ENSEMBLE

EUROPEAN COMMISSION

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

ENSEMBLE

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

Deliverable No.	D2.13	
Deliverable Title	SOTIF Safety Concept	
Dissemination level	Public	
Written By	Prashanth Dhurjati, IDIADA	05-17-19
Contributors	Simon Ellwanger, Daimler Hans Nordin, SCANIA Julien Stephane, Volvo Patrick Jiskra, MAN	05-17-19

	Wim Baaten, DAF Luca Toninello, IVECO Elmar Staudacher, Bosch Massimo Distefano, Brembo	
Checked by	Lina Konstantinopoulou, CLEPA	28-05-2019
Approved by	Marika Hoedemaeker TNO	05-06-2019
Status	Final, submitted under approval by EC	05-06-2019

Please refer to this document as:

Prashanth Dhurjati, (2019). *SOTIF Safety Concept.* D2.13) 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 are 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	17/05/2019	Prashanth Dhurjati (IDIADA)	First Release	Prepared / Revised/ Authorised
1.1	28/05/2019	Prashanth Dhurjati (IDIADA)	Adjusted based on input partners	Submitted to WP leader
1.2	05/06/2019	Prashanth Dhurjati (IDIADA)	Adjusted based on comments WP leader	Submitted to coordinator
2.0	05/06/2019	Prashanth Dhurjati (IDIADA)	Finalised with latest comments	Final

FIGURES

1. EXECUTIVE SUMMARY

1.1. Context and need of a multi brand platooning project

Context

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

Project scope

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

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

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

Abstract of this Deliverable

This deliverable contains SOTIF (Safety Of The Intended Functionality) requirements that are applicable to platooning level A when operated within the defined Operation Design Domain.

Platooning level A is defined within Ensemble as follows (more detailed specifications can be found in D2.4):

- a benefit in terms of e.g. fuel savings, safety, logistics...
- longitudinal automation with fail operation, not lateral automation.
- a following distance targeting between 0.8 and 1.4 s. (as close as possible to reach the benefits), This requires new longitudinal functions, e.g. Brake Performance Calculation and safety functions e.g. redundant braking functions, additional sensors.

- the system is in control of the longitudinal functional safety of the vehicle.

This deliverable consists of 3 parts:

- Introduction: This section provides an overview of the basic concepts behind SOTIF analysis.
- SOTIF Hazard Identification and Risk Evaluation: This section compiles all the known unsafe scenarios that have been identified to be relevant to platooning level A and analyse the risks associated with them. This section also outlines the counter measures defined to address the safety risks.
- SOTIF safety requirements: This section derives the SOTIF safety requirements from the counter measures defined after hazard identification and risk evaluation.

2. INTRODUCTION

2.1. Background

Safety of the Intended Functionality (SOTIF) aims to avoid unreasonable risk caused by hazards associated with the nominal functionality and its implementation. This includes hazards arising from technological and system shortcomings, performance limitations and reasonably foreseeable misuse. Hazards arising due to E/E failures are dealt separately through functional safety and do not form part of the SOTIF activities.

The current standard available on SOTIF is the ISO/PAS 21448. This standard is generally applicable to Advanced Driver Assistance Systems (ADAS) with automation levels (1 and 2) where proper situational awareness derived from complex sensors and processing algorithms is critical to safety. Although the standard does address functions working in a co-operative manner on multiple vehicles, its basic methodology can be applied to Platooning.

2.2. Key SOTIF definitions and concepts

2.2.1. Definitions

This section defines key vocabulary used for SOTIF activities.
Note: The following definitions are taken from J3016, ISO 21448 and ISO 26262 for consistency.

Operation Design Domain (ODD):
Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics."

Use case
A specific situation in which a vehicle could potentially be used.

Operational situation
A scenario that can occur during a vehicle's life.

Scenario
Description of the temporal development between several scenes in a sequence of scenes.

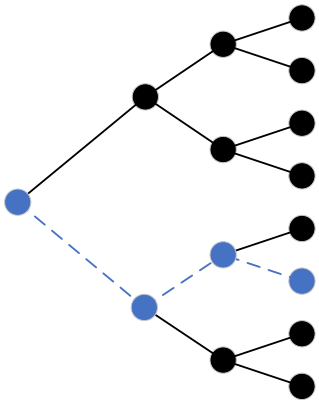


Figure 1 - Scenario (dashed) as a temporal sequence of events (edges) and scenes (nodes)

Scene
Snapshot of the environment including the scenery, dynamic elements, and all actor and observer self-representations, and the relationships between those entities.

Misuse
Usage of the system by a human in a way not intended by the manufacturer of the system.
Misuse can result from overconfidence in the performance of the system.
Misuse also includes human behaviour that is not specified but does not include deliberate system alternations.

Triggering Events
Specific conditions of a driving scenario that serve as an initiator for a subsequent system reaction possibly leading to a hazardous event.
E.g. While driving in a platoon, a vehicle misidentifies a road sign as a lead vehicle resulting in braking at X g for Y seconds.

Hazard
A potential source of harm caused by unintended behaviour of the function.

Hazardous Event
Combination of a hazard and an operational situation.

Harm
Physical injury or damage to the health of persons.

Hazardous Event Model
The diagram below provides a visualization of a potential SOTIF related hazardous event model.

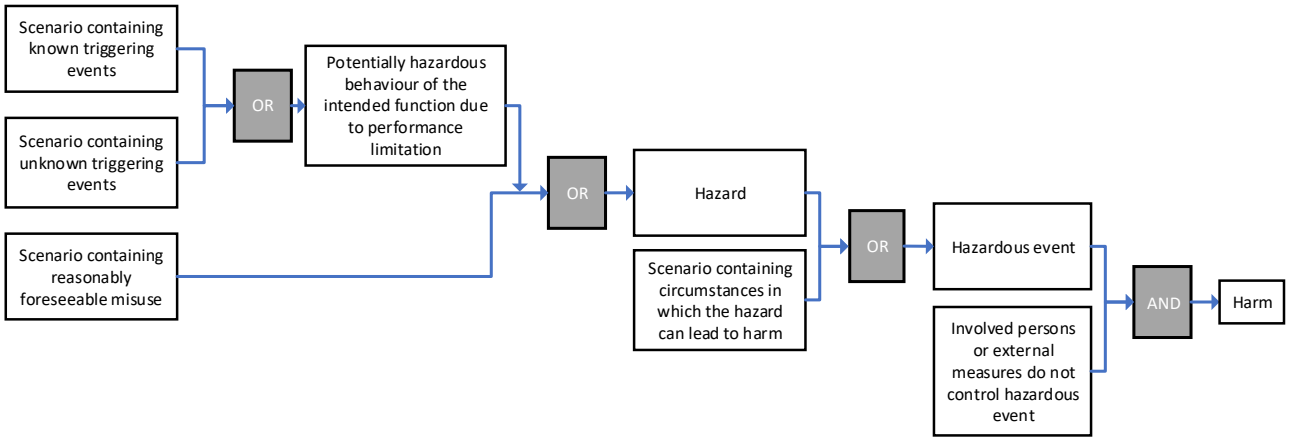
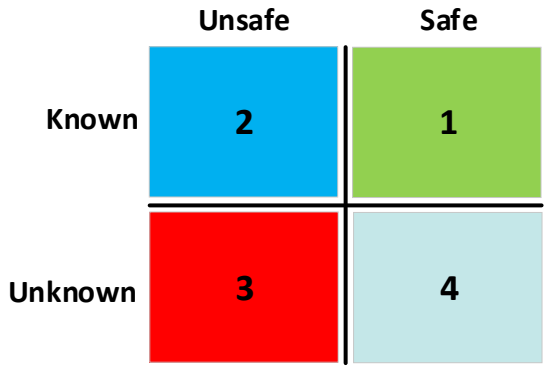


Figure 2 - Hazardous Event Model (ISO/PAS 21448)

The operational design domain (ODD) of the function consists of several use cases that contain triggering events related to external factors such as environmental conditions, road conditions, traffic conditions or driver misuse. The hazards arising from these triggering events when combined with specific operational scenarios lead to a hazardous event that can result in harm.

2.2.2. SOTIF scenarios

The scenarios that can be encountered within the operational design domain (ODD) of any automated driving function can be categorised as below:



1. Known Safe Scenarios
2. Known unsafe scenarios
3. Unknown unsafe scenarios
4. Unknown safe scenarios

The diagram below provides a graphical view of how all the scenarios that can be encountered by an autonomous system in the field are categorised. The area under each region is roughly representing the number of scenarios in each category.

