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.	D 2.15
Deliverable Title	Final version of Iterative development process and Item Definition

Dissemination level	Public	
Written By	Prashanth Dhurjati, Alessandro Pezzano, IDIADA	10-12-2021
Checked by	Edoardo Mascalchi, CLEPA	28-01-2022
Approved by	Dehlia Willemsen, TNO	15-02-2022
Status	APPROVED BY EC	05-08-2022

Please refer to this document as:

Prashanth Dhurjati el al., (2022), Final version of the iterative process and item definition, D2.15 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
1.0	13/03/2021	Prashanth Dhurjati (Applus IDIADA)	First version	Prepared
1.1	16/04/2021	Prashanth Dhurjati (Applus IDIADA)	Updated based on review comments from various partners	Revised
1.2	10/12/2021	Prashanth Dhurjati (Applus IDIADA)	Updated based on the latest modifications in D 2.3 and D2.5.	For approval by WP2 partners
1.3	28/01/2022	Edoardo Mascalchi (CLEPA)	Review by WP Leader	For approval by coordinator
1.4	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 fuel economy, traffic safety 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 three main sections:

- Iterative Development Process: This section describes the iterative process used for the functional safety analysis in the ENSEMBLE project.
- Item Definition of the Platooning Support Function: After each iteration of the safety analysis, the definition of the platooning support function was modified so that it can be deployed safely with the current state of the art technology. This section defines the final version of the platooning function that was accepted to be safe as a support function by the ENSEMBLE partners.
- Item Definition of the Platooning Autonomous Function: This section defines the purpose and describes the functionality of the platooning autonomous function. Common item architecture to be used as the reference for all the subsequent safety activities will be defined. The item definition also compiles information on operational and environmental constraints.

1. INTRODUCTION

1.1. Background

The purpose of this deliverable is to describe the iterative process adopted by the ENSEMBLE project to carry out the concept phase activities as per ISO 26262 (ISO26262, 2018).

This work has been performed for the Platooning Support Function only since the iterative process was not required for a concept level like the Platooning Autonomous Function.

These two levels (and related use cases) are defined in D2.3 (Willemsen, 2022) and the related requirements and specifications are listed in D2.5 (Mascalchi E., 2022). Additional details on the Communication protocol can be also found in D2.8 (B. Atanassow, D2.8a) and D2.9 (B. Atanassow, 2022b).

Furthermore, the Safety of the intended functionality (SOTIF) of both levels can be found in D2.13 (P. Dhurjati e. a., 2022). The Functional Safety analysis can be found in D2.14 (A. Pezzano, 2022).

For the first platooning level, the iterative process resulted in multiple iterations of the platooning Level A function's definition and culminated in the current version of the Platooning Support Function.

The first version of the platooning function was defined as the platooning "Level A" function in the deliverable *D 2.10 Iterative Process Document and Item Definition* (P. Dhurjati, 2018) . This deliverable assumed a time gap of 0.8 seconds between the platooning trucks and full automation of the longitudinal control for the following trucks. i.e. the following trucks could apply full deceleration (maximum braking) when applicable as part of the platooning level A function. Safety analysis showed that platooning cannot be deployed as a support function with time gaps below the legal safe limit because the driver could not be expected to supervise the system and act as a fallback immediately when something goes wrong with such low time gaps. Consequently, time gaps close to the theoretical minimum would require fault tolerant ASIL D systems. Such elements (both SW and HW) are not readily available. For this reason, the project ENSEMBLE decided to go with a larger time gap (>1.4s) and limit the automated deceleration to 3.5 m/s^2 for the demonstrations that utilize commercially available trucks without redundant braking systems.

The deliverable D 2.15 Final version of Iterative Process and Item Definition (this document) provides the final version of the Platooning Support Function that was defined in the ENSEMBLE project after multiple iterations of the safety analysis.

Multiple discussions were held with the ENSEMBLE stakeholders to have a first version of the Platooning Autonomous Function. This report also provides the first version of the Item Definition of the Platooning Autonomous Function. It provides an overview of the purpose and describes the functionality of the platooning autonomous function including its Operation Design Domain.

1.2. Structure of the report

This deliverable consists of 3 main sections:

1. Iterative Development Process (Chapter 3)
2. Item Definition of the Platooning Support Function (Chapter 4)
3. Item definition of the Platooning Autonomous Function (Chapter 5)

2. ITERATIVE DEVELOPMENT PROCESS

This section defines the iterative development process followed for the functional safety activities carried out in the ENSEMBLE project. As each OEM will follow their internal development processes for the technical implementation of the defined functional safety requirements, the process defined in this document only applies to the concept phase activities.

