ENSEMBLE

EUROPEAN COMMISSION

HORIZON 2020
H2020-ART-2016-2017/H2020-ART-2017-Two-Stages
GA No. 769115

ENSEMBLE

ENabling **S**af**E** **M**ulti-**B**rand p**L**atooning for **E**urope

Deliverable No.	D2.11	
Deliverable Title	First version Hazard Analysis and Risk Assessment and Functional Safety Concept	
Dissemination level	Public	
Written By	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	[22-02-2019]
Checked by	Lina Konstantinopoulou, CLEPA	[27-02-2019]
Approved by	Marika Hoedemaeker, TNO]	[06-03-2019]

Status	Final, approved by EC	[08-03-2019]

Please refer to this document as:

Mengani, L., Dhurjati, P., 2019. *Hazard Analysis and Risk Assessment and Functional Safety Concept, D2.11* of H2020 project ENSEMBLE, (www.platooningensemble.eu)

Disclaimer:

ENSEMBLE is co-funded by the European Commission, DG Research and Innovation, in the HORIZON 2020 Programme. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

TABLE OF CONTENTS

Revision history

Version	Date	Author	Summary of changes	Status
0.1	27/11/2018	Luca Mengani, IDIADA HQ	Initial draft of the HARA for Platooning Level A based on previous activity “PL-A functions and malfunctioning behaviours”.	Prepared
0.2	30/11/2018	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	HARA template reviewed by all partners during the 1st Safety Workshop. HARA analysis performed together with all partners.	Prepared
0.3	28/12/2018	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	First release of the HARA for Platooning Level A based on 1st Safety Workshop feedbacks.	Prepared
0.4	14/01/2019	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	Calculation of TTC reviewed and ASIL determination in HARA Template automated	Prepared
0.5	22/02/2019	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	Second release of the HARA for Platooning Level A based on 2nd Safety Workshop feedbacks.	Prepared
0.6	22/02/2019	Luca Mengani, IDIADA HQ Prashanth Dhurjati, IDIADA UK	First release of D2.11 deliverable submitted for review	Prepared
0.7	27/02/2019	Marika Hoedemaeker, TNO and Lina	Review by WP2 and coordinator	

		Konstantinopoulou, CLEPA		
0.8	29/02/2019	Luca Mengani, IDIADA HQ	Deliverable reviewed according to WP2 and coordinator feedbacks	Reviewed

TABLES

FIGURES

1. Executive Summary

1.1 Context and need of a multi brand platooning project

Context

Platooning technology has made significant advances in the last decade, but to achieve the next step towards deployment of truck platooning, an integral multi-brand approach is required. Aiming for Europe-wide deployment of platooning, 'multi-brand' solutions are paramount. It is the ambition of ENSEMBLE to realise pre-standards for interoperability between trucks, platoons and logistics solution providers, to speed up actual market pick-up of (sub)system development and implementation and to enable harmonisation of legal frameworks in the member states.

Project scope

The main goal of the ENSEMBLE project is to pave the way for the adoption of multi-brand truck platooning in Europe to improve fuel economy, traffic safety and throughput. This will be demonstrated by driving up to seven differently branded trucks in one (or more) platoon(s) under real world traffic conditions across national borders. During the years, the project goals are:

- Year 1: setting the specifications and developing a reference design with acceptance criteria
- Year 2: implementing this reference design on the OEM own trucks as well as perform impact assessments with several criteria
- Year 3: focus on testing the multi-brand platoons on test tracks and international public roads

The technical results will be evaluated against the initial requirements. Also, the impact on fuel consumption, drivers and other road users will be established. In the end, all activities within the project aim to accelerate the deployment of multi-brand truck platooning in Europe.

1.2 Abstract of this Deliverable

The objective of D2.11 is identify the Hazard Analysis and Risk Assessment and Functional Safety Concept.

This deliverable consists of the following two work products:

- Hazard analysis and risk assessment

  The objectives of the HARA are:

  a. to identify and to categorise the hazardous events caused by malfunctioning behaviour of the "Platooning Level A" item;

b. and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

- Functional safety concept

  The objectives of the FSC are:

  a. to derive the functional safety requirements from the safety goals, and

  b. to allocate the functional safety requirements to the preliminary architectural elements of the item, or to external measures

A preliminary Hazard Analysis and Risk Assessment activity was carried out to understand the safety critical malfunctions arising from the platooning function Level A. Based on their associated risk, ASILs levels have been assigned and top-level safety requirements have been derived for the safety critical hazards in the form of safety goals.

The outcome of the Hazard analysis and risk assessment shows that the current Platooning Level A definition stated in the D2.2 deliverable is not consistent so that the functional safety concept activity in subsequent sub-phase cannot be performed.

In fact, time gaps below 2 seconds in the best case cannot be achieved while longitudinal control remains driver responsibility.

After several discussion, all partners have reached the conclusion that there are two possible project alternatives to proceed:

1. Support function: driver is responsible for longitudinal control so that platooning functionality is a help;

2. Full longitudinal automation: driver is not responsible, the system itself performs all longitudinal operations under certain conditions.

Further concept phase activities will be based on the alternative as chosen by the steering board.

2. Methodology

2.1 Functional Safety process

The primary purpose of this safety activity is to study and analyse the potential source of harm caused by malfunctioning behaviour of the Platooning Level A . To achieve functional safety, the safety activities follow the ISO26262 standard that provides a reference for the automotive safety lifecycle. The standard is based upon a V-model as a reference process model for the different phases of project development.

At this stage, the concept phase, the safety activities follow the ISO26262 part 3 and the top-level safety requirements resulting from this part are not expressed in terms of technological solutions, but in terms of functional objectives.

The functional safety lifecycle related to the concept phase is represented below:

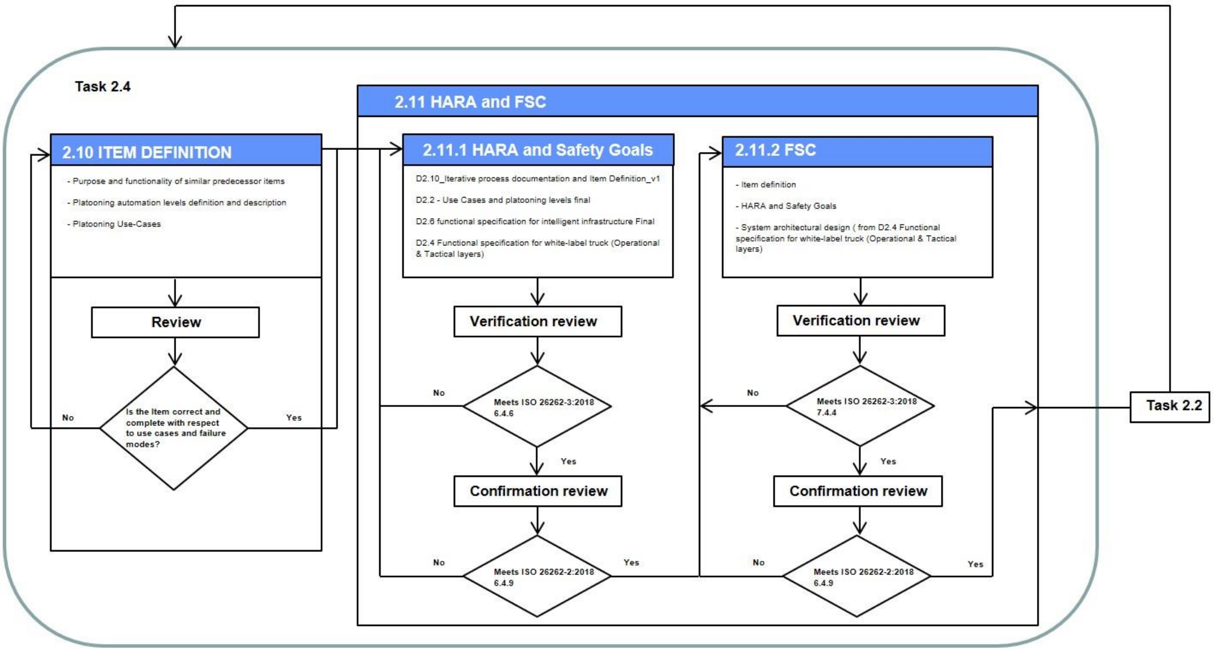

Task 2.4
2.11 HARA and FSC
2.10 ITEM DEFINITION
- Purpose and functionality of similar predecessor items
- Platooning automation levels definition and description
- Platooning Use-Cases
Review
Is the Item correct and complete with respect to use cases and failure modes?
No
Yes
2.11.1 HARA and Safety Goals
D2.10_Iterative process documentation and Item Definition_v1
D2.2 - Use Cases and platooning levels final
D2.6 functional specification for intelligent infrastructure Final
D2.4 Functional specification for white-label truck (Operational & Tactical layers)
Verification review
No
Meets ISO 26262-3:2018 6.4.6
Yes
Confirmation review
No
Meets ISO 26262-2:2018 6.4.9
Yes
2.11.2 FSC
- Item definition
- HARA and Safety Goals
- System architectural design (from D2.4 Functional specification for white-label truck (Operational & Tactical layers)
Verification review
No
Meets ISO 26262-3:2018 7.4.4
Yes
Confirmation review
No
Meets ISO 26262-2:2018 6.4.9
Yes
Task 2.2

Figure 1 Functional Safety lifecycle related to the concept phase

The first activity relating to this deliverable is the hazard analysis and risk assessment which considers the available information concerning the Item. After completing the HARA and their associated safety goals, then the verification review activity takes place to ensure the technical correctness and completeness of the Platooning Level A with respect to the use-cases. This verification review can be performed by using different methods such as technical review, walk-through or inspection. In case the technical part is correct and complete, a confirmation review to check the correctness with respect to formality, contents, adequacy and completeness regarding the requirements of ISO 26262 is performed. Once the HARA and Safety Goals is completed, the functional safety concept activity is performed, followed by the verification and confirmation review activities, as for the previous one.