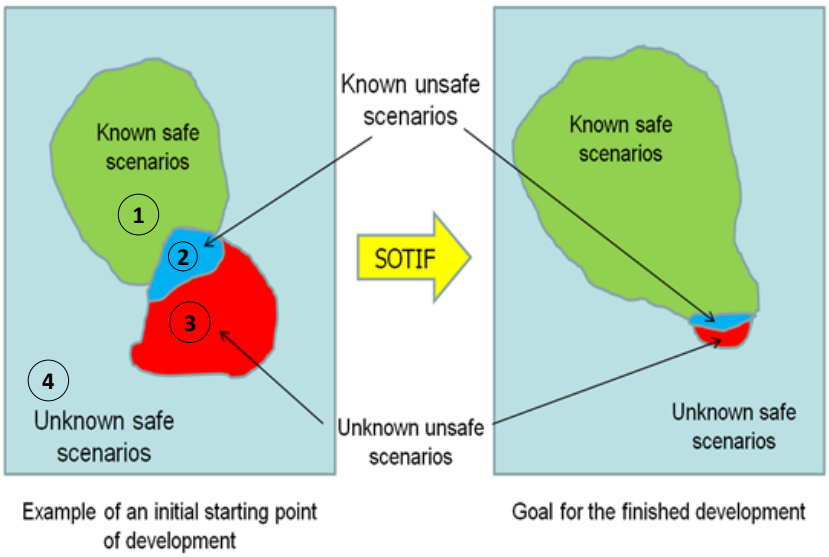


Figure 3 - Evolution of scenario categories (ISO /PAS 21448)

At the start of the SOTIF activities, the area under the unsafe scenarios (both known and unknown) is large resulting in unacceptable residual risk. The objective of the SOTIF activities is to identify and reduce the number of unsafe scenarios such that the residual risk falls to an acceptable level.

The goals of the SOTIF activities with respect to Area1, Area2, and Area3 (see Figure 3 - Evolution of scenario categories (ISO /PAS 21448) and relevant scenarios are:

- Area1: Maximize or maintain area, by minimizing the areas 2 & 3. This retains or improves safe functionality.
- Area2: Minimize area by identifying the risks arising from the known unsafe scenarios and implement technical measures to improve the function (if possible) or by restrict performance or use of the function (e.g. redefining ODD). Once the measures are evaluated through testing, the scenarios can be moved to Area 1.
- Area3: Minimize area (the risk of the unknown) using field operations tests (validation) tests to identify previously unidentified unsafe scenarios and move them to Area2.

2.3. Aim

In the ENSEMBLE project, the SOTIF activities will be confined to Area 2 – known unsafe scenario. This includes identifying and documenting known unsafe scenarios and related triggering events, evaluating risks associated with these scenarios and defining counter measures and safety requirements to shift the known unsafe scenarios to known safe scenarios.

2.4. Structure of this report

The report contains two main sections:

2.4.1. Hazard Identification and Risk Evaluation

This section documents the known unsafe scenarios identified to be unsafe for the platoon and combines them with associated triggering events to analyse their potential hazardous consequences. These hazards are then evaluated for their risk levels and if applicable counter measures are defined to lower the risk to an acceptable level.

The methodology proposed by ISO 26262 is used to identify risks associated with each hazard. Since SOTIF does not handle malfunctions, the exposure class of the scenarios will not be classified. The risk assessment is solely based on the controllability and severity of the hazardous event.

The risk levels are rated from 1 to 6, where hazards resulting in risk levels below 2 are considered low risk, 2 – 4 medium risk and 5 – 6 high risk. Higher the risk, greater should be the integrity level of the safety mechanisms.

This section also documents the counter measures proposed for each hazard analysed during the safety workshops.

For each of the scenarios that resulted in a hazard, counter measures were derived by answering three main questions:

1. Does this scenario (and the trigger event) fall under the current platooning level A's operation design domain (ODD)? If yes, then

2. Does the required reaction of platoon to be safe involve only longitudinal control?

If answers to the above two questions is yes, then they shall be handled without any driver intervention (i.e. handled automatically by the platooning function). No shared responsibilities for longitudinal control between the system and the driver shall be allowed within the ODD.

This led to the final question:

3. How should the function be improved to handle this scenario?

This three questions methodology was followed for all the use cases analysed for SOTIF.

2.4.2. SOTIF Safety Requirements

This section refines the counter measures defined after the hazard identification and risk evaluation activity to safety requirements that fall under the following four categories:

1. Application requirements: Requirements on the platooning function.

2. Communication requirements: Requirements on the V2V communication established between the trucks
3. HMI requirements: Requirements on the interactions between the driver and the platooning system.
4. Driver requirements: Requirements on the drivers.

3. HAZARD IDENTIFICATION AND RISK EVALUATION

This section contains the results of the hazard identification and risk evaluation activity carried out through various safety workshops and discussions.

Seven different categories of use cases were analysed under this activity:

1. Infrastructure and other external factors: These use cases contain triggering events that either originate from the infrastructure e.g. toll gates, tunnels, obstacles on the lane… or other external factors like adverse weather conditions, loss of GPS signal...

2. Emergency braking: These use cases contain triggering events resulting in full emergency braking of the trucks in the platoon.

3. Cut-ins: These use cases contain triggering events related to external vehicles intruding into the platoon.

4. Platoon function specific or other internal factors: These use cases contain triggering events intrinsic to the platoon function (e.g. increasing or decreasing the time gap, joining from behind…).

5. Driver Behaviour and misuse: These use cases contain triggering events originating from driver's interaction with the function (e.g. driver forcing control back, making uninformed lane change…).

6. Communication: These use cases contain triggering events related to communication between the trucks.

7. Non-EE malfunctions: Even though not part of the SOTIF, a use case related to non-EE malfunctions like tyre blowout, oil leaks... is analysed here.

3.1. Infrastructure and other external factors

3.1.1. Loss of GPS Signal

Ego truck loses GPS signal during steady state platooning.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Loss of GPS signal
Consequence	Trucks cannot estimate their positions accurately
Hazard	The impact of loss of GPS is not yet known. To be defined after the specifications are complete.

Risk Evaluation:	
Severity (S0 – S3)	-
Severity Rational	-
Controllability (C0 – C3)	-
Controllability Rational	-
Risk Value	To be defined.

Counter Measures Definition:	
Counter Measures	Requirement: The trucks shall continue sending PCM (Platoon control messages) irrespective of the availability of the GPS signal.
Rational	The usage of the GPS signal for the function is not yet defined. So, the consequence of missing GPS information is unknown. This situation will be reanalysed once the specifications are available.

3.1.2. Approaching a highway Entry/Exit ramp

Platoon is approaching a highway entry/exit ramp while other vehicles are trying to enter or exit the highway.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Platooning in steady state mode
Triggering Event	Platoon approaches a highway Entry/Exit ramp

Consequence	Other road vehicles are not able to exit/enter the highway until the entire platoon has passed
Hazard	Other road vehicles stopped on the entry ramp or near the exit ramp (on the highway) may cause rear end collisions on the entry lane or some vehicles may try to forcefully cut-in instead of waiting

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents between external vehicles and a platoon on a highway can result in life threatening injuries
Controllability (C0 – C3)	C2
Controllability Rational	Highway entry ramp: The situation is simply controllable as most of the cut-in drivers will wait for the platoon to pass by before entering the highway. But in rare cases, the drivers might lose patience if the platoon is long or new drivers entering the entry ramp might not notice the stopped vehicle and lead to rear end collision. (C1) Highway exit ramp: This situation is more difficult to control, as any vehicle on the left lane trying to exit the highway will encounter a convoy that does not give enough space to cross over. Cut-through might be easily controllable, but wrong reaction from the external vehicle can result in him braking aggressive or coming to a stop in the middle of the highway which is difficult to control. (C2)
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation will not be automated. - The existing function shall not be modified for this situation: • Increase the time-gap automatically if zone policies require it. • If no zone policies exist, then for Level A the function shall continue platooning in the current state. - Each truck driver still has the right to decide on his own if he wants to give way by decreasing the speed or increasing the time-gap or exiting the platoon.
Rational	It would be inefficient to increase and decrease the time gap or speed every time an entry or exit ramp is encountered (on an average every 2 - 3 kms). This will defeat the whole purpose of platooning for efficiency. Moreover, cut-ins are encouraged due by increasing the time-gaps.

	For the exit ramps, usually vehicle will plan for their exit in advance and place themselves behind the platoon. Any cut-through action at the last movement will be treated as any cut-in event. Unless the number of trucks in a platoon is high (> 5), it should not create safety issues. No hazard arises if the vehicles using the ramp follow traffic rules. Note: Road transport authorities in Germany have requested special measures to handle highway entry/exit ramps. Comments: Entry and exits will be treated as cut-ins.

3.1.3. Passing through toll gates

Platoon is approaching a toll gate.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon approaches a toll gate
Consequence	V2V communication between vehicles is restricted due to interference with the toll's infrastructure
Hazard	Trucks might not be able to transmit safety critical information via V2V which might make maintaining a time-gap of 0.8 seconds unsafe.

Risk Evaluation:	
Severity (S0 – S3)	S2
Severity Rational	Since the trucks are already slowing down when approaching a toll gate, collision at low speed might not result in life threatening injuries.
Controllability (C0 – C3)	C2
Controllability Rational	Since the vehicles are slowing down and approaching a toll gate, the driver is more attentive to the situation and any abnormal behaviour is normally controllable.
Risk Value	4 (Medium Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall not be automated.

