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.	D2.12	
Deliverable Title	Preliminary Safety Case	
Dissemination level	Confidential	
Written By	Yinghao Shi, IDIADA	14-06-2021
	Prashanth Dhurjati, IDIADA	10-12-2021
Checked by	Edoardo Mascalchi, CLEPA	28-01-2022
Approved by	Dehlia Willemsen, TNO	15-02-2022

Status	Final, submitted, UNDER APPROVAL BY EC	21-02-2022

Please refer to this document as:

Yinghao Shi et al., (2022) Preliminary Safety Case, D2.12 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	14/06/2021	Yinghao Shi (IDIADA)	Initial Draft	Prepared
0.2	21/06/2021	Prashanth Dhurjati (IDIADA)	Updated based on internal review	Final
0.3	10/12/2021	Prashanth Dhurjati (IDIADA)	Updates from WP leader review	For approval by WP2 partners
1.0	28/01/2022	Edoardo Mascalchi (CLEPA)	Reviewed by WP Leader	For approval by coordinator
1.1	18/02/2021	CLEPA	Feedback from Coordinator implemented	Final

FIGURES

TABLES

EXECUTIVE SUMMARY

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 traffic safety, fuel economy and throughput. This has been 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 were:

- Year 1: setting the specifications and developing a reference design.
- Year 2 and 3: implementing this reference design on the OEM own trucks, as well as performing impact assessments with several criteria.
- Year 4: focus on testing the multi-brand platoons on test tracks and public road.

The technical results were evaluated against the initial requirements, after which these were updated. 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.

Platooning levels

Two levels of platooning have been defined:

- **Platooning Support Function**: the driver is responsible for the driving task. Hence (s)he is also responsible to choose a safe following distance and monitor the system e.g. whether the right platooning partner is being followed (though supported by the system as much as possible). To give the driver sufficient time to react, minimum time gaps around 1.5 s have to be respected. The Platooning support function is a longitudinal control function, but lateral driver assistance systems, such as e.g. lane keeping, might be optionally available as well.

- **Platooning Autonomous Function**: The lead truck has a driver responsible for the driving task, but the following trucks are fully automated, i.e. the system performs the complete driving task within the specified (limited) operational design domain. Taking the driver(s) out-of-the-loop offers the possibility to reduce time gaps to a minimum of 0.3 s.

In contrast to the Platooning Support Function, implementation of the Platooning Autonomous Function is not part of the ENSEMBLE project and the specification of the Platooning Autonomous Function and its use cases is solely done on theoretical considerations to sketch a future vision of platooning. The latter is also due to the low technology readiness level of certain required autonomous driving subfunctions at the time of writing.

Abstract of this Deliverable

This deliverable consists of a safety case for the demo version of the Platooning Support Function (PSF). The results provided in this document were generated and shared with all the partners prior to the testing and the demo activities so that the required safety measures can be implemented on time. This document provides evidence to show that the testing and the demo activities were carried out safely.

1. INTRODUCTION

1.1. Background

The ENSEMBLE Platooning Support Function was developed to implement the requirements and specifications defined in the deliverable D2.5 (Mascalchi E., 2022). The Platooning Support Function and its use cases are defined in D2.3 (Willemsen, 2022). Concept phase functional safety activities were carried out before the system development started, to define the following work products:

- Item definition
- Hazard Analysis and Risk Assessment
- Functional Safety Concept

The above work products were defined as per ISO 26262:2018 (ISO26262, 2018) and ENSEMBLE project management requirements. The followings Functional safety deliverables were defined for the ENSEMBLE project:

- D 2.15 - Final version of Iterative Process and Item Definition (P. Dhurjati, 2022)
- D 2.14 - Final version Hazard Analysis and Risk Assessment and Functional Safety Concept (A. Pezzano, 2022)
- D 2.12 – Preliminary Safety Case (This document itself)

The purpose of the current deliverable is to develop a safety case for the demo version of the Platooning Support Function to provide arguments and evidence for the achievement of functional safety as per ISO 26262:2018 (ISO26262, 2018) based on Item Definition, HARA and Functional Safety Concept. Since external measures (elements outside the item boundary diagram) were used in the functional safety concept to assure functional safety, no further safety work products were generated after the concept phase.