Input to this deliverable are the item definition, uses cases, functional specification and platooning level A definition. Considering the previously available information, the first draft of the Platooning Level A functions and malfunctioning behaviours is created together with all the partners supported by brainstorming sessions through conference calls.

On this basis, the first version of the Hazard Analysis and Assessment is created and reviewed together with all the partners during the 1st safety workshop. Subsequent verification review sessions to verify the appropriate selection regarding the driving situations and hazard identification, compliance with the Platooning Level A definition and use-cases descriptions are performed. The objective of this verification reviews is to check the hazard analysis and risk assessment of the Platooning level A for correctness and completeness evaluating the considered assumptions, operational situations, hazards and estimated parameters severity, probability of exposure and controllability.

In order to meet ISO26262 verification review requirements, a 2nd safety workshop took place. During this workshop the most critical hazards were identified and studied, including the criteria to evaluate the time to collision and the minimum deceleration values required to avoid collision according to the partners experiences. After this verification activity, the second version of the HARA was released.

Once the HARA analysis will be agreed and completed, the next step is to formally check if its procedure complies with the requirements of ISO26262 through the confirmation review activity.

In accordance with the ISO26262-3:2018 Annex B, a risk (*R*) can be described as a function (*F*) of:

- the frequency of occurrence (*f*) of a hazardous event, and that in turn is influenced by the probability of exposure (*E*) of each operational situation and the failure rate (λ) of the item:

  $f = E \times \lambda$

- the controllability (*C*), that is the ability to avoid physical injury or damage to the health of persons through timely reactions of the persons involved, and

- the potential severity (*S*) of the resulting injury or damage

$R = F(f, C, S)$

Hazard analysis and risk assessment determine the minimum set of requirements on the item, in order to avoid unreasonable risk.

The failure rate of the item is not considered a priori in the risk assessment because an unreasonable residual risk is avoided through the implementation of the resulting safety requirements.

The hazard analysis and risk assessment sub phase comprises of three steps:

1) *Hazard identification:* The goal of the situation analysis and hazard identification is to identify the potential unintended behaviours of the item that could lead to a hazardous event. The situation analysis and hazard identification activity is based on the item's behaviour; therefore a clear definition of the item, its functionality and its boundaries is needed.

2) *Hazard classification*: The hazard classification comprises the determination of the severity, the probability of exposure, and the controllability associated with the hazardous events of the Platooning Level A item. The severity represents an estimate of the potential harm in a particular driving situation, while the probability of exposure is determined by the corresponding situation. The controllability rates how easy or difficult it is for the driver or other road traffic participant to avoid the considered accident type in the considered operational situation. For each hazard, depending on the number of related hazardous events, the classification will result in one or more combinations of severity, probability of exposure, and controllability.

3) *ASIL determination*: Determining the required automotive safety integrity level. ISO26262 defines four ASILs: ASIL A, ASIL B, ASIL C and ASIL D, where ASIL A is the lowest safety integrity level and ASIL D the highest one. n addition to these four ASILs, the class QM (quality management) denotes no requirement to comply with ISO 26262.

2.1.1 Hazard identification

Hazard identification is supported through a functional hazard and operability analysis (HAZOP). This is a structured and systematic technique for identifying and evaluating malfunctioning behaviours of the item that could lead to hazards that create the potential for physical injury or damage to the health of persons.

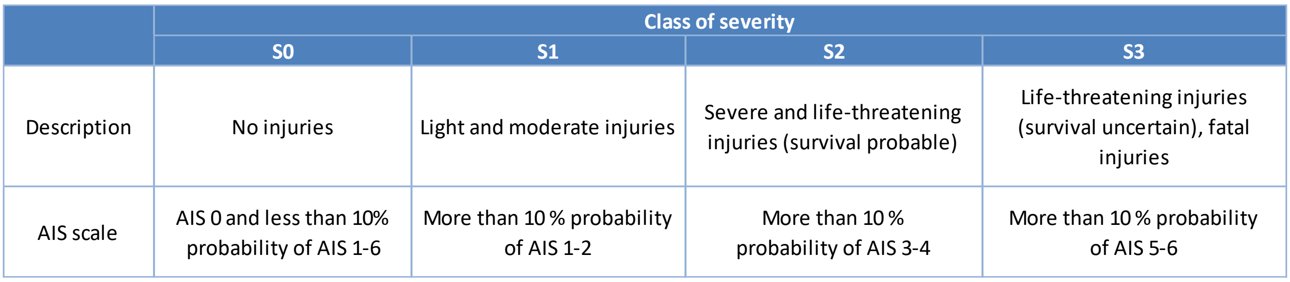
2.1.2 Hazard classification

The hazards are classified with respect to severity (S), probability of exposure (E) and controllability (C).

If classification of a give hazard is difficult to make, then it is classified conservatively so that higher S, E or C classification are chosen.

The severity of potential physical injury or damage to the health of persons, the probability of exposure of each operational situation and the controllability of each hazardous event are estimated on a proper rationale for each hazard.

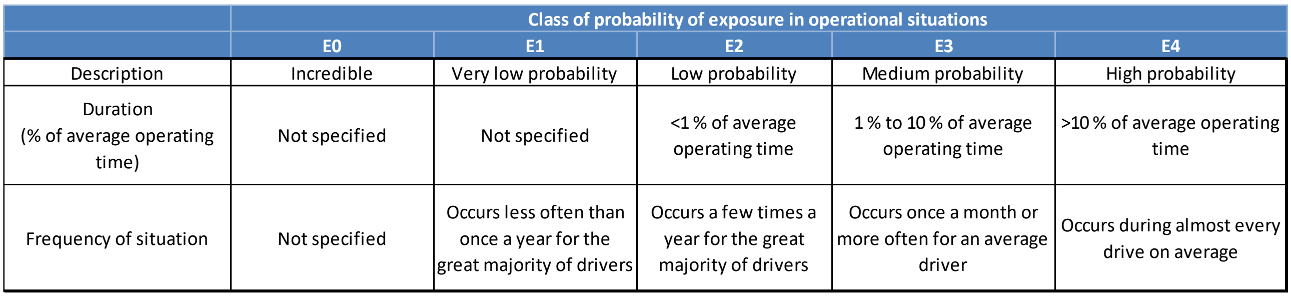
The severity is assigned to one of the severity classes S0, S1, S2 or S3 in accordance with Table 1.



	Class of severity			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
AIS scale	AIS 0 and less than 10% probability of AIS 1-6	More than 10 % probability of AIS 1-2	More than 10 % probability of AIS 3-4	More than 10 % probability of AIS 5-6

Table 1 - Classes of severity

The probability of exposure is assigned to one of the probability classes E0, E1, E2, E3 or E4 in accordance with Table 2:



	Class of probability of exposure in operational situations				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time)	Not specified	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time
Frequency of situation	Not specified	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average

Table 2 – Classes of probability of exposure regarding operational situations

The exposure to a hazard is estimated in two ways, the fist is based on the duration of a situation, temporal overlap, and the second is based on the frequency of occurrence of a situation.

The controllability of each hazardous event is assigned to one of the controllability classes C0, C1, C2 or C3 in accordance with Table 3.

	Class of controllability			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Driving factors and scenarios	Controllable in general	More than 99% of all drivers or other traffic participants are usually able to avoid harm	Between 90% an 99% of all drivers or other traffic participants are usually able to avoid harm	Less than 90% of all drivers or other traffic participants are usually able to avoid harm

Table 3 - Classes of controllability

An ASIL is assigned for each hazardous event based on the classification of severity, probability of exposure and controllability, in accordance with Table 4.