	- The existing function shall not be modified for this situation: • If Zonal policy restrictions are communicated through V2I, then each truck shall decrease the power levels of the V2V communication radios (part of normal functionality). • If no zone policies requests (reduce speed, min distance between vehicles, …) are available, then the function need not do anything specific for traversing the toll gates. Platoon shall maintain the current state. • If any truck experiences loss of information/ communication (e.g. due to reduction in power or separation at the toll), then follow the strategy for loss of safety critical information via V2V as defined by the functional safety concept.
Rational	Toll gates are not the same throughout EU. Even automated toll gates in some countries (e.g. Italy & Spain) have gates that separate vehicles until the tele-tag is read and cleared. This would interrupt the platoon. Not all toll gates have V2I communication to automate the tolling process. If zone policies information is available (via v2I or maps), then the platoon shall follow the instructions of reducing radio power, reducing speed, maintaining min gap... If no information is available, then it shall continue in the previous state. Any driver can reduce speed, steer or leave the platoon at will.

3.1.4. Approaching a construction zone

Platoon is approaching a construction zone.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon approaches a construction zone
Consequence	The platoon will require to reduce speed or change lanes or both
Hazard	Lane change or braking by the leading truck without prior intimation might leave the following trucks prone to accident

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents involving trucks in construction zones can result in life threatening injuries, especially when people are working on the construction site.

Controllability (C0 – C3)	C3
Controllability Rational	Even if the lead truck can detect the situation and react (for e.g. by steering), the rest of the platoon will not be able to control the situation if not informed about it in advance.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall not be automated. - The existing function shall not be modified for this situation: • The leading vehicle shall reduce speed as per zonal requirements. • If the forward vehicle brakes, then the platoon will brake automatically. • If the forward vehicle steers, then each driver is responsible to react appropriately (lateral control is manual for Level A). No driver has the right to disengage the entire platoon. Lead driver or any driver can leave the platoon at will.
Rational	The reactions to situations encountered in construction zones vary in complexity from simply reducing speed to complex ones like changing lanes, detecting cones, avoiding obstacles… Therefore, a combination of both longitudinal and lateral control is required. This cannot be automated for platooning Level A. The function will be left as it is. If the lead vehicle reduces speed or brakes, then the entire platoon reacts accordingly. If steering intervention is required, then as per Level A definition, each driver is responsible for their trucks lateral control. No warning/stay alert buttons to make the driver aware of the special zone will be introduced in the trucks as the implications of this addition are not clear. This will be analysed after running tests and having feedback from the drivers. The lead truck driver will not have any extra responsibilities of the platoon. Additional risk when passing through construction zones: When changing the lane often the central reservation (middle strip) has to be passed with waves in the ground (rumble strips). This can cause jitter in measurement values like yaw rate, lateral acceleration…. Exceeding a lateral acceleration threshold can lead in a follower emergency braking since this is evaluated as evasive manoeuvre.

3.1.5. Special zone policy

Platoon is approaching an area requiring special zone policy (bridges, city-limits).

Related use case in D2.2:	
Use Case ID	3.4.1
Title	Platoon gap adaptation because of I2V interaction.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then strategical layer issues a zone policy Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle received a zone policy from strategical layer and location determines the policy is applicable
Consequence	The zone policy has to be enforced in a safe way
Hazard	Zone policy might not be detected causing the system (platoon) to enter an unsafe state

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents involving trucks in special zones.
Controllability (C0 – C3)	C1
Controllability Rational	Since the lead truck driver is still responsible for both lateral and longitudinal control, the situation should be simply controllable.
Risk Value	4 (Medium Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • Each truck shall be able to identify zone policies applicable in its current route. • Each trucks' speed and time gap shall be automatically adjusted to meet the zone policies requirements.
Rational	Presently the zone policies are only communicated through road signs. If zone policing information is not available through V2I communication, then vehicles need to be equipped with advanced technologies for road sign recognition and dynamic maps for geo fencing.

	As per the level A definition the detection of all zone policies shall be automated. Driver shall not bear any responsibility to detect and react if they involve longitudinal control. Each vehicle shall implement mechanisms to detect zone policies (V2I, cameras, maps, etc...) All road policies are not limited to speed limits. E.g. Zone policy requesting maintaining a minimum distance between vehicle (e.g. inside tunnels) or zone policies requesting to turn ON head lights. The project prefers the detection of zone policies to be automated by the infrastructure (V2I). This implies that the infrastructure will have a role/responsibility in safety. Alternatively, each vehicle shall implement on-board systems to detect zone policies automatically. The idea to communicate the information if any truck detects zone policies was discussed, but since there might be legal implications and problems if different messages are received from different trucks! So, each truck is responsible for its own decision. For the demo, each driver will be responsible to detect and follow the rules independently.

3.1.6. Special zone policy not appropriate for current situation

Platoon receives a zone policy instruction not appropriate for the current situation.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then strategical layer issues a zone policy Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle received a zone policy from strategical layer and location determines the policy is applicable, but the request is not safe for current traffic / situation
Consequence	The zone policy has to be enforced but it must be sure that it is valid and not a risk
Hazard	zone policy might be wrong or unsafe for the current traffic situation (e.g. a speed limit of 30 kph on a highway with few cars)

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents involving trucks in special zones.
Controllability (C0 – C3)	C2

Controllability Rational	Having wrong zone policy information that is unsafe for the current traffic situation can be dangerous, but since the lead driver's tasks are not automated, the situation is normally controllable.
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	Not part of SOTIF, will be analysed for functional safety.
Rational	The information coming from the infrastructure is wrong. This should be in the scope of functional safety, as there is a malfunction in the implementation of the infrastructure's side. Consequently, the infrastructure shall also meet safety requirements with a safety integrity level.

3.1.7. Unexpected obstacle in the lane

Platoon encounters an unexpected obstacle in the lane

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon encounters an unexpected obstacle on the lane
Consequence	The platoon will have to take evasive manoeuvre to avoid the obstacle
Hazard	Lane change or braking by the leading truck without notifying the following trucks prior intimation might leave the following trucks prone to accident

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents involving a platoon colliding with an obstacle on the road will result in life threatening injuries, especially if the obstacle is a hard item like boulders, wooden box (fallen from another vehicle), ...
Controllability (C0 – C3)	C3
Controllability Rational	Even if the lead truck can detect the situation and react (for e.g. by steering), the rest of the platoon will not be able to control the situation if obstacle is not visible until the last moment. The situation is especially critical in case the obstacle falls out from one of the vehicles in the platoon.
Risk Value	6 (High Risk)

<table>
<tr><th colspan="2">Counter Measures Definition:</th></tr>
<tr><td>Counter Measures</td><td>- This situation might arise within the ODD.

- The trucks will not detect obstacles in the lane but shall detect aggressive steering manoeuvre by the forward truck.

- The existing function shall be modified for this situation:

• Each truck shall transmit its steering information to the following trucks (Steering angle, yaw rate, …)
• If the forward truck performs an aggressive steering manoeuvre, then the following truck shall perform an emergency braking manoeuvre
• If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode.
• Once overridden, the function shall wait for resume input from the driver to restart platooning.</td></tr>
<tr><td>Rational</td><td>How will making ADAS functions mandatory for the lead vehicle effect the situation?
• Non-metallic obstacles like boxes, boulders, animals... cannot be detected by current ADAS systems. So, making ADAS functions like ACC mandatory will not cover all situations.

How will transmitting ADAS warnings to the following vehicles effect the situation?
• Transmission of automated warnings to the following truck might not help either as the information to be transmitted is not clear (ADAS warnings?) nor is the required reaction in each case (steer? brake? increase time gap…)

Can we put any steering restrictions on the lead truck driver? E.g. brake if possible, instead of steering?
• No restrictions can be put on the lead truck driver (e.g. no sudden steering, always brake to avoid collision, …) as they cannot be enforced in a practical way.

The best solution for Level A:
1. If the forward vehicle brakes to avoid the obstacle, then the following trucks will brake in any case (longitudinal control is automated).
2. If the forward vehicle steers aggressively (detected based on yaw rate or steering speed) then the following vehicle shall apply emergency braking (> 4 m/s2) automatically.
3. If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode.</td></tr>
</table>

	4. Once overridden, the function shall wait for resume input from the driver to restart platooning. The following truck drivers remain responsible for the steering.