This deliverable aims to argue that the risks/hazards which may arise due to malfunctioning behaviour of the support function during the testing and the demo activities are appropriately identified and mitigated. As the ENSEMBLE project is for demonstration only and is not intended for production, a complete satisfaction of functional safety standard ISO26262:2018 (ISO26262, 2018) should not expected (e.g. confirmation reviews by independent partners, etc..).

1.2. Structure of the report

This deliverable consists of 2 main sections:

- Functional Safety Activities: Evidence and rationale
- Summary and conclusions

2. FUNCTIONAL SAFETY ACTIVITIES: EVIDENCE AND RATIONALE

2.1. Overview

The functional safety objective of the demonstration function 'ENSEMBLE Platooning Support Function' is based on the following concept phase work products:

- Item Definition
- HARA
- Functional Safety Concept

The platooning support function is for demonstration only, so there is no mandatory requirement to assign ASIL to the systems involved and no guarantee that the SW/HW are supporting any assigned level of safety integrity. For this reason, as stated before only partial compliance of ISO26262:2018 (ISO26262, 2018) is possible at this stage and the identified functional safety hazards are only to be prevented or mitigated through external measures without depending on the prototype HW/SW implementations.

2.2. Item Definition

2.2.1. Objective

The Item Definition for Platooning Support Function is conducted in accordance with ISO26262: 2018 (ISO26262, 2018), the objectives of item definition are

a) To define and describe the item, its functionality, dependencies on, and interaction with, the driver, the environment, and other items at the vehicle level; and

b) To support an adequate understanding of the item so that the activities in subsequent phases can be performed

The item definition for ENSEMBLE Platooning Support Function describes the context in which the support function is implemented. The platooning trucks for this demo project are to be tested in dedicated proving grounds (IDIADA, Santa Oliva, Spain) followed by testing and demonstration on a public highway (around Barcelona, Spain).

Truck platooning is the linking of two or more trucks in convoy, using connectivity technology and automated driving support systems (ACEA, 2017). Platooning allows to drive trucks in organized convoys communicating with each other via vehicle-to-vehicle communication (V2V). The platooning trucks consist of a leading truck, following trucks and the trailing truck. The platoon participants communicate to the followers their respective driving dynamic values. Consequently, the followers can react synchronously to longitudinal vehicle motion control actions of the forward trucks. This allows driving at closer distances, which opens the possibility to potentially reduce fuel consumption and CO_2 output by air drag benefits and increase the road's traffic intensity in a safe way (to be investigated in the ENSEMBLE WP4).

The ENSEMBLE Platooning Support Function is described in:

- D2.3 – Platooning use cases, scenario definition and Platooning Levels (Willemsen, 2022)
- D2.5 – Final Version Functional specification for white-label truck (Mascalchi E., 2022)
- D2.8 – Platooning protocol definition and communication strategy (B. Atanassow, 2022a)
- D2.9 – Security framework of platooning (B. Atanassow, 2022b)

These deliverables have been used by the partners to implement the function in the respective trucks.

2.2.2. The Item Boundary

The boundary diagram illustrates the item, its elements, and relationships to external elements:

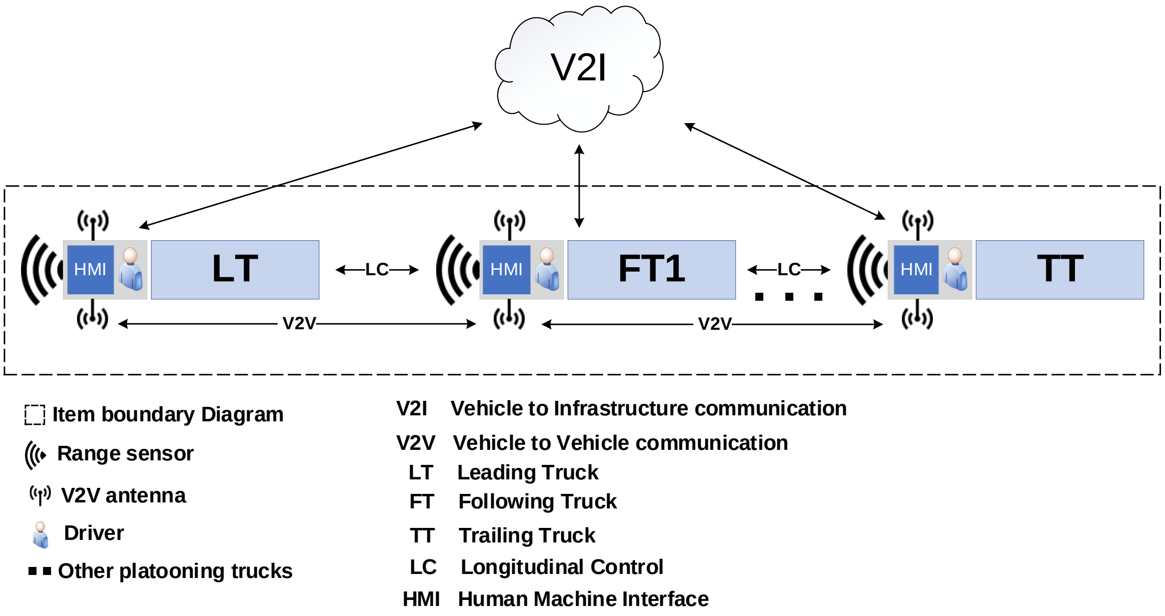

Figure 1 Item boundary diagram – Support function

2.2.3. The Primary Function

The high-level requirements of the ENSEMBLE Platooning Support Function are listed below:

Table 1 Sub Functions for ENSEMBLE Support Function

REQ ID	Sub-Function	Requirement
HLR_PSF_01	V2V Communication	While platooning, each truck shall communicate its dynamic parameters to the following trucks.
HLR_PSF_02	Braking	The following trucks shall brake autonomously with a deceleration of up to 3.5 m/s² to maintain a safe distance to the forward truck.
HLR_PSF_03	Acceleration	The following trucks shall accelerate autonomously to maintain the set time gap to the forward truck.
HLR_PSF_04	Driver Information	The drivers shall be continuously informed of the status of the platooning function.

2.2.4. Assumptions

The following assumptions on the support function outline the various aspects including operational situations and interactions with external environment under which the platooning trucks are to be operated. The following assumptions made during the concept phase have been reviewed and agreed amongst the project stakeholders.

- Drivers are mandatory in all the trucks.
- The maximum number of trucks in a platoon is limited to 7. Actual number on the roads may be lower due to authority or road restrictions.
- Driver of any vehicle can disengage from the platoon at any moment.
- Engagement will only occur while driving on the highways.
- Once established, the platoon is expected to keep cohesion during “stop & go” situations, e.g. in traffic jams.
- Administration and road operators may impose operative platoon restrictions. E.g. forbid platoon in some tunnels, increase time gap on bridges, etc.
- The vehicles shall be able to carry loads as per the legal weight limits of member countries.
- Under any adverse weather condition, drivers can adjust the time gap or disable the platooning function under their own criteria (driver education or incentives is out of the scope of the ENSEMBLE).
- Platoon is expected to be operative in both downhill and uphill. Time gap, speed, and other parameters are expected to be dynamically adapted to ensure platoon cohesion and safety.

- Maintaining the platooning function inside tunnels is optional. If the platooning function cannot be maintained, the longitudinal control will be handed back to the driver with appropriate warning.
- Platoon communication will be switched to lower power when passing toll gates due to ETSI TS 102 792 requirements (V1.2.1, 2015). Deactivation is responsibility of the driver.
- The project shall aim to maintain a minimum time gap of 1.4 seconds for the platooning support function.

2.3. HARA

2.3.1. Objectives

The HARA analysis for Platooning Support Function is conducted based on the well-defined item definition. According to ISO26262: 2018 (ISO26262, 2018), the objectives of HARA are:

a) to identify and to classify the hazardous events caused by malfunctioning behaviours of the item; and

b) to formulate the safety goals with their corresponding ASILs related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

2.3.2. Hazards

The hazards resulting from malfunctioning behaviour of the item are listed below:

Table 2 Functional Hazards with Associated Hazardous Events

Sub-Function	Hazard ID	Relevant Hazards	Hazardous Event ID
Communication	Haz_01:	Loss of deceleration by the following truck	HE_ID_1; HE_ID_2; HE_ID_3; HE_ID_4;
	Haz_02:	Insufficient deceleration by the following truck	HE_ID_5; HE_ID_6; HE_ID_7; HE_ID_8; HE_ID_9; HE_ID_10; HE_ID_11; HE_ID_12; HE_ID_13; HE_ID_14; HE_ID_15; HE_ID_16
Braking	Haz_03:	Unintended deceleration by the following truck	HE_ID_17; HE_ID_18; HE_ID_19; HE_ID_20;
	Haz_02:	Insufficient deceleration by the following truck	HE_ID_21; HE_ID_22; HE_ID_23; HE_ID_24; HE_ID_25; HE_ID_26; HE_ID_27; HE_ID_28; HE_ID_29;
	Haz_01:	Loss of deceleration by the following truck	HE_ID_30; HE_ID_31; HE_ID_32; HE_ID_33;
Acceleration	Haz_04:	Unintended acceleration by the following truck	HE_ID_34; HE_ID_35; HE_ID_36; HE_ID_37; HE_ID_38; HE_ID_39; HE_ID_40; HE_ID_41;
Driver Information	Haz_05:	Lack of steering by the following truck drivers	HE_ID_42; HE_ID_43;

2.3.3. Rationale for Hazardous Events Classification

Haz_01: Loss of deceleration by the following truck

Rationale: Hazardous events related to this hazard are caused by loss of braking information from any forward truck leading to lack of braking by the following truck. No ASIL has been assigned to these hazardous events because they get S0 for severity (they do not cause collisions). This is due to the presence of production approved autonomous emergency braking (AEB) systems in all the trucks. Since the AEB target is a forward truck of considerable size and the tests are being carried out within the nominal ODD conditions for the AEB to work, the chances of false negative are almost negligible. Moreover, since trained test drivers are being used for the testing activities and the demo, lack of braking is easily controllable (C0) due to their experience and quick reaction times.

Haz_02: Insufficient deceleration by the following truck

Rationale: Hazardous events related to this hazard are caused when any of the forward truck communicates in acceleration/deceleration information incorrectly leading to insufficient autonomous braking by the following truck. The analysis was conducted considering braking situations of decelerations between 2m/s² to 8m/s² assuming an insufficient deceleration of 25%, 50% and 75% by the following truck. Similar to the previous case, no ASIL has been assigned to these hazardous events because they get S0 for severity (they do not cause collisions). This is due to the presence of production approved autonomous emergency braking (AEB) systems in all the trucks. Since the AEB target is a forward truck of considerable size and the tests are being carried out within the nominal ODD conditions for the AEB to work, the chances of false negative are almost negligible. Moreover, since test drivers are being used for the testing activities and the demo, lack of braking is easily controllable (C0) due to their experience and quick reaction times.

Haz_03: Unintended deceleration by the following truck

Rationale: Unintended longitudinal deceleration is controllable within the platoon as all the trucks receive the current acceleration information via V2V communication and react autonomously with braking limited to - 3.5m/s². But this hazard can cause collisions between external vehicles following the platoon and the trailing truck of the platoon. Unintended deceleration of both 2m/s^2 and 3.5m/s^2 with a time gap of 1s and 0.8s (closer than usual following traffic) were analysed. Any deceleration above 3.5m/s² was not considered for analysis because the platooning function is implemented on the existing ACC systems and decelerations above 3.5 m/s² are not allowed by the existing systems. since the drivers in the following external vehicles cannot be assumed to be expert drivers capable of reacting quickly to any braking situation under low time gaps, an **ASIL B** was assigned to the hazardous events resulting from this hazard.

Haz_04: Unintended acceleration by the following truck

Rationale: The relevant hazardous events due to unintended acceleration of following truck were determined in different scenarios under different operating mode (Engaging, Platooning and Disengaging) with wide range of truck speed. No ASIL has been assigned to these hazardous events because they get S0 for severity (they do not cause collisions). This is due to the presence of production approved autonomous emergency braking (AEB) systems in all the trucks. Since the AEB target is a forward truck of considerable size and the tests are being carried out within the nominal ODD conditions for the AEB to work, the chances of false negative are almost negligible. Moreover, since test drivers are being used for the testing activities and the demo, unintended acceleration is easily controllable (C0) due to their experience and quick reaction times.