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Table 4 - ASIL determination

2.1.3 ASIL determination

Top-level safety requirements for the Item are called safety goals. For each hazardous event with an ASIL associated a safety goal is determined. If similar safety goals are specified, then these can be combined into one safety goal and the highest ASIL is assigned to it.

Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives.

2.1.4 HARA methodology

This section illustrates and discusses the approach for analysing possible hazards caused by malfunctioning behaviour of the Item, including interaction of their systems, Figure 1.

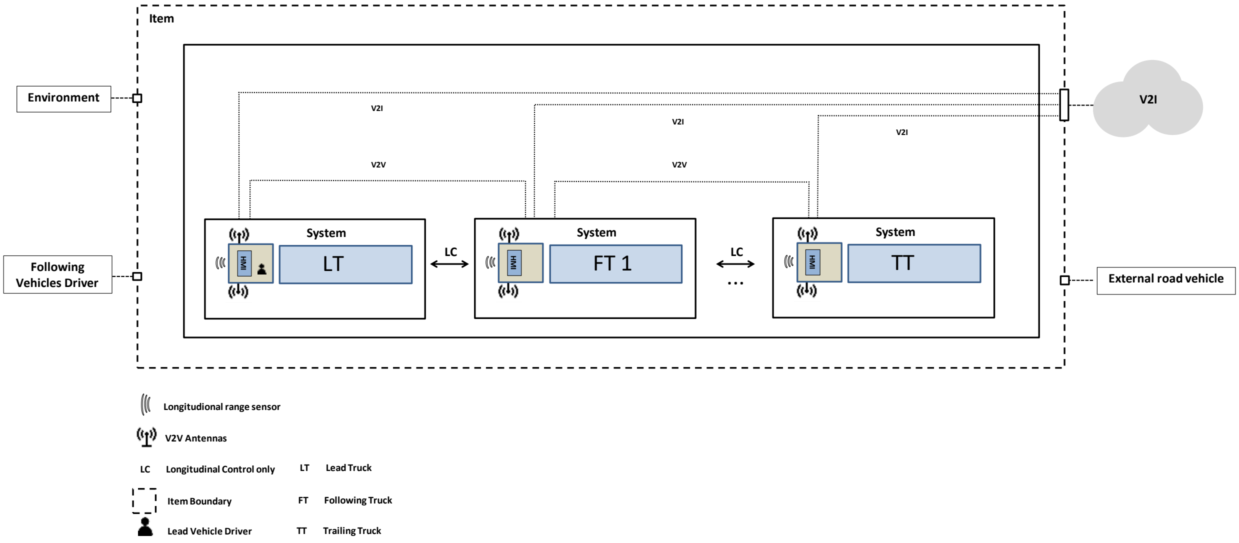


Figure 2 - Item definition

2.1.5 HAZOP

The hazards will be determined systematically based on the possible malfunctioning behaviour of the item.

The Hazard and Operability analysis (HAZOP) approach is suitable to support hazard identification at the item level. This is an explorative type of analysis where applicable guidewords are applied to each of the functions/sub-functions of an item to postulate malfunctioning behaviours.

The HAZOP method can be applied during the different safety lifecycle phases of safety-related systems. At this phase of the safety lifecycle, the concept phase, the requirements of the Item, including its boundary, interfaces and the assumptions concerning its interaction with its elements are defined but the system architectural design and documentation required to conduct the HAZOP do not exist. Nevertheless, it is necessary to identify major hazards at this stage, to include them into the development process and to facilitate future hazard analysis studies.

2.2 Assumptions

The following assumptions have been made during the current HARA analysis:

A1) The objectives of the hazard analysis and risk assessment are to identify and to categorise the hazardous events caused by malfunctioning behaviour of the item; and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk;

A2) Prerequisites are information which should be available as work products of a previous phase. D2.2 and D2.10 are prerequisites for the HARA;

A3) HARA is performed taken into consideration the following available inputs:

- D2.10_Iterative process documentation and Item Definition_v1
- D2.2 - Use Cases and platooning levels final
- D2.6 functional specification for intelligent infrastructure Final
- D2.4 Functional specification for white-label truck (Operational & Tactical layers)

A4) Notes and examples within the HARA are intended to be used only for guidance in understanding how to make use of the template;

A5) The hazards are identified systematically using HAZOP approach which utilizes the predefined set of guide words;

A6) SAE J2980:2018 is used as guidance for identifying and classifying hazardous events, which are per ISO 26262;

A7) Only hazards associated with malfunctioning behaviour of the item are considered, every other external system is presumed to be functioning correctly;

A8) Potential hazard’s causes related to the item's implementation are outside of the scope of ISO 26262;

A9) The item is evaluated without external measures (ACC, AEB) during the hazard analysis and risk assessment;

A10) The following variances are considered when conducting a hazard analysis and risk assessment, in accordance with the ISO26262: base vehicle type, truck vehicle configuration and truck vehicle operation;

A11) All the platoon trucks are equipped with driver assistance systems such as ACC, AEB. LKA driver assistance system is optional for each standalone truck;

A12) If a hazardous event is assigned severity class S0, or exposure class E0, or controllability class C0, no ASIL assignment is required;

A13) Speed Definitions and range: low speed [≤ 30 km/h], medium speed [30 km/h < v < 80 km/h], high speed [80 km/h ≤ v ≤ maximum permitted speed];

A14) The list of operational situations is not very detailed on purpose. A larger number of different operational situations can lead to a consequential reduction of the respective classes of exposure, and thus to an inappropriate lowering of the ASIL;

A15) If the driver is attentive, then as per the Köller Model a reaction time of 1.55 seconds is considered a reaction delay for the driver;

A16) Every hazards event that can lead to rear-end collision will be considered S3;

A17) Overall reaction time (system + driver) is assumed to be 3s: 0,6s trigger + 0,45 margin + 1,55s Köllner model + 0,4 brake ramp-up

A18) The time gap to the following traffic is assumed to be 1s or greater (Exposure E4). Lower time gap is assumed to be E3;

A19) The time gap to the preceding traffic is assumed to be 1s or greater (Exposure E4). Lower time gap is assumed to be E3;

A20) A malfunctioning behaviour of the braking function coincident with the driving situation platooning with preceding traffic:

- braking up to -2.0m/s^2 is assigned E4, the highest exposure level;
- braking more than -2.0m/s^2 up to -3,5m/s^2 is assigned E3 exposure level;
- braking more than -3.5m/s^2 to -5,0m/s^2 is assigned E2 exposure level;
- braking more than -5.0m/s^2 to -8,0m/s^2 is assigned E1 exposure level;

A21) Since the lead vehicle is controlled manually, acceleration and deceleration malfunctions of the lead vehicle will not be considered for HARA;

A22) All malfunctions will originate in the ego vehicle;

A23) Assumptions on controllability (Assumptions agreed during the Safety workshop 2. For internal use only):

- TTC ≤ 3 s is assigned C3;
- 3 s < TTC ≤ 4 s is assigned C2;
- 4 s < TTC ≤ 5 s is assigned C1;

- TTC > 5 s is assigned C0;

A24) Assumptions on controllability (Used for the HARA). Required deceleration to avoid collision:

- Deceleration less than or equal to 3.5 m/s² (light braking) is assigned C0;
- 3.5 m/s² < deceleration ≤ 5 m/s² (moderate braking) is assigned C1;
- 5 m/s² < deceleration ≤ 8.0 m/s² (full braking) is assigned C2;
- Deceleration greater than 8.0 m/s² (severe braking) is assigned C3.

3. Hazard analysis and risk assessment

The hazard analysis and risk assessment is carried out on Platoon Level A item.

The Item is evaluated without external measures (e.g. ACC, AEB) in accordance with the assumptions.

3.1 Hazard Analysis

The first step of the analysis is the identification of the Malfunction categories, the malfunctions and the platooning states in which the malfunctions will be analysed. The hazard identification at the item level was performed using the HAZOP approach which was supported by brainstorming and analysis performed together with all the partners.

The following malfunction categories were considered for the HARA:

- Communication
- Braking
- Acceleration
- Human Machine Interface

Even though the malfunctions from the communication category can be observed at the acceleration, braking or HMI level, it was decided to analyse them in a separate category because the V2V communication is the main enabler of the platooning function and it is interesting to identify hazards resulting from malfunctions in communication at the concept phase instead of leaving them to the system level.

For each of the malfunction category, the identification of deviations from the design intent is achieved by a questioning process using guidewords tailored according to the scope and context of the analysis, Table 5.