3.1.8. Unexpected object/vehicle on the road shoulder

Platoon encounters an unexpected object/vehicle on the road shoulder

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon approaches an unexpected object closely parked/situated near the edge of the lane
Consequence	The platoon will have to take evasive steering manoeuvre to avoid driving very close to the obstacle
Hazard	The following vehicles will not be prepared for the steering manoeuvre due to lack of anticipation

Risk Evaluation:	
Severity (S0 – S3)	S2
Severity Rational	Since the obstacle is on the road shoulder and not completely in the lane, the probability of having life threatening injuries is lower compared to the item being in the lane.
Controllability (C0 – C3)	C2
Controllability Rational	Since in level A platooning, the lateral motion of the trucks is controlled by the drivers, the situation is normally controllable.
Risk Value	4 (Medium Risk)

Counter Measures Definition:	
Counter Measures	- This situation might arise within the ODD. - The trucks will not detect obstacles in the lane but shall detect aggressive steering manoeuvre by the forward truck. - The existing function shall be modified for this situation: • Each truck shall transmit its steering information to the following trucks (Steering angle, yaw rate, …) • If the forward truck performs an aggressive steering manoeuvre, then the following truck shall perform an emergency braking manoeuvre

	• If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode. • Once overridden, the function shall wait for resume input from the driver to restart platooning.
Rational	How will making ADAS functions mandatory for the lead vehicle effect the situation? Non-metallic obstacles like boxes, boulders, animals... cannot be detected by current ADAS systems. So, making ADAS functions like ACC mandatory will not cover all situations. How will transmitting ADAS warnings to the following vehicles effect the situation? Transmission of automated warnings to the following truck might not help either as the information to be transmitted is not clear (ADAS warnings?) nor is the required reaction in each case (steer? brake? increase time gap…) Can we put any steering restrictions on the lead truck driver? E.g. brake if possible, instead of steering? No restrictions can be put on the lead truck driver (e.g. no sudden steering or brake to avoid collision and not steer etc...) as they cannot be enforced in a practical way. The best solution for Level A: 1. If the forward vehicle brakes to avoid the obstacle, then the following trucks will brake anyway (longitudinal control is automated). 2. If the forward vehicle steers aggressively (detected based on yaw rate or steering speed) then the following vehicle should apply emergency braking (> 4 m/s2) automatically. 3. If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode. 4. Once overridden, the function shall wait for resume input to restart platooning. The following truck drivers remain responsible for the steering.

3.1.9. Humans or big animals on the road

Platoon encounters humans or big animals on the road (Dynamic obstacles)

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then there are humans/animal on the road ahead

	Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle needs to be informed of or sense humans/animals on the road
Consequence	Ego vehicle has to consider unpredicted movement of humans/animals
Hazard	Ego truck risks hitting humans/animals

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Severe injuries in incidents involving animals usually happen in subsequent events when a vehicle runs off the road or collides with other road participants.
Controllability (C0 – C3)	C3
Controllability Rational	Even if the lead truck can detect the situation and react (for e.g. by steering), the rest of the platoon will not be able to control the situation if not informed about it in advance and the evasive manoeuvre is not braking
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation might arise within the ODD. - The trucks will not detect obstacles in the lane but shall detect aggressive steering manoeuvre by the forward truck. - The existing function shall be modified for this situation: • Each truck shall transmit its steering information to the following trucks (Steering angle, yaw rate, …) • If the forward truck performs an aggressive steering manoeuvre, then the following truck shall perform an emergency braking manoeuvre • If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode. • Once overridden, the function shall wait for resume input from the driver to restart platooning.
Rational	How will making ADAS functions mandatory for the lead vehicle effect the situation? Non-metallic obstacles like boxes, boulders, animals, etc cannot be detected by current ADAS systems. So, making ADAS functions like ACC mandatory will not cover all situations. AEB VRU systems do not work at highway speeds

	How will transmitting ADAS warnings to the following vehicles effect the situation? Transmission of automated warnings to the following truck might not help either as the information to be transmitted is not clear (ADAS warnings?) nor is the required reaction in each case (steer? brake? increase time gap…) Can we put any steering restrictions on the lead truck driver? E.g. brake if possible, instead of steering? No restrictions can be put on the lead truck driver (e.g. no sudden steering or brake to avoid collision and not steer etc...) as they cannot be enforced in a practical way. The best solution for Level A: 1. If the forward vehicle brakes to avoid the obstacle, then the following trucks will brake anyway (longitudinal control is automated). 2. If the forward vehicle steers aggressively (detected based on yaw rate or steering speed) then the following vehicle should apply emergency braking (> 4 m/s2) automatically. 3. If any driver overrides the braking (through accelerator pedal input), then the braking shall be disabled, and the function shall enter standby mode. 4. Once overridden, the function shall wait for resume input to restart platooning. The following truck drivers remain responsible for the steering.

3.1.10. Driving on a curved lane

Platoon is approaching curvy sections of a highway

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon approaches a curved lane (max highway limit)
Consequence	Speeds of individual trucks need to be adjusted for stability based on their loads.
Hazard	Underestimating the curvature can make heavier trucks unstable.

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway due to improper steering manoeuvre by the truck drivers can lead to life threatening injuries.

Controllability (C0 – C3)	C1
Controllability Rational	At 80 km/h with a time gap of 0.8 seconds, the field of view of the following truck drivers blocked by the forward truck is around 8 degrees (assuming width of the truck: 2.4 meters). Since the human field of view in the horizontal arc is around 210 degrees, it can be assumed that the situation is simply controllable.
Risk Value	4 (medium)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • The function shall automatically detect conditions that affect longitudinal control like road curvature, road mu, truck loads, … • Each truck shall automatically adjust its speed and time-gap to a safe level. • Driver shall be informed through HMI about the reduction in performance. • The platooning will continue as long as communication is maintained between trucks.
Rational	Since for Level A, the longitudinal control of the following trucks is automated, the platooning function shall be able to detect conditions that affect safety like the road curvature, mu, truck loads, gradient… and automatically adjust the speeds and time gap of its truck to a safe level.

3.1.11. Heavy traffic

Platoon is approaching heavy traffic with continuously changing conditions

Related use case in D2.2:	
Use Case ID	3.2.1
Title	Follow to stop Main Flow

Scenario Description:	
Operational Situation	Situation: traffic on motorway gets denser and speeds will decrease Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle needs to adjust speed. Higher probability of cut-ins, dissolving and even standstill
Consequence	The situation around the truck gets more complex

Hazard	Ego truck systems might not be capable of building an adequate picture of the environment

Risk Evaluation:	
Severity (S0 – S3)	S1
Severity Rational	Since all the traffic participants are at low speed and no pedestrians are assumed to be present on the highway, collisions might result in light to moderate injuries.
Controllability (C0 – C3)	C1
Controllability Rational	Since the driver a more attentive in heavy traffic conditions and the vehicle are at low speed, the situation is easily controllable by majority of the drivers
Risk Value	2 (Low Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall not be automated. - The existing function shall not be modified for this situation: • The following vehicles shall adjust the speed as per the forward vehicle's behaviour. • All the truck drivers are still responsible for lateral control. • Cut-ins are handled as defined for any other situation.
Rational	Adjusting the speed (longitudinal control) of the platoon to the traffic conditions is already automated for level A. Even cut-ins are handled by the same longitudinal control function. If a steering intervention is required, as per level A definition each truck driver shall handle it by himself. Giving way to other vehicles will make it difficult for the platoon to maintain cohesion later. So, increasing the time-gap in an automated way is not recommended. Any truck driver can leave the platoon if he thinks the conditions are unstable for the platooning function.

3.1.12. Emergency Vehicle

Platoon encounters an emergency vehicle.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon when an emergency vehicle is approaching (any direction) Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle needs to detect emergency vehicles
Consequence	driver has to be informed early in order to resolve the situation
Hazard	driver might not react, and ego vehicle might block the emergency vehicle

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Since emergency vehicles in critical situations need not follow the traffic laws completely, they might result in collision with the platoon if the platoon drivers are not returned control of the trucks immediately. E.g. Ambulance driving in the opposite lane, on the hard shoulder, cross solid white lines, etc
Controllability (C0 – C3)	C2
Controllability Rational	If the following truck drivers are attentive and the sirens are clearly audible (not mandatory), then the situation is normally controllable. If not, reacting to an emergency vehicle that is breaking traffic laws is difficult to control as the driver has less than a second to analyse the situation and take an appropriate action.
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation might arise within the ODD. - Detection of the situation will not be automated. - The existing function shall not be modified for this situation: • If the forward vehicle brakes, then the platoon will brake automatically. • If the forward vehicle steers, then since lateral control is manual for Level A, each driver is responsible to react appropriately. • If any of the drivers decides to give way, they can act individually by steering or braking
Rational	Since for the Level A platooning, the platoon will remain in the slowest lane, it should not come in the way of the emergency vehicles.

	And since steering is not automated, assistance in Level A can only be provided through longitudinal control, which will already give way if cut-ins are detected or braking is required. If any of the drivers decide to give way on their own, they can act individually by steering or braking.

3.1.13. Adverse weather conditions

Platoon encounters adverse weather conditions resulting in low mu and visibility.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon experiences adverse weather conditions including low mu and low visibility
Consequence	Trucks might find it difficult to maintain the time-gap safely
Hazard	Any unexpected change in situation might result in collision

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway in slippery and low visibility conditions can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Since the time gap between trucks is 0.8 seconds, there isn't enough time for the driver to react to a changing situation with lower braking performance.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • The function shall detect the road mu and visibility impeding weather conditions automatically (e.g. weather telematics, cameras...) • Each truck shall continuously communicate its current brake performance (due to changing conditions) to the following vehicle • Each truck shall adjust its speed and time-gap to a safe level.

	• Drivers shall be informed through HMI about the conditions and reduced performance. • The platooning will continue as long as communication is maintained between trucks. • Any driver in the platoon can decide to leave independently.
Rational	Since for Level A, the longitudinal control of the following trucks is automated, the platooning function shall be able to detect weather conditions that impact platoon safety within the ODD without any driver input. The function shall automatically decide the strategy (increase the time gap, reduce speeds or leave the platoon entirely) based on the conditions. Platooning shall not continue in unsafe conditions.

