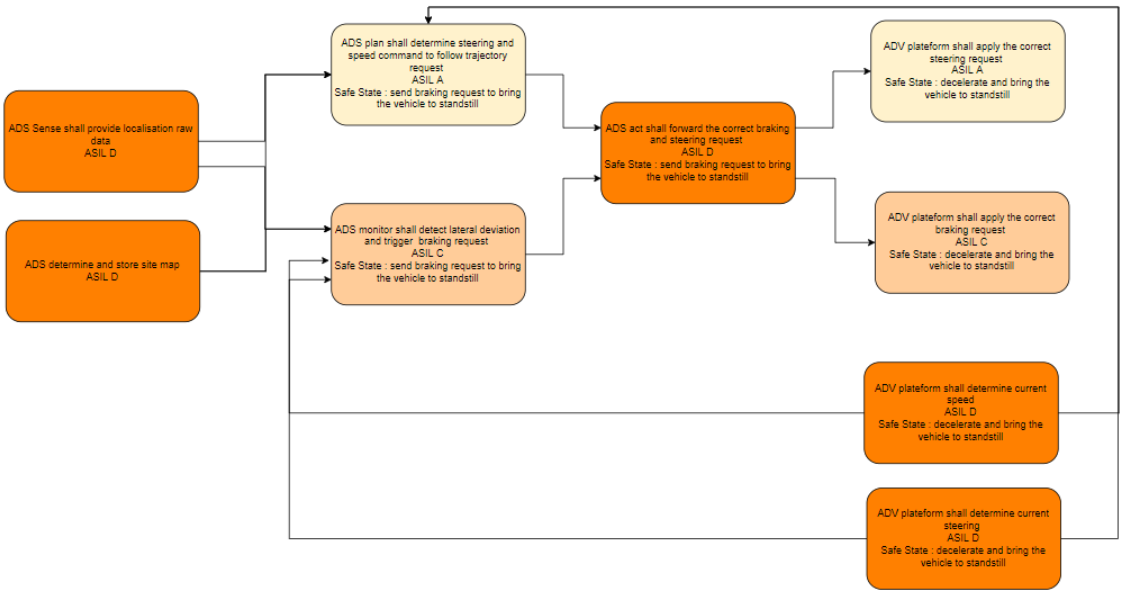


Figure 7: Lateral deviation ASIL allocation

4.4.3. Functional safety requirement

Based on the ASIL allocation and the preliminary architecture, a list of functional safety requirements has been defined (table 4).

Each functional safety requirement is allocated to an ADV subsystem and shall be compliant with a level of integrity (ASIL).

The implementation of all these functional safety requirements with the correct level of integrity will allow the ADV system to mitigate the risk of collision identified in the hazard analysis and risk assessment.

Table 4: Collision avoidance functional safety requirements

Topic	Text	ASIL	Allocation
Trajectory deviation detection	Provide stored site map	D(D)	ADS
	Localize ADV	D(D)	ADS Sense
	Determine commands to follow predefined trajectory	A(D)	ADS Plan
	Compute optimal steering command	A(D)	
	Compute optimal speed command	A(D)	
	Project the AV trajectory	C(D)	ADS Monitor
	Trigger safe state request	C(D)	
	Get steering feedback	C(D)	ADS Act
	Get speed feedback	C(D)	
	Forward speed and steering command to platform	A(D)	
	Decide to forward safe state request	C(D)	

	Apply requested steering command	A(D)	ADV platform
	Apply requested speed command	C(D)	
	Provide speed feedback	D(D)	
	Provide steering feedback	D(D)	

4.5. Crossing intersection with traffic light

4.5.1. Safety goal

The FSC: Crossing intersection with traffic light allow to mitigate all the situation related to the risk of unexpected intersection crossing and cover the following safety goals:

Crossing intersection (SG05-1/SG05-2/SG05-3/ SG05-4/ SG05-5/ SG05-6/ SG05-7/ SG05-8/ SG05-9/ SG05-10)

According to the risk analysis, the trajectory following feature shall be compliant with the higher ASIL of the above safety goals list:

AV truck shall avoid lateral deviation from the navigation lane – ASIL D.

4.5.2. ASIL allocation

Based on the preliminary architecture defined in D3.1 chapter 4.2.3.2 "Crossing intersection with traffic light", a fault tree analysis was performed to define the ASIL allocation to the different ADV subsystem. The top event is the risk of collision when crossing an intersection with traffic light, and then the fault tree is broken down to the different component failures that could lead to a collision when crossing an intersection with traffic light. The outcome of the fault tree analysis is the following cut sets (figure 8).