Guide word		Meaning
Loss		Function not provided when intended
Wrong	More than intended	Function provided incorrectly when intended
	Excessive	
	Less than intended	
	Insufficient	
	False	
Unintended		Function provided when not intended
Lack		Failure of the function to update as intended

Table 5 - Guide words and their meanings

The following malfunctions were selected for each category for the HARA analysis after the completion of the HAZOP study:

- Communication:
  - Loss of communication of the braking information to the following vehicle
  - Wrong braking/deceleration information communicated to the following vehicle
  - Wrong brake performance value communicated to the following vehicle
- Braking
  - Unintended braking
  - Lack of braking
  - Insufficient braking
  - Wrong brake performance estimation
- Acceleration
  - Unintended acceleration
  - Excessive acceleration
- Human Machine Interface
  - False inactive status informed to the driver
  - Lack of driver disengage request

The above malfunctions were analysed under the following platooning modes:

- Platoon Engaging
- Platooning (Steady state)
- Platoon Disengaging

During the brainstorming and analysis sessions, the Safety Team had examined each function of the Platooning Level A for deviation from the design intent which can lead to malfunctioning behaviours.

Once identified the functions and their sub-functions, the malfunctioning behaviours of the Platooning Level A that could lead to hazards are postulated using appropriate guidewords, Table 6.

The following table (Table 6) outlines the malfunction categories, the platooning modes and the malfunctions analysed for the HARA:

No.	Category	Function	Malfunction (from Ego vehicle's point of view)
H1	Communication	Platooning	Lack/loss of braking information from the ego vehicle
H2			Wrong braking/deceleration information (less than actual value) sent to the following vehicle: Wrong by 25%, 50% and 75%
H3			Wrong brake performance information (under estimate) sent to the following vehicle: Wrong by 12.5%, 25% and 37.5%
H4			Wrong brake performance estimation (Over estimate): Wrong by 37.5%
H5	Braking	Platooning	Unintended braking of the ego vehicle: Deceleration of -8 m/s2, -5 m/s2, -3.5 m/s2 & -2 m/s2
H6			Wrong brake performance estimation (Over estimate): Wrong by 12.5%, 25% and 37.5%
H7			Wrong brake performance estimation (Under estimate): Wrong by 37.5%
H8			Insufficient braking by the ego vehicle: Insufficient by 25%, 50% and 75%
H9			Lack/loss of braking by the ego vehicle
H10	Acceleration	Engaging	Excessive Acceleration by the ego vehicle
H11		Platooning Disengaging	Unintended acceleration of the ego vehicle
H12	HMI	Platooning	False inactive status information of the platoon
H13			Lack of platoon disengage

Table 6 – Category, functions and malfunctions

3.2 Risk Assessment

In total 60 different cases (combinations of malfunctions and operational situations) were analysed during the risk assessment activity. The following section summarises the results of the risk assessment activity by detailing the cases which resulted in Automotive Safety Integrity Levels (ASILs) above Quality Management (QM).

3.2.1 Malfunction Category: Communication

This section presents the results of the risk assessment carried out on communication related malfunctions.

Loss of braking information transmitted by the ego vehicle

1. Malfunction: Loss/lack of braking information transmitted by the ego vehicle

Ego vehicle does not communicate its braking information to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -2 m/s2
Malfunction:	Loss of braking information transmitted by the ego vehicle
Hazard:	Lack of braking by the following truck
Severity Rating:	S3
Rational Severity:	Impact speed 31.25 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E4
Rational Exposure:	High probability of being in a situation that requires a braking of up to -2 m/s2
Controllability Rating:	C1
Rational Controllability:	TTC 4.4 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 1.4 s to react. A minimum deceleration of around -3.9 m/s2 is required to avoid collision.
ASIL Classification:	B

2. Malfunction: Loss/lack of braking information transmitted by the ego vehicle
Ego vehicle does not communicate its braking information to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -3.5 m/s2
Malfunction:	Loss of braking information transmitted by the ego vehicle
Hazard:	Lack of braking by the following truck

Severity Rating:	S3
Rational Severity:	Impact speed 40.86 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C3
Rational Controllability:	TTC 3.3 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.3 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	C

3. Malfunction: Loss/lack of braking information transmitted by the ego vehicle
Ego vehicle does not communicate its braking information to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -5.0 m/s2
Malfunction:	Loss of braking information transmitted by the ego vehicle
Hazard:	Lack of braking by the following truck
Severity Rating:	S3
Rational Severity:	Impact speed 47.56 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E2
Rational Exposure:	Low probability of braking at decelerations between -3.5 m/s2 to -5 m/s2. Happens less than 1% of the operating time.
Controllability Rating:	C3
Rational Controllability:	TTC 2.7 seconds

	The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	B

4. Malfunction: Loss/lack of braking information transmitted by the ego vehicle
Ego vehicle does not communicate its braking information to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Loss of braking information transmitted by the ego vehicle
Hazard:	Lack of braking by the following truck
Severity Rating:	S3
Rational Severity:	Impact speed 58.79 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.1 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	A

Top level safety requirements:

SG1:

Safety Goal:	Avoid collision due to loss of V2V braking information from the forward vehicle
ASIL Category:	C

Wrong deceleration information transmitted by the ego vehicle

5. Malfunction: Wrong deceleration value transmitted by the ego vehicle

Ego vehicle communicates wrong deceleration information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -3.5 m/s2
Malfunction:	Wrong deceleration information transmitted by the ego vehicle (Less by 50%)
Hazard:	Insufficient deceleration of -1.75 m/s2 by the following truck
Severity Rating:	S3
Rational Severity:	Impact speed 29.23 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C1
Rational Controllability:	TTC 4.5 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 1.5 s to react. A minimum deceleration of around -4.8 m/s2 is required to avoid collision.
ASIL Classification:	A

6. Malfunction: Wrong deceleration value transmitted by the ego vehicle

Ego vehicle communicates wrong deceleration information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -3.5 m/s2
Malfunction:	Wrong deceleration information transmitted by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -2.625 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 35.03 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C3
Rational Controllability:	TTC 3.7 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.7 s to react. A minimum deceleration of around -8.1 m/s2 is required to avoid collision.
ASIL Classification:	C

7. Malfunction: Wrong deceleration value transmitted by the ego vehicle

Ego vehicle communicates wrong deceleration information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h

	Time gap = 0.8 seconds Ego vehicle deceleration = -5.0 m/s2
Malfunction:	Wrong deceleration information transmitted by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -3.75 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 41.98 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E2
Rational Exposure:	Low probability of braking at decelerations between -3.5 m/s2 to -5 m/s2. Happens less than 1% of the operating time
Controllability Rating:	C3
Rational Controllability:	TTC 3.1 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	B

8. Malfunction: Wrong deceleration value transmitted by the ego vehicle

Ego vehicle communicates wrong deceleration information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Wrong deceleration information transmitted by the ego vehicle (Less by 50%)
Hazard:	Insufficient deceleration of -4 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 43.81 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1

Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.9 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	A

9. Malfunction: Wrong deceleration value transmitted by the ego vehicle

Ego vehicle communicates wrong deceleration information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Wrong deceleration information transmitted by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -6 m/s^2 by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 52.02 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.4 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react.

	It is uncontrollable.
ASIL Classification:	A

Top level safety requirements:

SG2:

Safety Goal:	Avoid collision due to the communication of wrong (lower than actual by 50%) deceleration value by the forward vehicle
ASIL Category:	A

SG3:

Safety Goal:	Avoid collision due to the communication of wrong (lower than actual by 75%) deceleration value by the forward vehicle
ASIL Category:	C

Wrong brake performance information transmitted by the ego vehicle

As per the legal requirements it is assumed that all the trucks are at least able to achieve a deceleration of -5 m/s2. Hence, only malfunctions in situations where higher decelerations are required have been analysed.

10. Malfunction: Wrong brake performance information transmitted by the ego vehicle
Ego vehicle communicates wrong brake performance information (less than actual value) to the following truck

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Wrong brake performance information transmitted by the ego vehicle (Under estimate by 37.5%)
Hazard:	Insufficient deceleration of -3 m/s^2 by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 35.24 km/h.

	A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 3.3 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.3 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	A

Top level safety requirements:

SG4:

Safety Goal:	Avoid collision due to the communication of wrong (lower than actual by 37.5%) brake performance value by the forward vehicle
ASIL Category:	A

3.2.2 Malfunction Category: Braking

This section presents the results of the risk assessment carried out on braking related malfunctions.

Unintended braking by the ego vehicle

11. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended full braking of -8 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 1.0 second
Malfunction:	Unintended braking of -8 m/s2 by the ego vehicle

Hazard:	Unintended longitudinal deceleration of -8m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 67.43 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E4
Rational Exposure:	Highway driving situations where the external vehicles following the platoon are driving with a time gap of 1s.
Controllability Rating:	C3
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 2.4 seconds The overall delay in external following vehicle's driver's reaction: 1.55 sec. (1.55 s of reaction time- Köller Model). Driver has around 0.85 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	D

12. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended full braking of -8 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 0.8 seconds
Malfunction:	Unintended braking of -8 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -8m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 58.79 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability of having external vehicles following the platoon with a time gap less than 1 sec on a highway
Controllability Rating:	C3
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle.