3.1.14. Braking on slippery roads

Platoon requires braking (not full braking) under slippery road conditions (e.g. split mu).

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Braking event within the platoon
Consequence	Trucks need to brake in slippery conditions
Hazard	Different brake performances can lead to an accident

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway in slippery conditions can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Braking situations in slippery conditions in combination with low time gap between vehicles and different brake performances between vehicles can be difficult to control
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	Not applicable.
Rational	Same situation as above use case (platooning in adverse weather conditions). No special treatment required.

3.1.15. Platooning on a gradient

Platoon encounters roads with steep slopes (Maximum gradient allowed on a highway).

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Platoon encounters routes with a steep slope
Consequence	Trucks will find it difficult to maintain the time-gap safely due to newer requirements on powertrain and braking
Hazard	Any unexpected change in situation might result in collision

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C2
Controllability Rational	Since the time gap between trucks is 0.8 seconds, there isn't enough time for the driver to react to a changing situation. But the drivers are more attentive on slopes and might react quickly to changing conditions.
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • The function shall detect the road gradient automatically (e.g. using maps, sensors...) • Each truck shall adjust its speed, acceleration and time-gap to a safe level. • Driver shall be informed through HMI about the reduction in performance. • The platooning will continue as long as the communication is maintained between trucks.
Rational	Since for Level A platooning the longitudinal control is automated for the following trucks, the system shall be able to detect the road gradient and

	adjust the speeds of individual trucks to a safer value based on their loads, brake performance, powertrain performance, etc. This shall apply for both driving up-hill and down-hill.

3.1.16. Driving in Tunnels

Platoon approaches a tunnel while steady state platooning.

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Entering a tunnel
Consequence	Trucks are driving with a reduced time-gap in a closed environment
Hazard	Any unexpected change in situation has higher risk of collision

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Any accident inside a tunnel can be considered life threatening due to issues arising with fire risk, low visibility (if fire or smoke are involved), accessibility (for the rescue team) and situation of panic caused by difficulty in escaping.
Controllability (C0 – C3)	C3
Controllability Rational	The situation is normally controllable in steady state driving, but if a braking situation is encountered inside tunnel along with low visibility, then the situation is difficult to control.
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • The function shall detect the approaching tunnels automatically (e.g. using maps) • Each truck shall adjust its speed, acceleration and time-gap to a safe level as per regulatory requirements. • Driver shall be informed through HMI about the approaching tunnel. • The platooning will continue as long as communication is maintained between trucks.

	• Joining shall not be allowed inside a tunnel? Will be confirmed once the specifications are clear. Joining will not be allowed if GPS is required for joining. - This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • Each truck shall be able to identify zone policies applicable in its current route. • Each trucks' speed and time gap shall be automatically adjusted to meet the zone policies requirements.
Rational	Since for Level A platooning the longitudinal control is automated for the following trucks, the function shall be able to detect special zone policy requirements if applicable for the tunnels and adjust the platoon parameters to comply with legal requirements. Same case as special zone policies (3.1.5). If no special zone requirements are available, then the trucks shall continue platooning in the current state. Joining might not be allowed inside a tunnel if the loss of GPS signal impacts joining. This case will be analysed once the specifications are available. Other questions to be analysed once the specifications are available: How do you decrease the gap after cut-ins inside tunnels? How do you know if the new vehicle in front of you is not another cut-in vehicle?

3.2. Emergency Braking

3.2.1. Emergency braking/Full braking in a platoon

Platoon encounters a situation requiring full braking.

Related use case in D2.2:	
Use Case ID	3.3
Title	Emergency Braking

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr

	Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) and weather conditions System Status: Any platoon driving mode Vehicle status: Under all vehicle loads
Triggering Event	Any forward vehicle performs full Emergency Braking (deceleration > 6 m/s2)
Consequence	All the following vehicles need to brake immediately to avoid collision
Hazard	Risk of forward collision due to different brake performance of the trucks in the platoon

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents caused by emergency braking on a highway can lead to severe life-threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Since the time gap between trucks is 0.8 seconds, there isn't enough time for the driver to react in a safe manner.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation might arise within the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • The function shall automatically detect an emergency braking situation without any driver intervention. • Any truck that experiences emergency braking (manual braking, or AEB) shall communicate the event via V2V to the following trucks • Each truck shall brake independently to avoid collision to the forward vehicle. • If emergency braking event is active until the truck comes to a complete stop, each truck driver shall use the resume button to re-join the platoon (to avoid trucks moving until the drivers are ready). • If emergency braking event becomes inactive while the trucks are still moving, then the function shall stop braking but shall not initiate acceleration/longitudinal control until a resume input is received from the driver. • If the legal safe gap is reached before receiving the resume request, then the control shall be handed over to the driver. • Driver shall be informed through HMI about the emergency braking event.

Rational	Since for Level A, the longitudinal control of the following trucks is automated, the function shall be able to detect and react to any braking situation (including full braking) autonomously. Based on the brake performances (of the ego truck and the forward truck) each truck shall calculate the required deceleration to maintain a safe distance to the forward truck. If emergency braking event is active until the truck comes to a complete stop, each truck driver shall use the resume button to re-join the platoon (to avoid trucks moving until the drivers are ready). If emergency braking event becomes inactive while the trucks are still moving, then the function shall stop braking but shall not initiate acceleration unless a resume input is received from the driver. If the legal safe gap is reached before receiving the resume request, then the control shall be handed over to the driver. The driver can press the resume button to reactive longitudinal control if he sees that the situation is not present anymore. If the forward trucks deceleration is below the emergency braking limit, then the ego truck shall resume longitudinal control at the end of the braking event. Imp requirement: Driver needs to clearly know who is in control (system or the driver?) Note: How to handle FCW only or HCW? Is part of AEBS cascade, but from deceleration perspective no emergency braking.

3.3. Cut-in

3.3.1. External vehicle enters the platoon

Platoon encounters a cut-in by an external vehicle.

Related use case in D2.2:	
Use Case ID	3.4.2
Title	Cut-in handling within the platoon. Cut in vehicle remains for a long period (as opposed to cut-through).

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr

	Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) and weather conditions System Status: Any platoon driving mode External vehicle conditions: At constant or Decelerating (worst case)
Triggering Event	An external vehicle enters the platoon (performs a cut-in)
Consequence	All the following vehicles need to brake immediately to avoid collision
Hazard	Risk of collision (within the platoon or with the external vehicle) due to sudden braking requirement

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents between cut-in vehicles and a platoon on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Since the time gap between trucks is 0.8 seconds, there isn't enough time for the driver to react in a safe manner.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Detection of the situation shall be automated. - The existing function shall be modified for this situation: • Cut-ins shall be automatically detected by the ego truck. • The ego truck shall automatically adjust the gap to the reach legally required safe distance to the cut-in vehicle. • Once the intruder leaves, the ego vehicle shall automatically reduce the time gap to the forward truck.
Rational	Since for Level A, the longitudinal control of the following trucks is automated, cut-ins shall be detected and handled autonomously. Even after legal safe gap is reached to the intruder, the platoon function shall maintain longitudinal control. The function shall also detect the leaving intruder and decrease the gap autonomously. If more intruders enter the gap between the ego truck and the external vehicle (first intruder), then continue increasing the distance as long as communication is active with the forward truck. Then leave the platoon as per the nominal functional behaviour. Note: Can close cut-ins be detected by the current radar technology?

3.3.2. Multiple cut-ins

Platoon encounters multiple cut-ins by external vehicles (e.g. crowded highway entry ramp)

Scenario Description:	
Operational Situation	Situation: Normal driving on a highway at 80 km/hr Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) and weather conditions System Status: Any platoon driving mode External vehicle conditions: At constant or Decelerating (worst case)
Triggering Event	Crowded roads leading to multiple cut-ins near a highway entry/exit ramp
Consequence	Multiple vehicles enter as intruders in the platoon
Hazard	Risk of collision (within the platoon or with the external vehicle) due to complex driving situation

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents between cut-in vehicles and a platoon on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Since the time gap between trucks is 0.8 seconds, there are multiple intruders in the platoon, the situation is difficult to control.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. Same reaction as above use case (3.3.1), each truck shall be responsible to safely manage the cut-ins in front of it. No special functions will be implemented to handle multiple cut-ins.
Rational	Same reaction as above use case (3.3.1), each truck should be responsible to safely manage the cut-ins in front of it. The vehicles cutting-in behind the ego vehicle shall be handled by the truck following it. No special functions will be implemented to handle multiple cut-ins. Infrastructure (V2I) communication can be used to indicate busy highway entries and exits. This information can be used to increase the time gap between trucks.

3.4. Platooning function specific or internal factors

3.4.1. Increase time gap in steady state

Platoon needs to increase time-gap (e.g. due to zone policies).