Haz_05: Lack of steering by the following truck drivers (Lead truck driver steers assuming platoon is inactive)

Rationale: The relevant hazardous events are caused by incorrect driver information in the lead truck (HMI indicates platoon is inactive when it is active). This would change the lead truck drivers' behaviour, as he/she would only worry about his/her own truck (and not lead the entire platoon). If a sudden steering intervention is required to avoid collision, information is transmitted via V2V communication, but no alert is given to the following drivers of the hazardous situation. The lead truck steers away to avoid obstacle, while the following truck drivers are not aware of the hazard until the last moment. No ASIL has been assigned to these hazardous events because this hazard is easily controllable by the test drivers who are trained and certified to test prototype vehicles and are fully aware of the monitoring requirements, therefore C0 is assigned to the controllability rating.

2.3.4. Hazardous Event Classification

Severity, Exposure and Controllability rating were discussed, reviewed and agreed upon as followings:

Severity Rationale:

Assumptions on Severity:

As a conservative value, all hazardous events that lead to a collision were considered S3.

Exposure Rationale:

The determination of exposure is based on ISO26262: 2018 part 3 and expert judgement of project safety team (ISO26262, 2018).

Controllability Rationale:

The below assumptions were made based on the various discussions within the safety group that took place during the safety workshops held for the project.

- ***Expert Driver in the Platoon:***

Assumptions on controllability are based on the deceleration required to avoid collision after considering the driver reaction time:

- Deceleration less than 8.0 m/s² [full braking] after subtracting 1.8 sec (see assumption A5 in section 3.3.5) reaction time: C0- Controllable in general.
- Deceleration greater than 8.0 m/s² [severe braking]: C3 - Uncontrollable.

Therefore, it is assumed that, if there is enough time to react, a test driver will always avoid a collision even in situations that require full braking.

- ***Normal Driver external to the Platoon:***

- Light Braking (e.g. high performant truck 0.0 to 3.5 m/s²) is assigned C0 controllability rating
- Intermediate Braking (e.g. high performant truck 3.6 to 5 m/s²) is assigned C1 controllability rating
- Heavy Braking (e.g. high performant truck 5.1 to 8 m/s²) is assigned C2 controllability rating
- Full Braking (e.g. high performant truck > 8 m/s²) is assigned C3 controllability rating

2.3.5. Safety Goal

The safety goal is derived as result of classified hazardous event HE_ID_17 and HE_ID_18 rated with ASIL B and ASIL A respectively.

Table 3 Safety Goal with Associated Hazardous Events

SG ID	SG Description	ASIL	Safe State	Hazardous Events ID
SG_01	Rear end collisions due to unintended braking shall be prevented	B	Not applicable	HE_ID_17 HE_ID_18

No Fault Tolerant Time Interval (FTTI) or safe state are necessary as the risk is prevented/avoid by external measures and no safety mechanism is implemented within the system.

2.3.6. Assumptions

The following table outlines the assumptions used in HARA for assessing the hazardous events. These assumptions are contributing to the justification of appropriate safety integrity level of hazardous event. In the HARA, each hazardous event is assigned relevant assumptions IDs for traceability. These assumptions are to be validated on the integrated item as per ISO26262:2018 Part 4 (ISO26262, 2018).

Table 4 HARA Assumptions

Assumption ID	Assumption description
A1	The demo will be carried out on public roads but in a controlled environment (e.g. no steep gradients, extreme weather conditions, etc…)
A2	The drivers used for the demo will be trained experts with lower reaction times than an average driver.
A3	The demo will only continue for few hours during which the test drivers are able to remain fully alert and react quickly against unintended behaviour of the function.
A4	As the test drivers are assumed to be attentive, once a fault is detected, a reaction time of only 0.95 seconds (as per the Köller Model) is considered achievable by the driver.
A5	Overall reaction time of the test driver considered for the HARA is 1.8 s (0.4 seconds of brake ramp-up of the forward vehicle, 0.45 seconds of driver realisation (of the malfunction) time and 0.95 seconds of driver reaction time).
A6	Only hazards associated with malfunctioning behaviour of the item are considered, every other external system (e.g. powertrain, ESC…) is assumed to be functioning correctly.
A7	The item is evaluated without internal safety mechanisms during the hazard analysis and risk assessment (e.g. for HARA it is assumed that the platooning function is only using the V2V communication and no camera or radar is used as backup, they can be later introduced as safety mechanisms).
A8	As a conservative value, all hazardous events that lead to a collision will be considered S3.
A9	The time gap of 1s or greater to the following traffic (behind the platoon) is assumed to have an Exposure E4.
A10	The time gap of 1s or lower to the following traffic (behind the platoon) is assumed to have an Exposure E3.