	TTC is 2.1 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time- Köller Model). Driver has around 0.55 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	C

13. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended moderate braking of -5 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 1.0 second
Malfunction:	Unintended braking of -5 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -5m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 54.76 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E4
Rational Exposure:	Highway driving situations where the external vehicles following the platoon are driving with a time gap of 1s.
Controllability Rating:	C2
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 3.1 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time- Köller Model). Driver has around 1.55 s to react. A minimum deceleration of -6.5 m/s2 is required to avoid collision.
ASIL Classification:	C

14. Malfunction: Unintended braking by the ego vehicle

Ego vehicle performs unintended moderate braking of -5 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 0.8 seconds
Malfunction:	Unintended braking of -5 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -5m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 47.56 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability of having external vehicles following the platoon with a time gap less than 1 sec on a highway
Controllability Rating:	C2
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 2.7 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time-Köller Model). Driver has around 1.15 s to react. A minimum deceleration of -7.3 m/s2 is required to avoid collision.
ASIL Classification:	B

15. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended light braking of -3.5 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 1.0 second
Malfunction:	Unintended braking of -3.5 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -3.5m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 45.9 km/h.

	A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E4
Rational Exposure:	Highway driving situations where the external vehicles following the platoon are driving with a time gap of 1s.
Controllability Rating:	C1
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 3.7 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time-Köller Model). Driver has around 2.15 s to react. A minimum deceleration of more than -4.2 m/s2 is required to avoid collision. It is not controllable.
ASIL Classification:	B

16. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended light braking of -3.5 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 0.8 seconds
Malfunction:	Unintended braking of -3.5 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -3.5 m/s^2
Severity Rating:	S3
Rational Severity:	Impact speed 40.86 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability of having external vehicles following the platoon with a time gap less than 1 sec on a highway
Controllability Rating:	C1
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 3.3 seconds

	The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time-Köller Model). Driver has around 1.75 s to react. A minimum deceleration of more than -4.5 m/s2 is required to avoid collision. It is not controllable.
ASIL Classification:	A

17. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended light braking of -2.0 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 1.0 second
Malfunction:	Unintended braking of -2.0 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -2.0 m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 34.85 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E4
Rational Exposure:	Highway driving situations where the external vehicles following the platoon are driving with a time gap of 1s.
Controllability Rating:	C1
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 4.9 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time-Köller Model). Driver has around 3.35 s to react. A minimum deceleration of -2.2 m/s2 is required to avoid collision.
ASIL Classification:	B

18. Malfunction: Unintended braking by the ego vehicle
Ego vehicle performs unintended light braking of -2.0 m/s2

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle in the platoon Ego vehicle speed = 90 km/h Following external vehicle speed = 90 km/h External vehicle following the platoon with a time gap of 0.8 seconds
Malfunction:	Unintended braking of -2.0 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal deceleration of -2.0 m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 31.25 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability of having external vehicles following the platoon with a time gap less than 1 sec on a highway
Controllability Rating:	C1
Rational Controllability:	Situation is controllable within the platoon. Controllability analysed for external following vehicle. TTC is 4.4 seconds The overall delay in driver reaction: 1.55 sec. (1.55 s of reaction time-Köller Model). Driver has around 2.85 s to react. A minimum deceleration of -2.3 m/s2 is required to avoid collision.
ASIL Classification:	A

Top level safety requirements:

SG5:

Safety Goal:	Avoid unintended full braking (more than -5.0m/s² up to -8.0m/s²) by the ego vehicle
ASIL Category:	D

SG6:

Safety Goal:	Avoid unintended moderate braking (more than -3.5m/s^2 up to -5.0m/s^2) by the ego vehicle
ASIL Category:	C

SG7:

Safety Goal:	Avoid unintended light to moderate braking (more than -2.0 m/s^2 up to -5.0m/s^2) by the ego vehicle
ASIL Category:	B

Wrong brake performance estimated by the ego vehicle

As per the legal requirements it is assumed that all the trucks are at least able to achieve a deceleration of -5 m/s2. Hence, only malfunctions in situations where higher decelerations are required have been analysed.

19. Malfunction: Wrong brake performance estimated by the ego vehicle
Ego vehicle wrongly (over) estimates its brake performance value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the lead truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds forward vehicle deceleration = -8.0 m/s2
Malfunction:	Wrong brake performance estimated by the ego vehicle (over estimate by 37.5%)
Hazard:	Insufficient deceleration of -3 m/s^2 by the ego truck
Severity Rating:	S3
Rational Severity:	Impact speed 35.24 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2. Occurs a few times a year for the great majority of drivers
Controllability Rating:	C3
Rational Controllability:	TTC 3.3 seconds

	The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.3 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	A

Top level safety requirements:

SG8:

Safety Goal:	Avoid collision due to over estimation (over estimate by 37.5%) of brake performance
ASIL Category:	A

Insufficient braking by the ego vehicle

20. Malfunction: Insufficient braking by the ego vehicle
Ego vehicle brakes at a deceleration lower than the expected value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -3.5 m/s2
Malfunction:	Insufficient deceleration by the ego vehicle (Less by 50%)
Hazard:	Insufficient deceleration of -1.75 m/s^2 by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 29.23 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C1

Rational Controllability:	TTC 4.5 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 1.5 s to react. A minimum deceleration of around -4.8 m/s2 is required to avoid collision.
ASIL Classification:	A

21. Malfunction: Insufficient braking by the ego vehicle
Ego vehicle brakes at a deceleration lower than the expected value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -3.5 m/s2
Malfunction:	Insufficient deceleration by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -2.625 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 35.03 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C3
Rational Controllability:	TTC 3.7 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.7 s to react.

	A minimum deceleration of around -8.1 m/s2 is required to avoid collision.
ASIL Classification:	C

22. Malfunction: Insufficient braking by the ego vehicle
Ego vehicle brakes at a deceleration lower than the expected value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -5.0 m/s2
Malfunction:	Insufficient deceleration by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -3.75 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 41.98 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E2
Rational Exposure:	Low probability of braking at decelerations between -3.5 m/s2 to -5 m/s2. Happens less than 1% of the operating time
Controllability Rating:	C3
Rational Controllability:	TTC 3.1 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	B

23. Malfunction: Insufficient braking by the ego vehicle
Ego vehicle brakes at a deceleration lower than the expected value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h

	Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Insufficient deceleration by the ego vehicle (Less by 50%)
Hazard:	Insufficient deceleration of -4 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 43.81 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.9 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	A

24. Malfunction: Insufficient braking by the ego vehicle
Ego vehicle brakes at a deceleration lower than the expected value

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the trailing truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle deceleration = -8.0 m/s2
Malfunction:	Insufficient deceleration by the ego vehicle (Less by 75%)
Hazard:	Insufficient deceleration of -6 m/s² by the following truck.
Severity Rating:	S3
Rational Severity:	Impact speed 52.02 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.4 seconds

	The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	A

Top level safety requirements:

SG9:

Safety Goal:	Avoid collision due to insufficient (less by 50%) braking by the ego vehicle
ASIL Category:	A

SG10:

Safety Goal:	Avoid collision due to insufficient (less by 75%) braking by the ego vehicle
ASIL Category:	C

Lack of braking by the ego vehicle

25. Malfunction: Lack of braking by the ego vehicle
Ego vehicle does not brake when expected

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Forward vehicle starts decelerating = -2 m/s2
Malfunction:	Lack of braking by the ego vehicle
Hazard:	Lack of deceleration by the ego vehicle
Severity Rating:	S3
Rational Severity:	Impact speed 31.25 km/h. A16 - Every hazard that can lead to collision will be considered S3

Exposure Rating:	E4
Rational Exposure:	High probability of being in a situation that requires a braking of up to -2 m/s2
Controllability Rating:	C1
Rational Controllability:	TTC 4.4 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 1.4 s to react. A minimum deceleration of around -3.9 m/s2 is required to avoid collision.
ASIL Classification:	B

26. Malfunction: Lack of braking by the ego vehicle
Ego vehicle does not brake when expected

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Forward vehicle starts decelerating = -3.5 m/s2
Malfunction:	Lack of braking by the ego vehicle
Hazard:	Lack of deceleration by the ego vehicle
Severity Rating:	S3
Rational Severity:	Impact speed 40.86 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Medium probability: On an average between 1% to 10% of the average operating time is spent braking at more than -2 m/s2 and less than -3.5 m/s2
Controllability Rating:	C3
Rational Controllability:	TTC 3.3 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego

	trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.3 s to react. It is uncontrollable as more than -9 m/s2 is required to avoid collision.
ASIL Classification:	C

27. Malfunction: Lack of braking by the ego vehicle
Ego vehicle does not brake when expected

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Forward vehicle starts decelerating = -5.0 m/s2
Malfunction:	Lack of braking by the ego vehicle
Hazard:	Lack of deceleration by the ego vehicle
Severity Rating:	S3
Rational Severity:	Impact speed 47.56 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E2
Rational Exposure:	Low probability of braking at decelerations between -3.5 m/s2 to -5 m/s2. Happens less than 1% of the operating time.
Controllability Rating:	C3
Rational Controllability:	TTC 2.7 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	B

28. Malfunction: Lack of braking by the ego vehicle
Ego vehicle does not brake when expected

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Forward vehicle starts decelerating = -8.0 m/s2
Malfunction:	Lack of braking by the ego vehicle
Hazard:	Lack of deceleration by the ego vehicle
Severity Rating:	S3
Rational Severity:	Impact speed 58.79 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E1
Rational Exposure:	Very low probability of braking at more than -5 m/s2 and up to -8m/s2.
Controllability Rating:	C3
Rational Controllability:	TTC 2.1 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	A

Top level safety requirements:

SG11:

Safety Goal:	Avoid collision due to lack of braking by the ego vehicle
ASIL Category:	C

3.2.3 Malfunction Category: Acceleration

The below section presents the results of the risk assessment carried out on acceleration related malfunctions.