Related use case in D2.2:	
Use Case ID	3.4.1
Title	Platoon gap adaptation because of I2V interaction.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon but with increased time gap Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Platooning in steady state mode
Triggering Event	Ego vehicle (tactical or strategical layer) issues an increase time gap command
Consequence	Distance between ego and immediate front truck will be increased
Hazard	Time gap increase might lead to unintended platoon oscillation

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Since the time gap between the trucks is low, instability with the platoon can lead to collisions which can lead to life threatening injuries.
Controllability (C0 – C3)	C2
Controllability Rational	If the instability is introduced quickly, there might not be enough time for take control of the situation. Moreover, since the system is trying to increase the time-gap, it can be assumed that the time-gap will not fall below 0.8 seconds. So, the situation should be normally controllable.
Risk Value	5 (High risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Reaction to this situation shall be automated. - The existing function shall be modified for this situation: • Each vehicle shall transmit the "increase time gap" request to the following vehicles. • The "increase time gap" request shall be sent at least 2 kms (TBC) prior to the target zone (e.g. tunnels, bridges, zone policies...)

	• Each vehicle shall automatically increase the time-gap to the forward vehicle upon receiving request (no driver intervention required). • Each truck can independently adjust its speed and acceleration to meet its efficiency targets (only coasting or coasting + braking). • During the transition, the ego vehicle's speed shall not deviate from that of the lead vehicle by more than 10 km/h (already present in D 2.4) • Driver shall be informed through HMI about the increasing time-gap.
Rational	Each truck can independently increase its gap to the forward vehicle in a way it determines to be most efficient. A limit shall be put on the maximum difference between the platoon's set speed and the ego vehicle's speed during transitioning. E.g. 10 km/h. Time-gap increase request needs to come early (e.g. 5 minutes before the applicable zone) to increase the gap safely before reaching the applicable point. The time depends on how much you want to increase the time gap, plus the speed of the platoon (can be checked through simulation)

3.4.2. Decrease time gap in steady state

Platoon needs to decrease the time gap (e.g. At the end of zone policies).

Related use case in D2.2:	
Use Case ID	3.4.1
Title	Platoon gap adaptation because of I2V interaction.

Scenario Description:	
Operational Situation	Situation: Any situation which required a higher time-gap is no longer present Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Platooning in steady state mode
Triggering Event	Ego vehicle (tactical or strategical layer) issues a decrease time gap command
Consequence	Distance between ego and immediate front truck will be decreased
Hazard	Time gap decrease might lead to unintended platoon oscillation

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Since the time gap between the trucks is low, instability with the platoon can lead to collisions which can lead to life threatening injuries.

Controllability (C0 – C3)	C3
Controllability Rational	Since the instability in the system is induced gradually, there is usually enough time for the drivers to recognise the issue and take control of their vehicles. But since the system is trying to decrease the time-gap, contradictory actions by different platoon members might lead to the time-gap falling below 0.8 seconds. So, the situation could be difficult to control.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall be part of the ODD. - Reaction to this situation shall be automated. - The existing function shall be modified for this situation: • Each vehicle shall transmit the "decrease time-gap" request to the following vehicles. • Each vehicle shall automatically decrease the time-gap to the forward vehicle upon receiving request (no driver intervention required). • Each truck shall independently adjust its speed and acceleration in accordance with its efficiency targets (low acceleration, medium acceleration ...). • During the transition, the time-gap to the forward vehicle shall not fall below 0.8 seconds or the current safety time-gap calculated by the ego truck as per it's braking performance, whichever is higher. • Speeds of the trucks shall not increase above the set legal limit for platooning. • Driver shall be informed through HMI about the decreasing time-gap.
Rational	Each truck can independently decrease its gap to the forward vehicle in a way it determines to be most efficient. While decreasing the distance between the trucks, the time-gap between the ego vehicle and the forward vehicle shall not fall below 0.8 seconds or the current safe time-gap calculated by the ego truck as per it's braking performance, whichever is the largest. Speeds of the trucks shall not increase above the set legal limit for platooning.

3.4.3. Increase the speed of the platoon

Platoon has to increase the speed from medium speed (50 km/h) to high (90 km/h).

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon but at lower speeds Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Platooning in steady state mode
Triggering Event	Platoon leader request to increase the speed of the platoon from medium (50 kmph) to high (90 Kmph)
Consequence	All the trucks will start accelerating to reach the target speed
Hazard	Unsynchronised speed increase might lead to unintended platoon oscillation

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Since the time gap between the trucks is low, instability with the platoon can lead to collisions which can lead to life threatening injuries.
Controllability (C0 – C3)	C0
Controllability Rational	Since the lead truck is increasing the speed and the remaining trucks are maintaining the time-gap, the situation should be controllable in general
Risk Value	0 (No risk)

Counter Measures Definition:	
Counter Measures	No special SOTIF counter measures are required for this situation.
Rational	Not a SOTIF scenario, as this is part of the nominal function. Same case as steady state platooning where each truck tries to maintain the safety time-gap and also keep up with the lead truck's speed. Only the lead vehicle is increasing the speed, everybody else is maintaining the time-gap.

3.4.4. Joining from behind

Ego truck is joining a platoon from behind when an external vehicle is closely following the forward truck/platoon

Related use case in D2.2:	
Use Case ID	2.1
Title	Join from behind by single vehicle

The following situations are also covered in the current case:

- Driving too close to the wrong vehicle.
- Connecting to the wrong platoon.

Scenario Description:	
Operational Situation	Situation: Normal driving situation during engaging phase Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Platooning in steady state mode
Triggering Event	Ego vehicle starts the automated joining procedure when a small vehicle is closely following the forward vehicle
Consequence	Since the accuracy of the GPS is around 5 to 10 meters, the ego vehicle might not detect the external vehicle and try to close the gap to the forward truck
Hazard	Closing the gap to the external vehicle to below 0.8 seconds might lead to collision

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Since the time gap between the trucks is low, instability with the platoon can lead to collisions which can lead to life threatening injuries.
Controllability (C0 – C3)	C1
Controllability Rational	Since the drivers are more attentive during the engaging phase, they are more likely to take control as soon as a risk is detected. The situation is simply controllable.
Risk Value	4 (Medium Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - Reaction to this situation shall be automated. - The existing function shall be modified for this situation: • The ego truck shall confirm that it is communicating to the correct platoon. • The ego truck shall confirm that it is in the correct lane before starting the joining manoeuvre. (indirectly solved by the first point) • The function shall detect the presence of any intruders between the ego vehicle and the platoon. • The joining procedure shall not start if an intruder is present between ego vehicle and the platoon (longitudinal control remains manual). • Driver shall be informed through HMI about the start of the joining procedure.

Rational	The ego truck should confirm that it is in the correct lane and joining the correct platoon. It should not join if there is an intruder present behind the platoon. Comments: How do you know that you are closing the gap to the right vehicle?

3.4.5. Accident within the platoon

One of the trucks have an accident within the platoon.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then steady state is no longer true Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	One of the trucks in the platoon has an accident
Consequence	All the following vehicles are put at risk due to lower time gaps.
Hazard	Risk of forward collision due to lack of system control

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Accidents at high speed will usually require maximum deceleration and/or extreme steering manoeuvre to avoid impact.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - Reaction to this situation shall be automated. - The existing function shall be modified for this situation: - Each truck (including the leading truck) shall utilize ADAS functions that can predict and react to forward collisions. • Any truck that detects a situation of imminent collision shall communicate it to the following vehicles. • Any truck that has an accident shall communicate it to the following vehicles. • On receiving "imminent collision" or "collision" message, the following trucks shall apply full braking.

	• Driver shall be informed through HMI about the emergency braking situation due to collision of the forward vehicle.
Rational	Deceleration required to avoid collision (in an accident situation) with the forward truck can be extremely high in a platoon (due to lower time gaps). Truck that have an accident should inform it immediately to the following trucks. Trucks should be fitted with ADAS system to alert the following trucks of imminent collision. With this, the risk of losing communication after collision is avoided. This would also give the following trucks more time to react. Reaction: Full braking from the following trucks as the forward truck conditions are unpredictable. Best to apply full braking to avoid collision. **Accident:** An accident or traffic collision, occurs when a vehicle strikes or collides another vehicle, a stationary object, a pedestrian, or an animal....

3.5. Driver Behaviour and Misuse

3.5.1. Transfer of driving task to the driver

Platoon function needs to transfer a task back to the driver.

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then the system needs immediate driver input Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	ego vehicle needs immediate driver input in order to resolve a situation that the system itself cannot handle due to insufficient information
Consequence	Driver has to be informed immediately and input has to be given quickly
Hazard	Driver might not understand the situation and give inadequate (or none) input

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3

Controllability Rational	Any steering or braking action requested to the drivers without increasing the time-gap to a safer level is not controllable in general.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation shall not be allowed within the ODD. - The function shall not return the longitudinal control task to the driver until the legal safe gap is established to the forward vehicle. Driver is still responsible for lateral control, so any emergency situation that requires a steering input will continue to be under the driver's responsibility.
Rational	For level A platooning, the longitudinal control for the following vehicle falls under the responsibility of the system. Therefore, the system shall not return this task to the driver while operating within the ODD. Handover of longitudinal control shall only be allowed after the legal safe gap is reached to the forward vehicle. The Handover procedure shall be defined by the HMI team. This shall include investigating the best type of warnings (audio, visual, haptic…) for handover and the handover confirmation procedure (e.g. acceptance feedback like input/acknowledgement from the driver). Driver is still responsible for lateral control, so any emergency situation that requires a steering input will continue to be under the driver's responsibility.