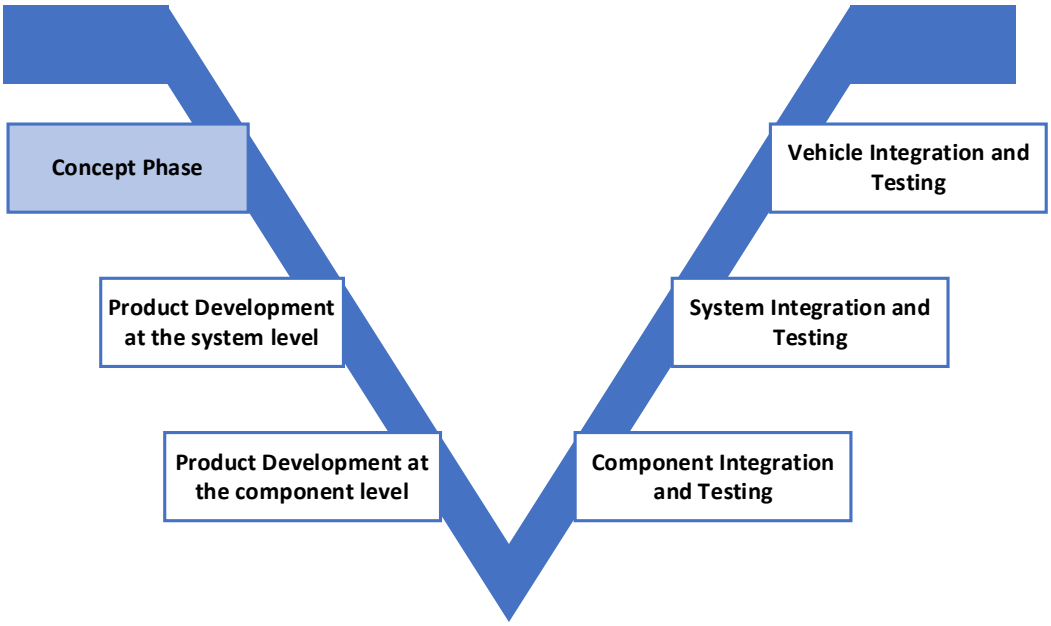

Figure 1 - V Model for Automotive Development

2.1. Iterative process for concept phase activities

Since prototype components (both hardware and software) will be widely used for implementing the support function for the demo, an iterative development process was adopted for the functional safety activities. This helped to keep the safety risks at a manageable level by modifying the functional specifications to lower the ASIL to an acceptable level. i.e. in line with the integrity levels of the existing components.

The following figure outlines the concept phase functional safety activities and the iterative workflow:

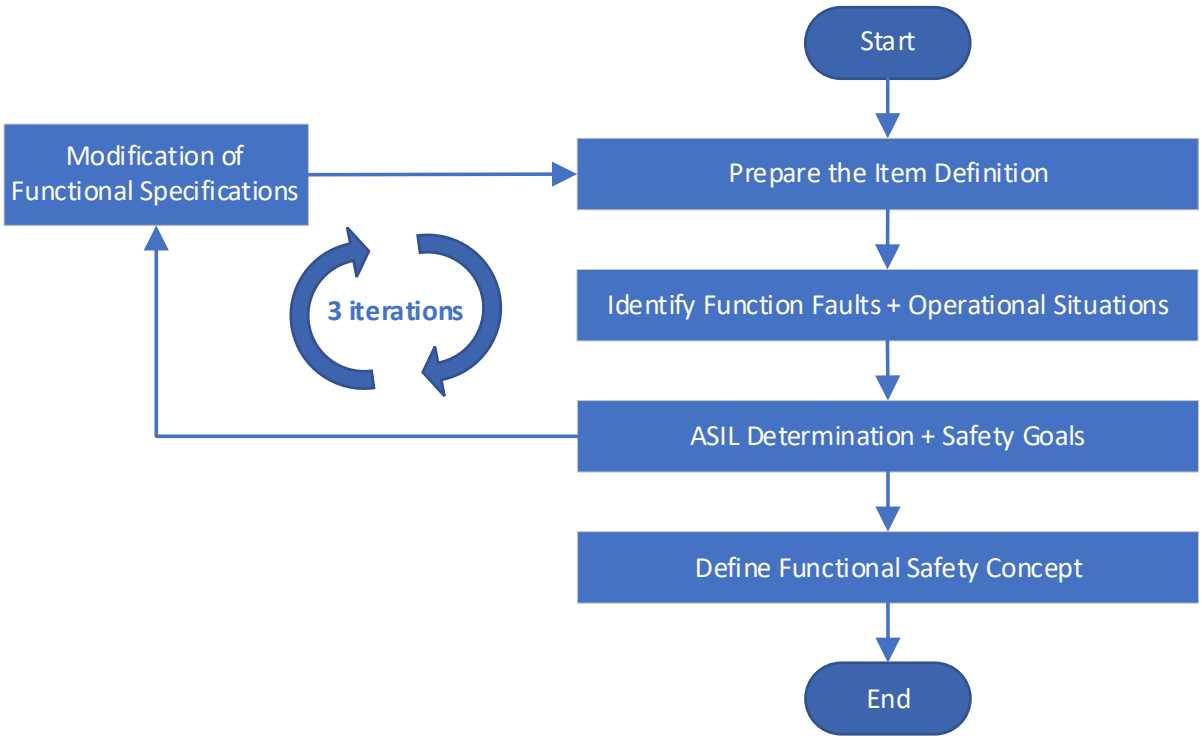

Figure 2 - Iterative process - safety activities

1. **Item Definition:**

The first activity of the concept phase which is common for both functional Safety (ISO26262, 2018) and Safety of the intended functionality (SOTIF) (ISO/PAS21448, 2019) is the generation of the "Item Definition" work product. The "Item Definition" encompasses all the information on the function under development that can assist safety analysis (both SOTIF and Functional Safety) in the subsequent phases of development.

The Item definition usually consists of:

- Functional concept and the high-level requirements of the item,
- Operating modes and states of the item,
- Performance requirements of the item,
- System architecture and the boundary of the item and its interfaces,
- Level of automation/authority on vehicle dynamics,
- Dependencies on and interactions with the driver and occupants,
- Interactions with the road infrastructure and other vehicles,
- Operation design domain including environmental constraints,
- Dependencies and interactions with other functions/systems of the vehicle,
- Constraints and interfaces related to the architecture,
- Potential consequences of behaviour shortfalls including known failure modes and hazards.

2. **Identification of functional faults + Operational Scenarios**

The first task in this activity is to define the function faults/malfunctions that will be analysed for the hazard analysis and risk assessment activity. It is important to limit the list to just the malfunctions at the vehicle level without going to a lower level to identify the source of the failure, E.g. 'Loss of transmission of the V2V information' instead of 'V2V antenna failure'. HAZOP (Hazard and Operability Analysis) methodology will be used to identify the malfunctions at the vehicle level, i.e. apply a set of guidewords that define various ways a function can deviate from its design intent.

Secondly, the operational scenarios in which the functional faults are to be analysed are defined. These conditions will be a combination on what the vehicle is doing (e.g. accelerating to form a platoon), where is this happening (on a highway in rainy conditions) and what is the situation around the vehicle (other vehicle of the platoon, other road vehicles, etc..).

The combination of a hazard with a particular operational situation results in a specific hazardous event. The next step assesses the risks arising from these hazardous events using the method defined in the ISO 26262 - part 3 (ISO26262, 2018).

3. **ASIL determination + Safety goals**

The first task in this activity is to determine the risk parameters (Severity, Exposure and Controllability) for each of the hazardous events identified in the previous activity. Once the risk parameters are determined, Automotive Safety Integrity Levels (ASIL) will be assigned to the hazardous event from the standardized matrix provided in the ISO 26262 (ISO26262, 2018).

Secondly, safety goals shall be defined for the hazardous events that have an ASIL greater than 'QM'. Safety goals are top level safety requirements that are not expressed in terms of technological solutions, but in terms of functional objectives.

4. **Modification of functional specifications**

After the determination of the ASILs and the safety goals, the required ASILs are compared with integrity levels of the available elements (SW and HW) that will be used for the project. If the ASILs do not meet the required targets, then the function is modified to reduce the risk to an acceptable level.

5. **Functional Safety Concept**

This activity shall derive the functional safety requirements from the safety goals and allocate them to the E/E functions, other technologies (e.g. mechanical, pneumatic,…) and external measures (elements outside the item boundary, e.g. guide rails).

These are implementation independent requirements to the behaviour of the item aimed at achieving the safety goals defined in the previous activity. The functional safety requirements shall be specified

by considering, if applicable, the operating modes, the fault tolerant time intervals, safe states, and emergency operational interval and function redundancies.

2.2. Changes after each iteration

The following table outlines the highest ASILs from each version of the platooning function and the subsequent modifications done to the function definition after each iteration to lower the ASILs to an acceptable level:

Function	Description	Highest ASIL	Comments
Version 1	Time Gap 0.8s Full longitudinal control	ASIL D	Unintended braking [ASIL D]. Unintended acceleration [ASIL B] Loss of braking [ASIL C] Loss of V2V communication [ASIL C]
Version 2	Time Gap 1.4s Full longitudinal control	ASIL D	Unintended braking [ASIL D]. Unintended acceleration [QM] Loss of braking [ASIL A] Loss of V2V communication [ASIL A]
Version 3 (Platooning Support Function)	Time Gap 1.4s Deceleration limited to 3.5 m/s^2	ASIL B	Unintended braking [ASIL B] (changed from ASIL D to ASIL B due to constraints on maximum permitted deceleration). Loss of platooning function [QM] (e.g. lack of braking, lack of acceleration, lack of V2V communication, …).