Assumption ID	Assumption description
A11	The following exposure ratings are considered for braking situations in normal driving conditions on a highway: - braking up to -2.0m/s² is assigned E4, the highest exposure level; - braking from -2.1m/s² to -3,5m/s² is assigned E3 exposure level; - braking from -3.6m/s² to -5,0m/s² is assigned E2 exposure level; - braking from -5.1m/s² to -8,0m/s² is assigned E1 exposure level;
A12	Since the lead vehicle is controlled manually, acceleration and deceleration malfunctions of the lead vehicle will not be considered for HARA.
A13	Assumptions on controllability (used for test drivers) based on the required deceleration to avoid collision (deceleration required to avoid collision the time left after subtracting 1.8 seconds from the time to collision): - Deceleration less than 8.0 m/s² [full braking] after remove 1.8sec reaction time - C0- Controllable in General; - Deceleration greater than 8.0 m/s² [severe braking] - C3 - Uncontrollable;
A14	The overall reaction time used for external vehicles outside the platoon is: 1.55 sec. (Köller Model for average attentive driver).
A15	**New Definition of the platooning function:** - The function is only support – Longitudinal control is not fully automated. Very similar to C-ACC. - A minimum time gap of 1.4 seconds shall be maintained at all time. The driver still has the option of increasing the time gap if he/she desires but cannot decrease it below 1.4 s. - A maximum deceleration of only -3.5 m/s^2 will be provided by the function. If more is required, then the driver will have to do it on his own or depend on other external functions like Autonomous Emergency Braking. - If more deceleration than -3.5 m/s^2 is required to avoid collision, then the function will provide an HMI warning for the driver to react. - All trucks can brake till standstill (as long as it is within -3.5 m/s^2). Accelerating from stand still is an option, i.e. OEM specific.
A16	It is assumed that all the trucks will meet a minimum brake performance of -5 m/s² in all driving conditions.
A17	Production approved AEB systems will be active in all the trucks. Due to the position and the clear visibility of the forward trucks, the AEB systems in the following trucks will always intervene to prevent collision in case of loss of braking by the platooning function.

Assumption ID	Assumption description

A18	Assumptions on controllability of external vehicles (internal use only):
	Minimum required deceleration to avoid collision:
	Deceleration up to 3.5 m/s^2 [light braking] - C0- Controllable in General;
	Deceleration greater than 3.5 m/s^2 up to -5.0 m/s^2 [moderate braking] - C1 - More than 99% can control;
	Deceleration greater than 5.0 m/s^2 up to 8.0 m/s^2 [full braking] - C2 - Between 90% - 99% can control;
	Deceleration greater than 8.0 m/s^2 [severe braking] - C3 - Uncontrollable;

A19	It is assumed that the demo system will be designed such that even if the platooning function requests to brake with a deceleration of more than -3.5 m/s^2, it will not be delivered by the existing ACC or the Braking system. So, no malfunction of the platooning function can result in a deceleration of more than -3.5 m/s^2.

2.4. Functional Safety Concept

2.4.1. Objectives

In accordance with ISO26262:2018 Part 3 (ISO26262, 2018), The objectives of Functional Safety Concept are

a) To specify the functional or degraded functional behaviour of the item 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 item level 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 measure

d) To allocate the functional safety requirements to the system architectural design, or to external measure and

e) To verify the functional safety concept and specify the safety validation criteria

2.4.2. Functional Safety Requirements

The following two functional safety requirements were defined for the demo activities. These take the form of external measures; safety measures that are separate and distinct from the item under development.