3.5.2. Driver forcing all control back immediately

Platoon encounters a situation where a driver in the platoon is forcing all control back immediately

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then the driver (PIC) will override the systems commands Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	As an SAE level 3 or lower system the driver is the "pilot in command" and might override at any time
Consequence	Driver's (PIC) command might contradict the systems command or disrupt the systems plan of action
Hazard	Driver might take over command without situation awareness and hence bring the system into an unsafe state

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	If the driver accelerates for some reason, a collision will be unavoidable.
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - Reaction to this situation shall be the following: • Steering manoeuvre resulting in lane change shall initiate platoon leave procedure for the ego vehicle. • Acceleration by the driver that results in time gap falling below the safety limit shall initiate platoon leave procedure for the ego vehicle. • Manual braking shall enter the platoon function into standby mode: longitudinal control shall be disabled. • In standby mode the driver shall provide resume command to reactivate longitudinal control.
Rational	Lateral control: Since lateral control is not automated, drivers can steer at any time. If the steering results in lane change, then platoon leave procedure shall be initiated for the ego vehicle. Longitudinal control: If the driver accelerates and reduces the time gap below the safe limit, platoon leave procedure shall be initiated for the ego truck. Trucks behind the ego vehicle will automatically increase the time gap to the accelerating truck (the ego truck is treated as an intruder (similar to cut-in). If the driver brakes manually, then he/she is indicating that they want to handle the situation/take control. Hence longitudinal control shall be disable (only for the ego vehicle). The driver can reactive the longitudinal control by pressing the resume button.

3.5.3. Uninformed lane change performed by the lead truck driver

The lead driver of the platoon performs an uninformed lane change

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then the system needs immediate driver input Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Not due to an obstacle, but gentle steering lane change!!
Consequence	Following drivers might not realise the change in time and collide with the obstacle
Hazard	Following vehicle might not take appropriate action to continue safely

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Since the visibility of the obstacles on the current lane is only visible to the lead vehicle driver, the following vehicle drivers will not have enough time to detect the problem and take the appropriate action (steer or brake)
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - Reaction to this situation shall be the following: • Non-aggressive lane change by the lead truck shall initiate platoon leave procedure. • All the following trucks shall detect if they are still following their assigned forward truck. • In the absence of the lead truck, the lead role shall be transferred to the next following truck in the platoon. • Once the handover is initiated, the platoon function in the new lead truck shall stop accelerating (start coasting). • The braking function of the new leader shall be maintained until the lead driver takes control of driving. • The platoon function shall reconfigure the platoon layout to reflect the current truck positions and roles.
Rational	Non-aggressive lane change by the platoon leader shall initiate leave procedure for the ego/lead truck. The following trucks shall also detect if they are still following the forward truck. Note: Aggressive steering by any truck in the platoon shall result in emergency braking of the following trucks (Refer to use case 3.1.7).

	In the absence of lead truck, the role of the platoon leader shall be transferred to the next following truck. This shall result in handing over the longitudinal control task to the driver of the new lead truck. Once the handover is initiated, the platoon function of the new leader shall stop accelerating and start coasting for the driver to take manual control. Braking function shall still be active for safety. If the new leader does not take control of driving, then the truck shall continue coasting and come to a complete stop. The Handover procedure shall be defined by the HMI team. This shall include investigating the best type of warnings (audio, visual, haptic…) for handover and the handover confirmation procedure (e.g. acceptance feedback like input/acknowledgement from the driver). The function shall reconfigure the platoon layout reflecting the current truck positions and roles. Note: The function detecting lane changes/aggressive steering shall be robust enough to filter out vibrations from road conditions like rumble strips, etc...

3.5.4. Uninformed lane change performed by a following driver

Any of the following drivers (other than the trailing truck) performs an uninformed lane change

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then the driver (PIC) will override the systems commands Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle drivers starts changing lane without intimating the other members of the platoon
Consequence	The following trucks must adapt to the situation safely
Hazard	Following vehicle might not take appropriate action to continue safely

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents between trucks in a platoon on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C2

Controllability Rational	Since the longitudinal control is still in automated mode, unintended steering by any driver should not result in collision between the trucks in the platoon. But if this change is lane is not detected, action of the exited truck may affect the platoon even if it is not in the same lane. Moreover, since the time-gap between trucks is below the legal limit, driver intervention might not be safe.
Risk Value	5 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - Reaction to this situation shall be the following: • Non-aggressive lane change by the any truck shall initiate platoon leave procedure for the leaving truck. • All the following trucks shall detect if they are still following their assigned forward truck. • The following truck shall accelerate to close the gap to the new forward truck. • The platoon function shall reconfigure the platoon layout to reflect the current truck positions and roles.
Rational	Non-aggressive lane change by any of the trucks in the platoon shall initiate leave procedure for the ego truck (leaving truck). The following trucks shall also detect if they are still following the forward truck. Note: Aggressive steering by any truck in the platoon shall result in emergency braking of the following trucks (Refer to use case 3.1.7). Other members of the platoon: The following truck shall close the time gap to the new forward vehicle and continue platooning. The platoon function shall reconfigure the platoon layout to reflect the current truck positions and roles. Note: The platoon shall continue even if the vehicles in the faster lane (left lane) are slower than the platoon. This applies to the truck that recently left the platoon or any other vehicles on the left lane. Note: The function detecting lane changes/aggressive steering shall be robust enough to filter out vibrations from road conditions like rumble strips, etc...

3.6. Communication

3.6.1. Wireless channel reception problems

Ego vehicle experiences wireless channel reception problems

Related use case in D2.2:	
Use Case ID	3.4.4
Title	Platoon time gap adaptation because of system status (e.g. packet loss)

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then wireless channel encounters problems (noise) Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	ego vehicle needs to detect wireless channel problems early
Consequence	tactical layer of ego vehicle must be informed of the degradation of the wireless channel
Hazard	risk of forward collision due to sensor malfunction

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Loss of safety critical information (e.g. deceleration) from the forward vehicle can result in delays in braking and collision with the forward vehicle.
Risk Value	6 (High)

Counter Measures Definition:	
Counter Measures	Not applicable.
Rational	If Ego truck detects that safety relevant information is missing, irrespective of the cause (system failure or environmental conditions effecting Wi-Fi), the strategies for missing messages defined in the functional safety concept shall be followed. No separate SOTIF requirements are required.

3.6.2. Wireless channel transmission problems

Ego vehicle experiences wireless channel transmission problems

Related use case in D2.2:	
Use Case ID	3.4.4
Title	Platoon time gap adaptation because of system status (e.g. packet loss)

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then wireless channel encounters problems (noise) Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	ego vehicle needs to detect wireless channel problems early
Consequence	tactical layer of ego vehicle has to be informed of the degradation of the wireless channel
Hazard	risk of forward collision due to sensor malfunction

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Loss of safety critical information (e.g. deceleration) from the forward vehicle can result in delays in braking and collision with the forward vehicle.
Risk Value	6 (High)

Counter Measures Definition:	
Counter Measures	Not applicable.
Rational	If Ego truck detects that safety relevant information is missing, irrespective of the cause (system failure or environmental conditions effecting Wi-Fi), the strategies for missing messages defined in the functional safety concept shall be followed. No separate SOTIF requirements are required.

3.7. Non-EE Malfunctions

3.7.1. Mechanical failures

Ego truck experiences system failure (tire blow-up, oil-leak...)

Scenario Description:	
Operational Situation	Situation: Normal driving in a platoon then the system detects an anomaly in its operation

	Environment: All conditions on a dedicated motorway/interstate (Autobahn, Autostrada...) System Status: Any platoon driving mode
Triggering Event	Ego vehicle needs to be able to detect any anomaly in operation and reports that early to the driver
Consequence	Driver has to be informed early and input has to be given quickly
Hazard	Driver might not understand the situation and give inadequate (or none) input

Risk Evaluation:	
Severity (S0 – S3)	S3
Severity Rational	Accidents on a highway can result in life threatening injuries.
Controllability (C0 – C3)	C3
Controllability Rational	Depending on the failure, it can be difficult to control
Risk Value	6 (High Risk)

Counter Measures Definition:	
Counter Measures	- This situation can arise within the ODD. - The reaction to this situation shall not be automated. Driver shall be responsible for detecting and responding to mechanical failures (tire blow-up, oil-leak...) in the ego truck.
Rational	Some malfunctions can be detected by E&E systems and other are usually detectable only by the drivers. (e.g. tyre blow-up, vibrations...). Detection of all the failures cannot be automated, therefore the longitudinal control cannot be fully automated. Can the system assist in some conditions? Malfunctions that require the vehicle to brake can be considered. The function can assist with braking in certain situations. Comments: In case of failures that are not detectable by EE systems, the driver is responsible to detect them and leave the platoon and react accordingly. Failures which result in wrong estimation of brake performance shall be analysed while defining the brake performance algorithm.