Table 1: Safety analysis iterations – Support function

In conclusion, for the Platooning Support Function, malfunctions that cause loss of the platooning function are acceptable (QM) since the drivers are responsible for the Dynamic Driving Task (DDT). Whereas the malfunctions that result in unintended behaviour still gets an ASIL, i.e. not acceptable.

3. ITEM DEFINITION OF THE PLATOONING SUPPORT FUNCTION

3.1. Platooning Support Function Concept

Truck platooning is a function to drive trucks in organized convoys communicating via vehicle-to-vehicle communication (V2V) to each other. The platooning trucks consist of a leading truck and following trucks. The platooning 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 in closer distances, which opens the possibility to reduce fuel consumption and CO_2 output by air drag benefits and increase the road's traffic intensity in a safe way.

The platooning support function developed within the ENSEMBLE project has the following features:

- **System Automation:** The support function is a SAE level 1 (SAEJ3016, 2014) automation feature where only the longitudinal vehicle motion (no steering automation) is automated for the following trucks.
  The current function does not automate any driving task for the leading truck.

- **Communication:** All platoon vehicles are connected via V2V wireless communication to share information like status, speed, current and intended acceleration and other dynamic parameters required for safe platooning.

- **Following distances:** Under steady-state driving conditions, the platooning function maintains minimum time gaps similar to state-of-the-art ACC systems (between 1.4 and 1.6 s). Drivers can select gaps above this value based on their current ACC systems.

- **Vehicle longitudinal motion control:** For the support function the automation of the longitudinal control for the following trucks is limited to acceleration values greater than -3.5 m/s^2. All situations that require acceleration smaller than – 3.5 m/s^2 are handled by the driver.

- **Vehicle lateral motion control:** Steering is not automated. The driver is responsible to steer the vehicle in all driving conditions.

- **Operation Design Domain (ODD):** The ODD is limited to:
  - Highways within the EU.
  - All weather conditions experienced with the EU.
  - All light conditions (day and night including low visibility conditions like fog, snow, etc…)

- Speed range from 0 to 90 km/h (top speed can be lower depending on country regulations).

- **Dynamic Driving Task (DDT):** Drivers are mandatory in all the trucks. In the following tucks, along with steering, the drivers are the DDT fallback of the support function. He/she is responsible to monitor the system's performance and respond to inappropriate actions taken by it.

  The platooning function does not have the ability to perceive the weather conditions and react appropriately. The driver is also responsible to increase the time gaps or disable the function if deemed appropriate under certain circumstances like adverse weather conditions, toll gates, etc.

- **Other services:** Interaction with platooning services and infrastructure is technically available. Features like zone policies and speed limits are displayed to the driver via the HMI. The V2I information has no influence on the platooning support function.

3.2. Item Boundary Diagram of the Platooning Support Function

The item is an array of systems (AoS) capable of implementing a platooning support function at the vehicles level, to which ISO 26262 (ISO26262, 2018) will be applied.

The following figure shows the item, its elements, and the relationship to external elements:

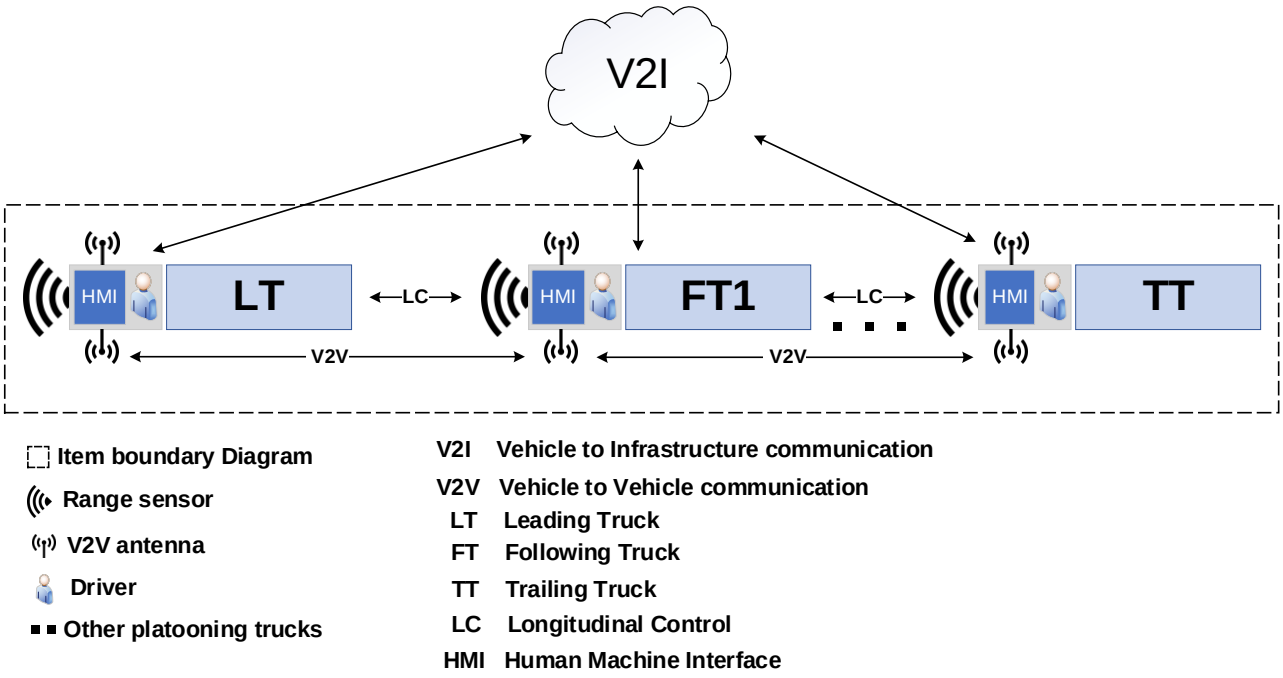

Figure 3 - Item boundary diagram – Support function

The item consists of the following elements:

Leading Truck (LT): The leading truck is the platoon leader. Longitudinal and lateral vehicle motion controls are not automated by default. Leading truck can be equipped with driver assistance systems (e.g. ACC, LKA). The automation of the leading truck is not within the scope of the ENSEMBLE project.

Following Truck (FT): Following trucks trail the leading truck. Longitudinal motion control is automated for the following trucks. Following trucks can also use other driver assistance systems (e.g. LKA) to assist while platooning.

Trailing Truck (TT): The last truck in a platoon is called the trailing truck. i.e. last of the following trucks.

Vehicle to Vehicle (V2V) communication: All platoon vehicles are connected via V2V to share information on their status, speed, current and intended acceleration and other dynamic parameters required for safe platooning.

Vehicle to Infrastructure (V2I) communication: The trucks may receive information related to zone policies or speed limits from infrastructure.

Drivers: Drivers are present in all the trucks and are responsible for the Dynamic Driving Task (DDT).

The following systems within each truck are outside the scope of the safety analysis:

Braking system: The system responsible to receive deceleration request from the platooning function and control the service brakes. The control of the brake lights also falls under the scope of the braking system.

Powertrain system: The engine and the drivetrain system responsible to receive acceleration request from the platooning function and provide the forward or backward movement of the vehicle.

3.3. High level requirements of the support function

This section defines the high-level functional requirements of the support function. These requirements will be used to identify malfunctions for the hazard analysis and risk assessment.

For complete set of requirements refer to the deliverable “D 2.5 – Final version Functional specification for white label truck, operational and tactical layers.” (Mascalchi, 2022).

Note: HLR_PSF = High Level Requirements _ Platooning Support Function

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.

3.4. Assumptions on the Platooning Support Function

The following assumptions have been made about the platooning support function:

- 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. For 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 project).
- 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. When the platooning function cannot be maintained, the longitudinal control will be handed back to the drivers with appropriate warning.
- Platoon communication will be switched to lower power when passing toll gates due to ETSI TS 102 792 (V1.2.1, 2015) requirements. Deactivation is responsibility of the driver. Platoon might be deactivated automatically based on information received from infrastructure.
- The project shall aim to maintain a minimum time gap of 1.4 seconds for the support function.

4. ITEM DEFINITION OF THE PLATOONING AUTONOMOUS FUNCTION

4.1. Platooning Autonomous Function (PAF) Concept

Truck platooning is a function to drive trucks in organized convoys communicating via vehicle-to-vehicle communication (V2V) to each other. The platooning trucks consist of a leading truck and following trucks. The platooning 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 in closer distances, which opens the possibility to reduce fuel consumption and CO_2 output by air drag benefits and increase the road's traffic intensity in a safe way.