Unintended acceleration by the ego vehicle

29. Malfunction: Unintended acceleration of the ego vehicle
Unintended acceleration of the ego vehicle while driving downhill at low speed

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 30 km/h Forward vehicle speed = 30 km/h Time gap = 0.8 seconds Small downhill (7% gradient)
Malfunction:	Unintended acceleration of 2 m/s2 by the ego vehicle
Hazard:	Unintended/Excessive acceleration of 2 m/s² by the ego vehicle
Severity Rating:	S3
Rational Severity:	Impact speed 17.57 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	Based on duration and location trucks on a highway can experience small downhill gradients for between 1% to 10% of their operating time.
Controllability Rating:	C3
Rational Controllability:	TTC 2.5 seconds The overall delay in driver reaction: 2.6 sec. (0.4 s for the ego truck to accelerate + 0.45 s malfunction realization margin +1.55 s of reaction time) Driver has no time to react. It is uncontrollable.
ASIL Classification:	C

30. Malfunction: Unintended acceleration of the ego vehicle
Unintended acceleration of the ego vehicle while disengage is request by a decelerating forward vehicle

Platooning Mode	Platoon Disengaging
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 80 km/h Forward vehicle speed = 80 km/h Platoon disengage requested by the forward vehicle Forward vehicle deceleration = -2 m/s2 Time gap = 0.8 seconds

Malfunction:	Unintended acceleration of 0.4 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal acceleration of 0.4 m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 32.33 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E3
Rational Exposure:	A situation where the platoon had to be disengaged while facing a situation of deceleration of -2.0 m/s2 occurs once a month or more often for an average driver.
Controllability Rating:	C2
Rational Controllability:	TTC 3.8 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has around 0.8 s to react. A minimum deceleration of around -6.7 m/s2 is required to avoid collision.
ASIL Classification:	B

31. Malfunction: Unintended acceleration of the ego vehicle
Unintended acceleration of the ego vehicle while disengage is request by a decelerating forward vehicle

Platooning Mode	Platoon Disengaging
Operational Situation	Ego vehicle is any vehicle other than the leading truck Ego vehicle speed = 80 km/h Forward vehicle speed = 80 km/h Platoon disengage requested by the forward vehicle Forward vehicle deceleration = -3.5 m/s2 Time gap = 0.8 seconds
Malfunction:	Unintended acceleration of 0.4 m/s2 by the ego vehicle
Hazard:	Unintended longitudinal acceleration of 0.4 m/s²
Severity Rating:	S3
Rational Severity:	Impact speed 39.89 km/h. A16 - Every hazard that can lead to collision will be considered S3
Exposure Rating:	E2

Rational Exposure:	A situation where the platoon had to be disengaged while facing a situation of deceleration of -3.5 m/s2 occurs few times a year for an average driver.
Controllability Rating:	C3
Rational Controllability:	TTC 2.9 seconds The overall delay in driver reaction: 3 sec. (0.6 seconds to detect forward truck braking (movement & lights) + 0.4 usual margin within which ego trucks deceleration is felt by the driver + malfunction realization margin 0.45 s + 1.55 s of reaction time- Köller Model). Driver has no time to react. It is uncontrollable.
ASIL Classification:	B

Top level safety requirements:

SG12:

Safety Goal:	Avoid collision due to unintended acceleration while platooning on a downhill
ASIL Category:	C

SG13:

Safety Goal:	Avoid acceleration when a platoon disengage request is received
ASIL Category:	B

3.2.4 Malfunction Category: HMI

The below section presents the results of the risk assessment carried out on HMI related malfunctions.

False inactive status information of the platoon by the ego vehicle's HMI

32. Malfunction: False inactive status information of the platoon
The HMI shows the platoon status as inactive to the driver when it is still in active state

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is the lead vehicle Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Lane change required due to road conditions (blocked, construction, etc..) Or Ego vehicle tires to overtake another vehicle assuming platoon is disengaged
Malfunction:	False inactive status by the ego truck HMI
Hazard:	Lack of steering by the following trucks
Severity Rating:	S3
Rational Severity:	Collisions between trucks and other road obstacle like construction zones, etc can be life threatening.
Exposure Rating:	E3
Rational Exposure:	How often does the driver need to perform steering manoeuvre to avoid collision? Exposure for overtaking as per Table B3, part 3
Controllability Rating:	C1
Rational Controllability:	Since changing of lane is usually noticeable by the following trucks and the lane change is done with enough gap to the forward obstacle/vehicle, more than 99% of the average drivers can avoid harm.
ASIL Classification:	A

33. Malfunction: False inactive status information of the platoon
    The HMI shows the platoon status as inactive to the driver when it is still in active state

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is the lead vehicle Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Steering manoeuvre (in the same lane) required to avoid collision with the obstacle on the road shoulder
Malfunction:	False inactive status by the ego truck HMI
Hazard:	Lack of steering by the following trucks
Severity Rating:	S3
Rational Severity:	Collisions with obstacles in the lane can be life threatening.
Exposure Rating:	E2

Rational Exposure:	Exposure for Evasive manoeuvre as per the table B3, part 3
Controllability Rating:	C3
Rational Controllability:	Depends on the view and the following drivers and reaction time. To be confirmed after simulation!! Worst case assumed for the initial analysis
ASIL Classification:	B

Top level safety requirements:

SG14:

Safety Goal:	Avoid false inactive platoon status information to the driver
ASIL Category:	B

Lack of platoon disengaging when requested

34. Malfunction: Lack of Platoon disengage
    The driver sees an obstacle on the lane and request platoon disengage to deal with it safely. But the platoon does not disengage as requested.

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is the lead vehicle Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Steering manoeuvre (in the same lane) required to avoid collision with the obstacle on the road shoulder Lead truck request disengage to increase the time gap and increase following driver's awareness
Malfunction:	Platoon not disengaging when requested
Hazard:	Platoon cannot be disengaged
Severity Rating:	S3
Rational Severity:	Collisions with obstacles in the lane can be life threatening.
Exposure Rating:	E2
Rational Exposure:	Exposure for Evasive manoeuvre as per the table B3, part 3
Controllability Rating:	C3

Rational Controllability:	Depends on the view and the following drivers and reaction time. To be confirmed after simulation!! Worst case assumed for the initial analysis
ASIL Classification:	B

35. Malfunction: Lack of Platoon disengage
    The driver sees an obstacle on the lane and request platoon disengage to deal with it safely. But the platoon does not disengage as requested.

Platooning Mode	Steady state platooning
Operational Situation	Ego vehicle is the lead vehicle Ego vehicle speed = 90 km/h Forward vehicle speed = 90 km/h Time gap = 0.8 seconds Ego vehicle wants to leave the highway and request platoon disengage: - to increase the time gap and increase following driver's awareness - to leave the highway
Malfunction:	Platoon not disengaging when requested
Hazard:	Platoon cannot be disengaged
Severity Rating:	S3
Rational Severity:	Following trucks may get confused and continue following the lead truck. Might have to correct their steering at the last moment to remain on the highway
Exposure Rating:	E4
Rational Exposure:	Requesting disengage to leave the platoon and exit the highway occurs during almost every drive on average.
Controllability Rating:	C2
Rational Controllability:	Depends on the reaction of the lead vehicle. If he decides to leave the platoon anyway, then the following vehicles might follow the lead truck blindly to leave the highway. Or notice the leaving and try to steer into the highway at the last moment, which might lead to collisions with the highway barriers, etc.. Situation should be normally controllable.
ASIL Classification:	C

Top level safety requirements:

SG15:

Safety Goal:	Avoid lack of platoon disengaging when requested by a driver
ASIL Category:	C

The safety goals are summarized in the table below:

Id	Safety Goal	ASIL
SG1	Avoid collision due to loss of V2V braking information from the forward vehicle	C
SG2	Avoid collision due to the communication of wrong (lower than actual by 50%) deceleration value by the forward vehicle	A
SG3	Avoid collision due to the communication of wrong (lower than actual by 75%) deceleration value by the forward vehicle	C
SG4	Avoid collision due to the communication of wrong (lower than actual by 37.5%) brake performance value by the forward vehicle	A
SG5	Avoid unintended full braking (more than -5.0m/s^2 up to -8.0m/s^2) by the ego vehicle	D
SG6	Avoid unintended moderate braking (more than -3.5m/s^2 up to -5.0m/s^2) by the ego vehicle	C
SG7	Avoid unintended light to moderate braking (more than -2.0 m/s^2 up to -5.0m/s^2) by the ego vehicle	B
SG8	Avoid collision due to over estimation (over estimate by 37.5%) of brake performance	A
SG9	Avoid collision due to insufficient (less by 50%) braking by the ego vehicle	A
SG10	Avoid collision due to insufficient (less by 75%) braking by the ego vehicle	C
SG11	Avoid collision due to lack of braking by the ego vehicle	C
SG12	Avoid collision due to unintended acceleration while platooning on a downhill	C
SG13	Avoid acceleration when a platoon disengage request is received	B
SG14	Avoid false inactive platoon status information to the driver	B
SG15	Avoid lack of platoon disengaging when requested by a driver	C

4. Functional Safety Concept

Functional safety is one of the key subjects of the overall safety of a system. ISO 26262 defines functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical and/or electronic systems (Part 1 Clause 3.67 in ISO 26262:2018). ISO26262 includes guidance to mitigate these hazards in order to avoid unreasonable risk by providing appropriate requirements and processes.

As technology evolves, and the systems are becoming more complex, an increasing number of safety-related systems comprised of electrical, electronic and software components, there are increasing risks from systematic failures and random hardware failures, all of them considered within the scope of functional safety.

In accordance with ISO26262-3:2018, Clause 7, the objectives of the functional safety concept are:

a) to specify the functional or degrade functional behaviour of the platooning level A in accordance with its safety goals;
b) to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals;
c) to specify the platooning level A strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures;
d) to allocate the functional safety requirements to the system architectural design, or to external measures; and
e) to verify the functional safety concept and specify the safety validation criteria

Functional safety concept includes safety measures to be implemented in the Platooning level A's architectural elements and specified in the functional safety requirements to comply with the safety goals.

During the safety lifecycle, safety requirements are specified in a hierarchical structure and are allocated or distributed among the elements.
The structure and dependencies of safety requirements are shown in Figure 3:

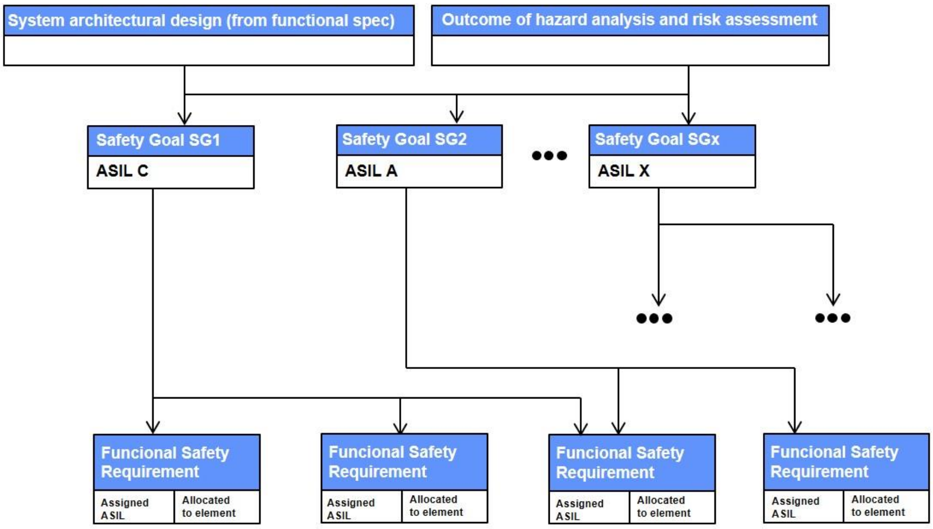

System architectural design (from functional spec)
Outcome of hazard analysis and risk assessment
Safety Goal SG1
ASIL C
Safety Goal SG2
ASIL A
Safety Goal SGx
ASIL X
Funcional Safety Requirement
Assigned ASIL
Allocated to element

Figure 3 – Hierarchical structure of safety requirements

In order to handle immature architectural information in this phase, preliminary architectural assumptions will be made.

From each safety goal, at least one functional safety requirement is derived. The same functional safety requirement can be derived from several safety goals.

Safety requirements inherit the ASIL from the safety requirements from which they are derived, except if ASIL decomposition is applied. ASIL decomposition is a method of ASIL tailoring during the concept and development phases. This allows to implement safety requirements redundantly by independent architectural elements, and to assign a potentially lower ASIL to these decomposed safety requirements. If the architectural elements are not sufficiently independent, then the redundant requirements and the architectural elements inherit the initial ASIL.

Functional safety requirements specify, where applicable, strategies for:

a) fault avoidance
b) fault detection and control of faults or the resulting malfunctioning behaviour;
c) transitioning to a safe state, and, if applicable, from a safe state;
d) fault tolerance:
e) the degradation of the functionality in the presence of a fault
f) driver warnings to reduce the risk exposure time to an acceptable duration
g) driver warning to increase the controllability by the driver
h) fault tolerant time interval
i) arbitration logic

The functional safety requirements consider information, where applicable, including operating modes, fault tolerant time interval, safe states, emergency operation time interval, functional redundancies and the necessary actions of the driver or other persons in order to prevent the violation of a safety goal. The functional safety requirements are then allocated to the preliminary architectural elements of the item or to other items (external measures). In addition, the acceptance criteria for safety validation of the Platooning Level A will be specified based on the functional safety requirements and the safety goals.

At this stage, preliminary hazard analysis and risk assessment have highlighted that the Platooning Level A definition from Deliverable 2.2 is not consistent. In accordance with the functional safety lifecycle, an iterative process is needed starting with an updated definition (based on the steering board decision) that serves as input to the Item definition and HARA safety activities.

In case the steering board selects the support function alternative, the next activity will be a further loop of Item definition and HARA revision and based on that the further development of the functional safety concept.

5. Summary and Conclusion

A preliminary Hazard Analysis and Risk Assessment activity was carried out to understand the safety critical malfunctions arising from the platooning function Level A. Based on their associated risk, ASILs levels have been assigned and top-level safety requirements have been derived for the safety critical hazards in the form of safety goals.

Hazards arising from different malfunctions in the communication, braking, acceleration and HMI categories were considered for the analysis. As a result, a highest ASIL of 'D' has been assigned to the function.

Since the V2V communication is the fundamental enabler of the platooning function, malfunctions communicated by one truck via V2V can result in hazards for the other members of the platoon. Therefore, even though their consequences can be assumed by the malfunctions of braking, acceleration or HMI categories, the V2V communication related malfunctions were also analysed at the concept level in the HARA activity.

A total of 60 cases (combination of operational situation and malfunction) were analysed which resulted in 35 cases having an ASIL above QM (not safety critical) and 25 that are safety critical. For these 25 safety critical cases a total of 15 different top-level safety requirements were identified that must be met with different ASIL levels varying from ASIL A to ASIL D.

As an iterative development process is being followed for the project, the preliminary HARA and the associated top-level safety requirements generated at this stage of the project shall be continuously updated throughout the project.

The outcome of the Hazard analysis and risk assessment shows that the current Platooning Level A definition stated in the D2.2 deliverable is not consistent. In fact, time gaps below 2 seconds in the best case cannot be achieved while longitudinal control remains driver responsibility.

After several discussions, all partners have reached the conclusion that there are two possible project alternatives to proceed:

1. Support function: driver is responsible for longitudinal control so that platooning functionality is a help;

2. Full longitudinal automation: driver is not responsible, the system itself performs all longitudinal operations under certain conditions.

Further concept phase activities will be based on the alternative as chosen by the steering board.

6. Bibliography

SAE J2980 2018.

ISO 26262:2018.

CEI/IEC 61882:2001.