Executive Summary | Importance | Minimal cuts set | Probabilities | Sensitivity

N°	Quantity	Probability	Percent	Events
1	2	0	0	ADS Monitor failure ADS Plan failure
2	1	0	0	ADS traffic light acquisition failure
3	1	0	0	Map failure
4	1	0	0	ADS Act failure
5	1	0	0	Traffic light status failure
6	1	0	0	Platform speed fdbk failure
7	1	0	0	Platform braking failure

Figure 8: Minimal cut set Crossing intersection with traffic light

According to the fault tree analysis related to collision avoidance feature, these cut sets have been identified:

- ADS traffic light failure
- Platform speed feedback failure
- Map failure
- ADS Sense failure
- ADS Act failure
- ADV platform braking failure.

Based on this analysis and the identification of the minimal cut set, the ASIL allocation to the subsystem was performed and is described in the block diagram below (figure 9).

If a minimal cut set has been identified as a potential subsystem failure, the consequence is that there is not ASIL decomposition allowed for this subsystem.

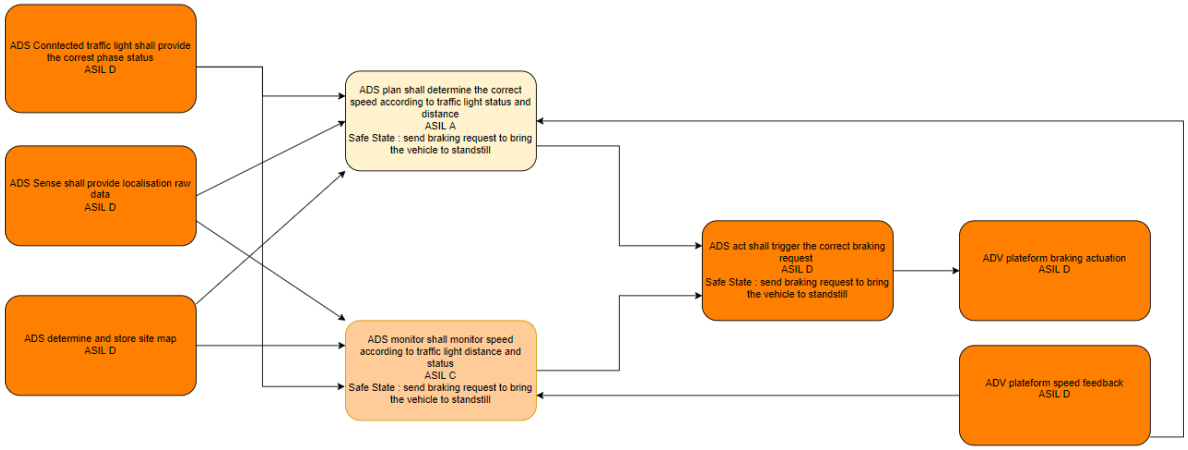


Figure 9: Crossing intersection with traffic light

4.5.3. Functional safety requirement

Based on the ASIL allocation and the preliminary architecture, a list of functional safety requirements was defined (table 5). Each functional safety requirement is allocated to an ADV subsystem and shall be compliant with a level of integrity (ASIL).

The implementation of all these functional safety requirements with the correct level of integrity will allow the ADV system to mitigate the risk related to unexpected intersection crossing identified in the hazard analysis and risk assessment.

Table 5: FSR Crossing intersection with traffic light

Topic	Text	ASIL	Allocation
Crossing intersections with traffic lights	Provide stored site map	D(D)	ADS
	Localize ADV	D(D)	ADS Sense
	[RSU] Provide current status of traffic light	D(D)	SI
	Determine AV speed according traffic light status	A(D)	ADS Plan
	Monitor AV speed according traffic light status	C(D)	ADS Monitor
	Trigger safe state request	C(D)	
	Forward speed command to platform	A(D)	ADS Act
	Decide to forward safe state request	C(D)	
	Apply requested speed command	D(D)	ADV platform
	Provide speed feedback	A(D)	

5. Technical safety concept

5.1. Methodology

Usually, the purpose of this part is to refine the functional safety requirements in a list of technical requirements. But in the scope of AWARD project, the goal of this part would not be to define a list of technical safety requirements. Indeed, due to intellectual property it is not possible to publish low level requirements about internal algorithms.

Instead of the list of low-level safety requirement, this chapter explains how the different safety concepts allow to mitigate the different risks that have been determined in the previous chapter.

Safety concepts with technical information are detailed below to explain the behavior of the following functional requirements:

- Evaluate collision risk with obstacle and trigger a safe state
- Localize ADV
- Monitor AV speed according traffic light status
- Project the AV trajectory and trigger a safe state.