The platooning autonomous function being defined within the ENSEMBLE project has the following features:

- **System Automation:** The autonomous function does not fall squarely into any of the SAE automation categories, but when in platooning mode, the function closely resembles an SAE level 4 feature where the entire Dynamic Driving Task (DDT) is automated for the following trucks within the ODD and the system is the DDT fallback. The DDT task include automation of longitudinal and lateral vehicle control and the task of Object and Event Detection and Response (OEDR). When required, the following trucks can perform Minimum Risk Manoeuvres (MRM) and reach a Minimum Risk Condition (MRC) without any human intervention.
  The current version of the function does not automate any of the driving tasks of the leading truck.

- **V2V Communication:** All platoon vehicles are connected via V2V wireless communication to share information like status, speed, current and intended acceleration and other dynamic parameters required for safe platooning.

- **Following distances:** As a starting point, under steady-state driving conditions, the platooning function maintains time gaps similar to the state-of-the-art ACC systems (between 1.4 and 1.6 s). Using the Braking Performance Assessment functionality (defined in D2.5 (Mascalchi E., 2022)) it is then possible to achieve shorter following distances.

- **Longitudinal Control:** Longitudinal control is fully automated for the following trucks and covers the whole vehicle capability envelope. Individual trucks can decelerate up to their maximum capability, enabling the system to perform emergency braking manoeuvres.

- **Vehicle lateral motion control:** Steering is fully automated for the following trucks and offers both in-lane driving and lane change capabilities. Emergency steering (high lateral acceleration) is considered out of scope for the current version of the autonomous function.

- **Perception:** The following trucks are fully equipped with perception system capable of L4 autonomous driving except for the detection of traffic signs which still fall under the responsibility of the leading truck driver. The trucks shall be able to independently detect obstacles in their vicinity and take evasive action without human intervention. This ability is used to follow the forward truck safely.

- **Operation Design Domain (ODD):** The ODD is limited to:
    - Maximum of 4-hour Hub-to-hub highway driving routes within the EU (This limitation is introduced to eliminate refuelling and leading truck driver resting times, as described in Regulation (EC) No 561/2006).
    - Traffic lights, roundabouts, tunnels, and T-junctions encountered on connector routes between the hubs and the highways.
    - Onramps, offramps, highway junctions, road works, toll gates and tunnels typically encountered on EU highways.
    - Resting areas and parking lots adjacent to EU highways.
    - All weather conditions experienced with the EU.
    - All light conditions (day and night including low visibility conditions like fog, snow, etc…)
    - Speed range from 0 to 90 km/h (top speed can be lower depending on country regulations).
    - Only the following trucks of the platoon.

- **Dynamic Driving Task (DDT):** Only the driver of the leading truck has the responsibility of the dynamic driving task (DDT). The driver is responsible to follow the traffic rules and navigate the following trucks to the destination but is not responsible for their safety. Each following truck must handle unsafe situations without any intervention from the leading truck's driver. The following trucks are driverless but can be manned. When manned, no DDT responsibilities are given to the occupants.

- **V2I Communication:** The platoon depends on intelligent infrastructure to maintain cohesion while traversing the routes between the hubs and the highways. V2I communication is used to inform the infrastructure (intelligent traffic lights, toll gates, etc …) about the approaching platoon, so that the surrounding traffic is controlled to favour easy passage of the platoon. The platoon also receives information related to specific events like accidents, speed limits, etc so that the leading vehicle's driver can plan his route efficiently.

4.2. Item Boundary Diagram of the PAF

The item is an array of systems (AoS) capable of implementing a platooning support function at the vehicles level, to which ISO 26262 (ISO26262, 2018) will be applied.

The following figure shows the item, its elements, and the relationship to external elements:

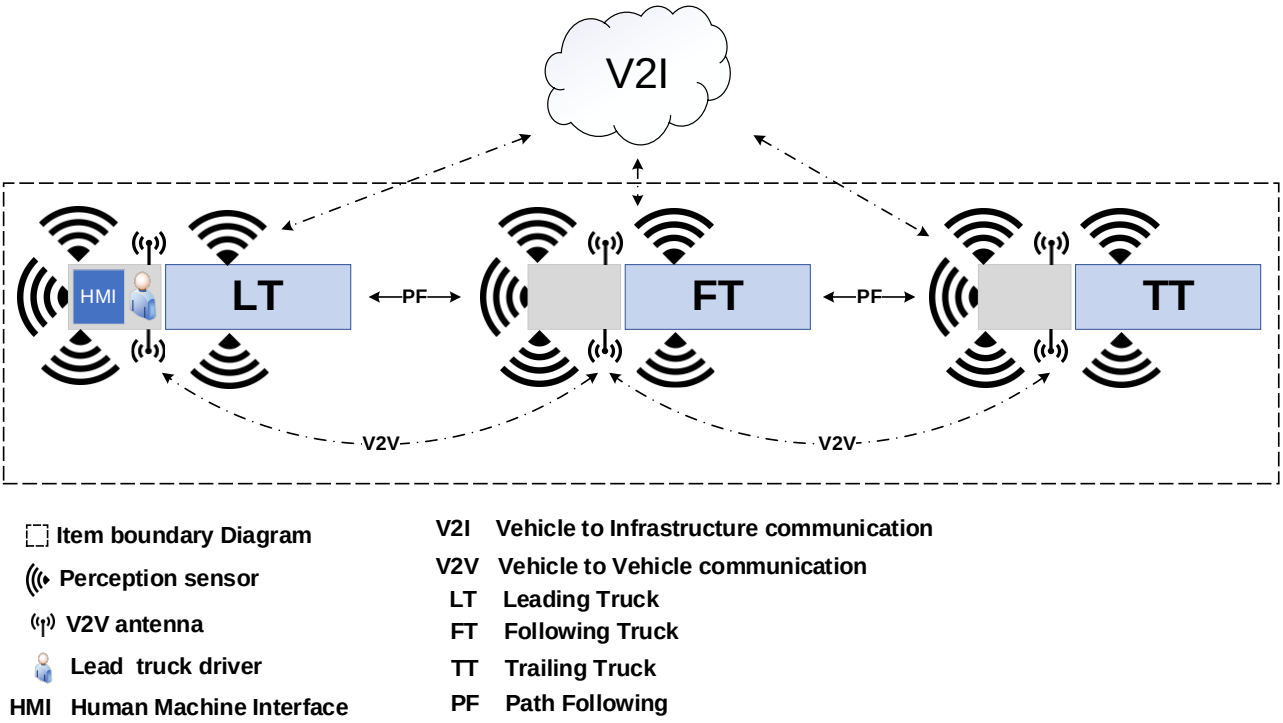

Figure 4 - Item boundary diagram – Autonomous function

The item consists of the following elements:

Leading Truck (LT): The leading truck is the platoon leader. Longitudinal and lateral vehicle motion controls are not automated by the platooning function, but the lead truck can be equipped with automated driving systems (e.g. ACC, LKA). The automation of the lead truck is not within the scope of the ENSEMBLE project.

Following Truck (FT): Following trucks trail the leading truck. Once engaged, no drivers are required in the following trucks and the entire task of DDT is automated. If required, the following trucks can perform Minimum Risk Manoeuvres (MRM) and reach a Minimum Risk Condition (MRC) without any human intervention.

Trailing Truck (TT): The last truck in the platoon is called the trailing truck. The automation is the same as any following truck.

Perception: Each following truck has its own on-boards perception system which can observe its surrounds and build an accurate model of the world around it. This information is used to follow the forward truck safely and perform minimum risk manoeuvres autonomously without any human intervention.

Vehicle to Vehicle (V2V) communication: All platoon vehicles are connected via V2V to share information on their status, speed, current and intended acceleration and other dynamic parameters required for safe platooning.

V2I: The leading truck communicates with the infrastructure to assist with the traffic flow. Platoon position is communicated to control the external traffic through intelligent traffic lights.

Drivers: Driver is only required in the leading truck of the platoon within the ODD. The driver is responsible to follow the traffic rules and navigate the following trucks to the destination.

The following systems within each truck are outside the scope of the safety analysis:

Braking system: The system responsible to receive deceleration request from the platooning function and provide the service brakes. The control of the brake lights is also considered within the scope of the braking system.

Powertrain system: The engine and the drivetrain system responsible to receive acceleration request from the platooning function and provide the forward or backward movement of the vehicle.

Steering system: The system responsible to receive steering requests from the platooning function and control the lateral movement of the vehicle by turning the wheels. The control of turn indicators is also considered within the scope of the steering system.

4.3. High level requirements of the Platooning Autonomous Function

This section defines the high-level functional requirements that will be analysed to identify malfunctions for the hazard analysis and risk assessment. For complete set of requirements refer to the deliverable D 2.5 – Final version Functional specification for white label truck (Mascalchi E., 2022).

Since the function is at a very early state of definition, HMI and driver information related functions has been excluded for now. They will be analysed in future projects.

Note: HLR_PAF = High Level Requirements _ Platooning Autonomous Function

HLR_PAF_01: V2V Communication
While platooning, each truck shall communicate its intended path and other dynamic parameters to the following trucks.

HLR_PAF_02: V2I Communication

The platoon shall be able to negotiate (send/receive information) its intention to cross specific infrastructure (e.g. toll gates, intelligent traffic lights, roundabouts) till the end of the manoeuvre.

HLR_PAF_03: Perception
The following trucks shall perceive their surroundings to create an environment model precise enough to follow the forward truck, avoid collisions and safely perform minimum risk manoeuvres when required.