APPENDIX A. GLOSSARY

Definitions

Term	Definition
Convoy	A truck platoon may be defined as trucks that travel together in convoy formation at a fixed gap distance typically less than 1 second apart up to 0.3 seconds. The vehicles closely follow each other using wireless vehicle-to-vehicle (V2V) communication and advanced driver assistance systems
Cut-in	A lane change manoeuvre performed by vehicles from the adjacent lane to the ego vehicle's lane, at a distance close enough (i.e., shorter than desired inter vehicle distance) relative to the ego vehicle.
Cut-out	A lane change manoeuvre performed by vehicles from the ego lane to the adjacent lane.
Cut-through	A lane change manoeuvre performed by vehicles from the adjacent lane (e.g. left lane) to ego vehicle's lane, followed by a lane change manoeuvre to the other adjacent lane (e.g. right lane).
Ego Vehicle	The vehicle from which the perspective is considered.
Emergency brake	Brake action with an acceleration of <-4 m/s2
Event	An event marks the time instant at which a transition of a state occurs, such that before and after an event, the system is in a different mode.
Following truck	Each truck that is following behind a member of the platoon, being every truck except the leading and the trailing truck, when the system is in platoon mode.
Leading truck	The first truck of a truck platoon
Legal Safe Gap	Minimum allowed elapsed time/distance to be maintained by a standalone truck while driving according to Member States regulation (it could be 2 seconds, 50 meters or not present)
Manoeuvre ("activity")	A particular (dynamic) behaviour which a system can perform (from a driver or other road user perspective) and that is different from standing still, is being considered a manoeuvre.
ODD (operational	The ODD should describe the specific conditions under which a given automation function is intended to function. The ODD is the definition of where

Term	Definition
design domain)	(such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an automation function is designed to operate.
Operational layer	The operational layer involves the vehicle actuator control (e.g. accelerating/braking, steering), the execution of the aforementioned manoeuvres, and the control of the individual vehicles in the platoon to automatically perform the platooning task. Here, the main control task is to regulate the inter-vehicle distance or velocity and, depending on the Platooning Level, the lateral position relative to the lane or to the preceding vehicle. Key performance requirements for this layer are vehicle following behaviour and (longitudinal and lateral) string stability of the platoon, where the latter is a necessary requirement to achieve a stable traffic flow and to achieve scalability with respect to platoon length, and the short-range wireless inter-vehicle communication is the key enabling technology.
Platoon	A group of two or more automated cooperative vehicles in line, maintaining a close distance, typically such a distance to reduce fuel consumption by air drag, to increase traffic safety by use of additional ADAS-technology, and to improve traffic throughput because vehicles are driving closer together and take up less space on the road.
Platoon Automation Levels	In analogy with the SAE automation levels subsequent platoon automation levels will incorporate an increasing set of automation functionalities, up to and including full vehicle automation in a multi-brand platoon in real traffic for the highest Platooning Automation Level. The definition of “platooning levels of automation” will comprise elements like e.g. the minimum time gap between the vehicles, whether there is lateral automation available, driving speed range, operational areas like motorways, etc. Three different levels are anticipated; called A, B and C.
Platoon candidate	A truck who intends to engage the platoon either from the front or the back of the platoon.
Platoon cohesion	Platoon cohesion refers to how well the members of the platoon remain within steady state conditions in various scenario conditions (e.g. slopes, speed changes).
Platoon disengaging	The ego-vehicle decides to disengage from the platoon itself or is requested by another member of the platoon to do so. When conditions are met the ego-vehicle starts to increase the gap between the trucks to a safe non-platooning gap. The disengaging is completed when the gap is large enough (e.g. time gap of 1.5 seconds, which is depends on the

Term	Definition
	operational safety based on vehicle dynamics and human reaction times is given). A.k.a. leave platoon
Platoon dissolve	All trucks are disengaging the platoon at the same time. A.k.a. decoupling, a.k.a. disassemble.
Platoon engaging	Using wireless communication (V2V), the Platoon Candidate sends an engaging request. When conditions are met the system starts to decrease the time gap between the trucks to the platooning time gap. A.k.a. join platoon
Platoon formation	Platoon formation is the process before platoon engaging in which it is determined if and in what format (e.g. composition) trucks can/should become part of a new / existing platoon. Platoon formation can be done on the fly, scheduled or a mixture of both. Platoon candidates may receive instructions during platoon formation (e.g. to adapt their velocity, to park at a certain location) to allow the start of the engaging procedure of the platoon.
Platoon split	The platoon is split in 2 new platoons who themselves continue as standalone entities.
Requirements	Description of system properties. Details of how the requirements shall be implemented at system level
Scenario	A scenario is a quantitative description of the ego vehicle, its activities and/or goals, its static environment, and its dynamic environment. From the perspective of the ego vehicle, a scenario contains all relevant events. Scenario is a combination of a manoeuvre (“activity”), ODD and events
Service layer	The service layer represents the platform on which logistical operations and new initiatives can operate.
Specifications	A group of two or more vehicles driving together in the same direction, not necessarily at short inter-vehicle distances and not necessarily using advanced driver assistance systems
Steady state	In systems theory, a system or a process is in a steady state if the variables (called state variables) which define the behaviour of the system or the process are unchanging in time. In the context of platooning this means that the relative velocity and gap between trucks is unchanging within tolerances from the system parameters.
Strategic layer	The strategic layer is responsible for the high-level decision-making regarding the scheduling of platoons based on vehicle compatibility and Platooning Level,

Term	Definition
	optimisation with respect to fuel consumption, travel times, destination, and impact on highway traffic flow and infrastructure, employing cooperative ITS cloud-based solutions. In addition, the routing of vehicles to allow for platoon forming is included in this layer. The strategic layer is implemented in a centralised fashion in so-called traffic control centres. Long-range wireless communication by existing cellular technology is used between a traffic control centre and vehicles/platoons and their drivers.
Tactical layer	The tactical layer coordinates the actual platoon forming (both from the tail of the platoon and through merging in the platoon) and platoon dissolution. In addition, this layer ensures platoon cohesion on hilly roads, and sets the desired platoon velocity, inter-vehicle distances (e.g. to prevent damaging bridges) and lateral offsets to mitigate road wear. This is implemented through the execution of an interaction protocol using the short-range wireless inter-vehicle communication (i.e. V2X). In fact, the interaction protocol is implemented by message sequences, initiating the manoeuvres that are necessary to form a platoon, to merge into it, or to dissolve it, also taking into account scheduling requirements due to vehicle compatibility.
Target Time Gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds, agreed by all the Platoon members; it represents the minimum distance in seconds allowed inside the Platoon.
Time gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds.
Trailing truck	The last truck of a truck platoon
Truck Platoon	Description of system properties. Details of how the requirements shall be implemented at system level
Use case	Use-cases describe how a system shall respond under various conditions to interactions from the user of the system or surroundings, e.g. other traffic participants or road conditions. The user is called actor on the system, and is often but not always a human being. In addition, the use-case describes the response of the system towards other traffic participants or environmental conditions. The use-cases are described as a sequence of actions, and the system shall behave according to the specified use-cases. The use-case often represents a desired behaviour or outcome. In the ensemble context a use case is an extension of scenario which add more information regarding specific internal system interactions, specific interactions with the actors (e.g. driver, I2V) and will add different flows (normal & alternative e.g. successful and failed in relation to activation of the system / system elements).

Acronyms and abbreviations

Acronym / Abbreviation	Meaning
ACC	Adaptive Cruise Control
ADAS	Advanced driver assistance system
AEB	Autonomous Emergency Braking (System, AEBS)
ASIL	Automotive Safety Integrity Level
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
C-ACC	Cooperative Adaptive Cruise Control
C-ITS	Cooperative ITS
CA	Cooperative Awareness
CAD	Connected Automated Driving
CAM	Cooperative Awareness Message
CCH	Control Channel
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DITL	Driver-In-the-Loop
DOOTL	Driver-Out-Of-the Loop
DSRC	Dedicated Short-Range Communications
ETSI	European Telecommunications Standards Institute
EU	European Union
FCW	Forward Collision Warning
FLC	Forward Looking Camera
FSC	Functional Safety Concept
GN	GeoNetworking
GNSS	Global Navigation Satellite System
GPS	Global Positioning System

Acronym / Abbreviation	Meaning
GUI	Graphical User Interface
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Analysis
HIL	Hardware-in-the-Loop
HMI	Human Machine Interface
HW	Hardware
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITL	In-The-Loop
ITS	Intelligent Transport System
IVI	Infrastructure to Vehicle Information message
LDWS	Lane Departure Warning System
LKA	Lane Keeping Assist
LCA	Lane Centring Assist
LRR	Long Range Radar
LSG	Legal Safe Gap
MAP	MapData message
MIO	Most Important Object
MRR	Mid Range Radar
OS	Operating system
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
OOTL	Out-Of The-Loop
PAEB	Platooning Autonomous Emergency Braking
PL-A	Platooning Level -A
PMC	Platooning Mode Control

Acronym / Abbreviation	Meaning
QM	Quality Management
RSU	Road Side Unit
SA	Situation Awareness
SAE	SAE International, formerly the Society of Automotive Engineers
SCH	Service Channel
SDO	Standard Developing Organisations
SIL	Software-in-the-Loop
SPAT	Signal Phase and Timing message
SRR	Short Range Radar
SW	Software
TC	Technical Committee
TOR	Take-Over Request
TOT	Take-Over Time
TTG	Target Time Gap
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WP	Work Package