4. SOTIF SAFETY CONCEPT

This section contains SOTIF safety requirements which are derived from the hazard identification, risk evaluation and the counter measures defined in the previous section.

The current set of requirements constitute the first version of safety requirements for SOTIF and they shall be worked upon and modified as the project progresses.

This section does not specify requirements for the nominal function of the platoon.

4.1. Application Requirements

The following section contains requirements on the platooning function:

STF_REQ_001: Each truck shall be able to independently identify the zone policies applicable in its current route.

STF_REQ_002: Each truck shall independently (no co-ordinated instruction) adjust its speed and time gap (to the forward truck) to meet the zone policies requirements.

STF_REQ_003: Lane change manoeuvre shall initiate platoon leave procedure for the ego truck.

STF_REQ_004: Each following truck shall detect if it is still following its assigned forward truck in the platoon (to detect lane change by the forward truck).

STF_REQ_005: While platooning, absence of assigned forward truck shall transfer the lead role to the ego vehicle.

STF_REQ_006: Once the lead role is assigned to a following truck, the platooning function shall enter into standby mode until the driver takeover acknowledgement is received. (For standby mode refer to requirements: STF_REQ_026, STF_REQ_027 and STF_REQ_029).

STF_REQ_007: Each following truck shall be able to detect aggressive steering intervention (used to avoid obstacles) by the forward truck in the platoon.

STF_REQ_008: Each following truck shall apply emergency braking (deceleration > 4 m/s2) on detection of an aggressive steering intervention by the forward truck in the platoon.

STF_REQ_009: Each following truck shall be able to detect emergency braking manoeuvre by the forward truck in the platoon.

STF_REQ_0010: In an emergency braking event, each following truck shall brake independently (no co-ordinated effort) to avoid collision with the forward truck in the platoon.

STF_REQ_011: During an emergency braking intervention, if the emergency event is revoked (forward truck stops braking), the platooning function in the ego truck shall enter standby mode. (For standby mode refer to requirements: STF_REQ_026, STF_REQ_027 and STF_REQ_028).

STF_REQ_012: Each truck shall be able to detect environmental and road conditions that affect longitudinal control (like road curvature, road mu, truck loads, gradient…) and adjust its speed and time gap to the forward truck (in the platoon) to a safe level.

STF_REQ_013: While platooning, each following truck shall be able to detect external vehicles (intruders) entering the space between the ego and the forward truck in the platoon (detect cut-ins).

STF_REQ_014: In case of a cut-in event, the following truck shall increase the distance to reach legal safe gap (2 seconds time gap) to the intruder.

STF_REQ_015: Any "increase time gap" request in the platoon shall be issued at least 2 kms (1.5 kms @ 90 km/hr = 1 min) prior to reaching the target/applicable zone (e.g. tunnels, bridges, zone policies...)

STF_REQ_016: During any time gap transition (increase or decrease), the ego vehicle's speed shall not deviate from that of the platoon leader by more than 10 km/h.

STF_REQ_017: During any time gap transition (increase or decrease), the time gap to the forward truck (in the platoon) shall not fall below 0.8 seconds or the current safety time gap calculated by the ego truck as per it's braking performance, whichever is higher.

STF_REQ_018: The ego truck shall confirm that it is in the correct lane before starting the joining manoeuvre.

STF_REQ_019: Before joining a platoon, the ego truck shall be able to detect the presence of external vehicle(s) (intruder) following the target platoon.

STF_REQ_020: The joining procedure shall not start if intruder(s) are present between ego vehicle and the platoon (Driver in full control).

STF_REQ_021: On receiving "imminent collision" or "collision" message from the forward trucks (in the platoon), the following trucks shall apply full braking (Maximum possible deceleration).

STF_REQ_022: In any handover situation (returning the driving task to any following truck driver), the function shall return the control only if the legal safe gap (time gap of 2 seconds) is reached to the forward vehicle or the ego vehicle has come to a complete stop.

STF_REQ_023: On activating the handover event, platoon leave shall be initiated for the ego truck.

STF_REQ_024: Time gap falling below the safety level (or 0.8 seconds) shall initiate platoon leave procedure for the ego vehicle. (This applies in both cases: driver depressing accelerator pedal or due to functional inaccuracy).

STF_REQ_025: Braking input from any following truck driver (manual braking) in the platoon shall enter the platoon function into standby mode for the ego truck.

Standby Mode:

STF_REQ_026: In standby mode, the platooning function shall not provide any acceleration but shall maintain brake support (if required) to prevent forward collision.

STF_REQ_027: In standby mode, the function shall resume platooning (accelerating) upon receiving resume request from the driver.

STF_REQ_028: In standby mode, if the legal safe gap (time gap of 2 seconds) to the forward vehicle is reached before receiving the resume request from the driver, then the complete responsibility of driving shall be handed over to the driver.

4.2. Communication Requirements

The following section contains requirements on the V2V communication between the trucks:

STF_REQ_029: Each truck shall transmit information related to its lateral movement to the following trucks (e.g. Steering angle, yaw rate, etc… to detect aggressive steering, lane change, …)

STF_REQ_030: While platooning, any truck that initiates emergency braking (manual braking or AEB) shall communicate the event via V2V to the following trucks in the platoon.

STF_REQ_031: Before joining a platoon, the ego truck shall confirm that it is communicating to the correct platoon.

STF_REQ_032: Any truck that detects a situation of imminent collision shall communicate it to the following trucks in the platoon.

STF_REQ_033: Any truck that has an accident (colliding with a large obstacle) shall communicate it to the following trucks in the platoon.

STF_REQ_034: Any truck entering platoon leave “mode” shall communicate the status to the following trucks

STF_REQ_035: Any change to the platoon layout (truck positions and roles) shall be updated and communicated to the entire platoon.

STF_REQ_036: The trucks shall continue sending PCM (Platoon control messages) irrespective of the availability of the GPS signal.

4.3. HMI Requirements

The following section contains requirements on the interactions between the system and the driver:

STF_REQ_037: The driver shall be able to provide “platooning resume” input to the function.

STF_REQ_038: The driver shall be able to provide “takeover acknowledgement” input to the function.

STF_REQ_039: The driver shall be informed about the emergency braking event in the platoon.

STF_REQ_040: The driver shall be informed (clearly) about the current responsible of the longitudinal driving task (Platooning function or the driver).

STF_REQ_041: The driver shall be informed about the increase time gap event.

STF_REQ_042: The driver shall be informed about the decrease time gap event.

STF_REQ_043: The driver shall be informed about the start of the joining procedure (longitudinal control autonomous status).

STF_REQ_044: The driver shall be informed (clearly) about the handover task initiation (return of the longitudinal control).

STF_REQ_045: The driver shall be informed about the standby event.
(For standby mode refer to requirements: STF_REQ_026, STF_REQ_027 and STF_REQ_029).

4.4. Driver Requirements

The following section contains requirements on the driver:

STF_REQ_046: Once the handover task is initiated, the driver shall take full control of the driving before the truck reaches a legal safe gap (2 s time gap) to the forward vehicle.

STF_REQ_047: The driver shall be responsible for detecting and responding to mechanical failures (tire blow-up, oil-leak...) in the ego truck.

5. SUMMARY AND CONCLUSION

The present deliverable evaluates the hazards arising from platoon's nominal function and its implementation. For this, 32 different SOTIF scenarios from 7 different categories of triggering events including driver misuse were analysed to identify hazards, evaluate their risks and define counter measures to handle these situations in a safe way within the platoon.

Once the counter measures were defined for each use case, safety requirements were derived for the platooning application, V2V communication, HMI and the Driver.

The critical requirement to operate the platoon in a safe manner is not to share the driving (longitudinal control) responsibilities between the system and the driver. Therefore, any situation that could be hazardous for the platoon within the operation design domain (ODD) shall be controlled in an automated manner for the following trucks. Moreover, depending on the driver's reaction and judgement with a time gap of 0.8 seconds to the forward truck will put the entire platoon at risk. Consequently, the longitudinal control of the platoon will not be given back to the drivers unless the legal safe gap (time gap of 2 seconds) is reached between the truck and the forward vehicle. The platoon function shall be designed to automatically detect any unsafe situations within the ODD and operate safety without any driver intervention.

The SOTIF analysis in this report has been performed on the ENSEMBLE level A definition which is not yet fully defined in the specifications of D2.4. Based on the update of D2.4 , the specifications the analysis may be impacted.

The SOTIF safety requirements generated in this deliverable complement the requirements for the nominal function defined in the deliverable D2.4. The interactions between these two sets of requirements will be analysed at the system design phase. Any contradiction between the two sets will be resolved at this phase of development.

6. BIBLIOGRAPHY

ISO 26262:2016 (E) – Road Vehicles – Functional Safety

ISO/PRF PAS 21448: Road Vehicles – Safety of the intended functionality

SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems

7. APPENDIX A. GLOSSARY

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.
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).

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
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
SOTIF	Safety Of The Intended Function
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