HLR_PAF_04: Braking
The following trucks shall brake autonomously to maintain a safe distance to the objects in its path.

HLR_PAF_05: Acceleration
The following trucks shall accelerate autonomously to maintain the set time gap to the forward truck.

HLR_PAF_06: Steering
The following trucks shall steer autonomously to keep their lane or change lane to follow the intended path of the forward truck in the platoon.

4.4. Assumptions on the Platooning Autonomous Function

The following assumptions:

- The maximum number of trucks in an autonomous platoon is limited to 3.
- Platoon formation is orchestrated and is a non-real time operation. i.e. drivers manually arrange vehicles in line and in the right order before engaging while stationary.
- Platoon engaging can be done while stationary (e.g. at the hubs) or while driving (for trucks joining with a driver).
- New members of a running platoon can only join from the rear of the platoon.
- Platoon disengaging can be done while stationary (e.g. at the hubs) or while driving.
- Only the trailing truck (when manned) can disengage while driving. This avoids a middle truck from disengaging and take an unmanned trailing truck with it.
- There are no limits on the deceleration of the following trucks. i.e. full braking is allowed in emergency situations.
- When in a platoon, the following trucks are fully capable of driving autonomously (build-in perception, localization, trajectory prediction, path planning and control). They only depend on the forward truck for information on path planning.
- Each following truck is responsible for its own safety. No human intervention (including the lead truck's driver) is required.
- The leading truck's driver can enable "lateral following" mode in which the following trucks will follow the same path as the leading truck, considering the restrictions from other traffic, delimiters, etc.

- When at standstill, the leading truck's driver can enable "Standby mode", wherein the following trucks shutdown the engines and maintain communication to unlock the truck or start it again for platooning.
- The vehicles shall be able to carry loads as per the legal weight limits of member countries.

5. SUMMARY AND CONCLUSION

This deliverable outlines the iterative development process followed by the safety team to carry out the concept phase functional safety activities (as per ISO 26262 (ISO26262, 2018)) of the Platooning Support Function. It shows how multiple iterations were required to keep the safety risks at a manageable level, by modifying the functional specifications to lower the ASIL to an acceptable level. This ensured that the risk posed by the function is in line with the integrity levels of the existing hardware and software components used for development by the various OEMs.

The deliverable also provides the final version of the item definition of the Platooning Support Function.

The support function has the following main features:

- ODD: EU highways.
- Automation: Only the longitudinal control is automated by the function for the following trucks.
- Deceleration: While platooning, the deceleration is limited a maximum of 3.5 m/s² (similar to existing adaptive cruise control systems).
- DDT: All the trucks must have a driver onboard and they are responsible for the Dynamic Driving Tasks (DDT).

Lastly, the deliverable also provides an initial version of the item definition of the platooning autonomous function.

The Platooning Autonomous Function has the following main features:

- ODD: Maximum of 4-hour Hub-to-hub highway driving routes within the EU.
- Automation: Both longitudinal and lateral vehicle motion is automated by the function for the following trucks.
- Deceleration: While platooning, there are no limits on the braking. i.e. if required, full braking can be applied autonomously by the following trucks.
- DDT: Only the leading truck must be manned to navigate the platoon, the following trucks can be driverless. All the Dynamic Driving Tasks (DDT) are fully automated for the following trucks and the platooning system is the DDT fallback.

6. REFERENCES

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

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.

ISO/PAS21448. (2019). *Road Vehicles - Safety of the intended functionality.* ISO/PAS.

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

J. Vissers, e. a. (2018). *D2.2 - V1 Platooning use-cases, scenarion definition and platooning levels.* H2020 Project ENSEMBLE.

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

P. Dhurjati, e. a. (2022). *D2.13 - SOTIF Safety Concept.* H2020 Project ENSEMBLE.

P. Dhurjati, L. M. (2018). *D2.10 Iterative process document and Item Definition.* IDIADA.

SAEJ3016. (2014). *SAE Levels of driving automation.* SAE.

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

7. APPENDIX A

7.1. Glossary

7.1.1. 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.

Term	Definition
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 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.

Term	Definition
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 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.

Term	Definition
	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

Term	Definition
	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).

7.1.2. 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

Acronym / Abbreviation	Meaning
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

Acronym / Abbreviation	Meaning
LSG	Legal Safe Gap
MAP	Map Data 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
PMC	Platooning Mode Control
QM	Quality Management
RSU	Road Side Unit
SA	Situation Awareness
SAE	SAE International, formerly the Society of Automotive Engineers
AoS	Array of Systems
SCH	Service Channel

Acronym / Abbreviation	Meaning
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
TTG	Target Time Gap
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WP	Work Package