FSR ID	Requirements	ASIL	Derived from	Comments
FSR_01	The trailing truck in the platoon shall display a warning sign (at the back) requesting the following vehicles to maintain a safe distance to the convoy.	N/A	SG_01	External Measures
FSR_02	The trailing truck shall be followed by a test vehicle to deter other vehicles from following the platoon closely.	N/A	SG_01	External Measures

Table 5 Functional Safety Requirement

For the FSR_01, any sticker with the purpose of warning the traffic behind to pay attention is enough to carry out the test safely.

The functional safety requirements derived from SG_01 are defined to be external measures due to the fact that systems implementing the demo platooning support function are not developed as per ISO 26262. Therefore, external measures are defined to prevent the hazardous event from occurring in first place, consequently reducing the effect of unintended braking to an acceptable level of safety.

Other safety measures include having dedicated lane reserved for the platoon while on test tracks to avoid risk of collision with other test vehicles. The test activities are also subject to safety policies of the IDIADA proving ground minimising the risk even further.

3. SUMMARY AND CONCLUSION

Since the ENSEMBLE Platooning Support Function is for demonstration purposes only, prototype hardware and software components were used for the development. Therefore, no safety requirements were assigned to the system because the development cannot be carried out with the safety integrity level mandated by the ISO 26262 standard (ISO26262, 2018). For this reason, only external measures (measures that are separate and distinct from the item under development) were used to prevent hazardous events from occurring or to mitigate the consequence of hazardous events that occur during the testing activities carried out at the proving grounds and the public roads.

As explained in the subsequent section of this document, the presence of expert test drivers in all the trucks and the requirement to always maintain a minimum time gap of 1.4s within the platoon has rendered most of the hazardous event occurring due to E/E malfunctions controllable in general. Only the hazardous events related to unintended braking were assigned ASILs (highest ASIL B) because even if they are controllable within the platoon, they can be hazardous to the trailing traffic (i.e. external vehicles following the platoon) or cut-in vehicles. To avoid accidents due to this hazard, dedicated lane was used for the platoon while testing in the proving grounds and test vehicle was trailing the platoon while driving on public roads. In addition to that, each truck had warning stickers at the back to discourage cut-ins to avoid the unlikely event of having an unintended deceleration malfunction exactly at the time of a cut-in.

The above-mentioned measures were implemented during the testing and the demo activities and no safety issues were identified during the verification and validation phases of the project.

4. BIBLIOGRAPHY

A. Pezzano, e. a. (2022). *D2.14 - Final Version Hazard Analysis and Risk Assessment and Functional Safety Concept.* H2020 Project ENSEMBLE\.

ACEA. (2017). *What is truck Platooning?* Retrieved from ACEA: https://www.acea.auto/files/Platooning_roadmap.pdf

B. Atanassow, K. S. (2022a). *D2.8 - Platooning protocol definition and Communication strategy.* H2020 Project ENSEMBLE.

B. Atanassow, K. S. (2022b). *D2.9 - Security Framework of Platooning.* H2020 Project ENSEMBLE.

ISO26262. (2018). *Road Vehicles - Functional safety.* The International Organization for Standardization.

Mascalchi E., e. a. (2022). *D2.5 - Final Version Functional specification for white label truck.* H2020 Project ENSEMBLE.

P. Dhurjati, e. a. (2022). *D2.15 - Final version of the iterative process and item definition.* H2020 Project ENSEMBLE.

V1.2.1, E. T. (2015). *Intelligent Transport Systems (ITS); Mitigation techniques to avoid intereference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range.* ETSI.

Willemsen, D. S. (2022). *D2.3 - Platooning use cases, scenario definition and Platooning Levels.* H2020 Project ENSEMBLE.

5. APPENDIX A

5.1. Glossary

5.1.1. 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.

Term	Definition
ODD (operational design domain)	The ODD should describe the specific conditions under which a given automation function is intended to function. The ODD is the definition of where (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

Term	Definition
	is large enough (e.g. time gap of 1.5 seconds, which is depends on the 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.

Term	Definition
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, 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 &

Term	Definition
	alternative e.g. successful and failed in relation to activation of the system / system elements).

5.1.2. 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

Acronym / Abbreviation	Meaning
GN	GeoNetworking
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
HARA	Hazard Analysis and Risk Assessment
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

Acronym / Abbreviation	Meaning
PMC	Platooning Mode Control
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