5.2. Evaluate collision risk with obstacle and trigger a safe state

5.2.1. TSC overview

As a system, AWARD ADS shall perceive and detect obstacles on the vehicle trajectory to mitigate and avoid any risk of collision.

The technical safety concept related to the collision avoidance feature is performed by the two following subfunctions:

- Nominal collision avoidance (Evaluate collision risk with obstacles by ADS Plan)
- Emergency collision avoidance (Evaluate collision risk with obstacles by ADS Monitor)

Obstacles are detected within virtual areas, called surveillance areas:

- Nominal surveillance area related to the nominal collision avoidance function
- Emergency surveillance area related to the emergency collision avoidance function

Both areas are dynamic, the size and the direction of the surveillance area will change according to different inputs (planned trajectory, vehicle speed or current steering).

As soon as an obstacle is detected in the nominal or emergency surveillance area, a braking request is sent to the ADV Platform to avoid the collision.

5.3. Localize ADV

5.3.1. TSC overview

As a system, AWARD ADS shall ensure a VHC safe localization meaning it should provide a reliable and safe localization estimation to ADS Plan and ADS Monitor.

The technical safety concept related to the localization feature is performed by the two following subfunctions:

- Determine the current position by fusion
- Monitor the localization consistency

If the consistency monitoring passed, the current position can be used, but if the consistency monitoring failed, then the system shall trigger a safe state.

Monitor the localization consistency feature consists in comparison of fusion results (position & uncertainty) with unitary localization modalities:

- Absolute position provided by Continental radar
- Absolute position provided by Navtech radar
- Absolute position provided by LIDARS (SLAM)
- Absolute position provided by Vision System
- Absolute position provided by GNSS
- Relative position provided by Odometry.

5.4. Monitor AV speed according traffic light status

5.4.1. TSC overview

The principle of safe intersection crossing with connected traffic light is defined as follows:

- The AV receives information from the traffic light (phase and remaining time for the current phase) thanks to a communication protocol between RoadSide Unit (RSU) and On Board Unit (OBU).
- The OBU provides a Signal Phase and Timing message to both Nominal and Emergency Intersection crossing functions which are then able to safely manage the intersection crossing.
- Signal Phase is used by the Nominal Intersection crossing function to stop at the traffic light if the remaining time is not sufficient to cross the intersection.
- The Emergency Intersection crossing shall monitor the *Nominal Intersection crossing* function and ensure that the deceleration is sufficient to safely reach the ultimate stopping position.

5.5. Project the AV trajectory and trigger a safe state

5.5.1. TSC overview

The safety concept is ensured by two features:

- The navigation command by ADS Plan will determine and send to the platform the correct steering and acceleration request.
- The lateral trajectory deviation avoidance by ADS Monitor will monitor the vehicle trajectory and react with a braking request if a risk of deviation has been identified.

In addition, the ADS Plan will also monitor the vehicle trajectory through the feature "Determine commands to follow predefined trajectory". In case of vehicle lateral deviation, the ADS Plan will also react by sending braking requests to the platform.

To determine the steering and the acceleration command, the ADS Plan will use the current localization information and will determine the trajectory *via* the cartography stored in the ADS Plan memory ("provide stored site map" feature).

The "Lateral trajectory deviation avoidance" function shall ensure the monitoring of the vehicle trajectory regarding:

- The predefined trajectory and current section of the path (including information about this section, e.g., lane width). This information about the correct trajectory is named "navigation lane area" and is stored in the ADS Monitor memory.
- The current absolute position. This information is provided by the localization feature.
- The current speed and steering values. This information is provided by the platform.

In case of the "Lateral trajectory deviation avoidance" function detect a risk of trajectory deviation; the feature will trigger a safe state to bring the vehicle to standstill.

6. Conclusion

This deliverable D4.6 proposes a safety architecture and allocation guided by the preliminary architecture from D3.1 Architecture design report. The safety allocation has been managed following the ISO 26262 standard and is based on three main activities:

- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept.

The scope and the outcome of these safety activities are strictly limited to the Operational Domain Design described in D2.3 Use cases specification.

The purpose of these safety activities described in the document is to propose a list of safety requirements and concepts allocated to the ADS subsystem to mitigate all the risks that could have an impact on the people safety.

So, to conclude, this list of safety requirements and concepts shall be implemented with the related integrity level described in this deliverable in order to design a safe ADS for the expected ODD.

7. References

[1] AWARD D3.1-Architecture-design-report

[2] AWARD D2.3-Use-cases-specification

[3] ISO26262 Road vehicles – Functional safety