EUROPEAN COMMISSION

SEVENTH FRAMEWORK PROGRAMME

Theme: ICT

Small or medium-scale focused research projects (STREP)

FP7-ICT-2013-10

Objective ICT-2013.6.5 Co-operative mobility

a) Supervised Automated Driving

GA No. 612035

Interoperable GCDC AutoMation Experience

Deliverable No.	i-GAME D2.5	
Deliverable Title	Protocol for the transition of control	
Dissemination level	Public	
Written By	Ellen van Nunen (TNO) Lorena García-Sol (Idiada) Pere Balaguer (Idiada) Dehlia Willemsen (TNO) Jeroen Ploeg (TNO)	12-03-2015
Checked by	Cristofer Englund (Viktoria) Alejandro Medina Morales (TU/e) Lorena Garcia-Sol (Idiada)	07-03-2015 10-03-2015 20-03-2015
Approved by	Almie van Asten (TNO)	01-04-2015
Status	FINAL	31-03-2015

Please refer to this document as:

DEL150331_i-GAME_D2.5 Protocol for the transition of control

Acknowledgement:

The authors would like to thank Cristofer Englund (Viktoria) and Alejandro Medina Morales (TU/e) for the review and Reinder J. Bril (TU/e) for his guidance in the process.

Disclaimer:

i-GAME is co-funded by the European Commission, DG Research and Innovation, in the 7th Framework Programme. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

Executive Summary

The scope of this document is to define a protocol for the transition of control, within the i-GAME challenge. The i-GAME challenge is based on two scenarios (a highway scenario and a crossing scenario). For each of these scenarios, the protocol for transition of control is described. The transition of control is typically to be found in starting and stopping of a scenario, and also in case of hazards.

The goal of this deliverable is to:

1. Design a scenario start mechanism
2. Design a scenario stop mechanism
3. Design a scenario abort mechanism (including collision avoidance controller)

Design of the scenario start and stop mechanism

The main task of the driver is to monitor the system. Further, the driver interacts with the system:

- at the start of a scenario,
- at the stop of a scenario,
- during the execution of a merging maneuver, and
- in case of a hazard, the driver should be able to abort the system.

For each situation the algorithm is explained by means of sequence diagrams, which are described in detail in this report. Summarized, the driver has to e.g. press a button to start a scenario, and the roadside unit also has to broadcast a message to start the scenario. When in a platoon, the stop mechanism first increases the time gap between the vehicles, before the driver takes over control.

In case of a hazard there are several ways for the driver to take over control immediately, e.g. by pressing the brake pedal or by pressing an emergency button.

Design of the scenario abort mechanism

A Hazard Assessment by Risk Analysis (HARA) is done to show which hazardous situations should be adressed. The solutions for these hazardous situations can be provided by either the system or by the driver. For a selection of hazardous situations software solutions are proposed. These solutions are approached from a fail-safe perspective (in the event of failure, no harm is caused, or at least a minimum of harm, to other devices or danger to personnel) and as a next step the system availability is increased by fault-tolerance (the property that enables a system to continue operating properly in the event of the failure).

Possible fail-safety solutions are presented based on a short literature overview on collision avoidance. There are several possible approaches for collision avoidance; physical approach, optimization approach and rule-based approaches.

Based on the realtime calculation time and the verification possiblities, the physical approach seems to be the most suitable method to apply for the collision avoidance in the highway challenge. For the crossing scenario the rule-based approach seems most feasible.

The proposed fault tolerant approach is mainly based on the calculation of brake distances of the preceding vehicle and the host vehicle. Hereby the behavior of the preceding vehicle has to be predicted, which will be based on assumptions. Further, the response of the host to the preceding vehicle can be described analytically and also string stability and sensor inaccuracies can be taken into account (when assuming these to be gaussian distributed). This approach will define safe controller settings (spacing policy).

Table of contents

EXECUTIVE SUMMARY 3

INTRODUCTION....................6

1 DRIVER INTERACTION....................7

1.1 Highway scenario start mechanism.................... 9

1.2 Highway scenario merging interaction.................... 9

1.3 Highway scenario stop mechanism 11

1.4 Crossing scenario start mechanism 13

1.5 Crossing scenario stop mechanism....................14

2 SCENARIO ABORT MECHANISM....................15

2.1 Driver aborts....................15

2.2 System aborts 17

3 HAZARDS 18

3.1 Functional architecture....................18

3.2 HARA 18

3.2.1 HAZOP (HAZard and OPerability study).................... 19

3.2.2 Situation analysis.................... 19

3.2.3 Hazard 19

3.2.4 Hazard events.................... 19

3.2.5 ASIL determination.................... 19

3.2.6 Safety goals 20

3.2.7 Prevention and detection on scenarios.................... 20

3.3 Selected hazardous events....................21

4 SAFETY SOLUTIONS 23

4.1 Approach 23

4.2 Fail-safety solutions 24

4.2.1 Cut-in AND emergency brake.................... 26

4.2.2 Front-to-side collisions.................... 26

4.2.3 General fail-safety approach 27

4.3 Fault tolerance solutions....................28

4.3.1 All functional, the predecessor issues emergency brake 28

4.3.2 All functional, cut-in 28

4.3.3 Communication degrades/fails, some time later predecessor issues emergency brake 28

4.3.4 Inaccurate sensor inputs 28

4.3.5 General fault-tolerance approach 28

5 CONCLUSIONS....................30

6 WORKS CITED....................31

APPENDIX A HARA (HAZARD ANALYSIS AND RISK ASSESSMENT) 32

A.1 Highway Scenario 32

A.1.1 HAZOP (HAZard and Operability study) 32

A.1.2 Situation analysis 34

A.1.3 Hazard 34

A.1.4 Hazard events 35

A.1.5 ASIL determination 37

A.1.6 Safety goals 39

A.1.7 Prevention and detection on scenarios 40

A.2 Intersection Scenario 51

A.2.1 HAZOP (HAZard and Operability study) 51

A.2.2 Situation analysis 53

A.2.3 Hazard 53

A.2.4 Hazard events 54

A.2.5 ASIL determination 55

A.2.6 Safety goals 57

A.2.7 Prevention and detection on scenarios 57

A.3 Emergency Vehicle Scenario (Demonstrator) 63

A.3.1 HAZOP (HAZard and Operability study) 63

A.3.2 Situation analysis 64

A.3.3 Hazard 64

A.3.4 Hazard events 65

A.3.5 ASIL determination 66

A.3.6 Safety goals 67

A.3.7 Prevention and detection on scenarios 68

Introduction

The i-GAME project

The objective of i-GAME is to develop technologies that speed-up the real-life implementation of automated driving, which is supported by communication between the vehicles and between vehicles and roadside equipment.

Background to functional architecture

The functional architecture is defined to fulfill the requirements of the scenarios to be performed in the i-GAME challenge. It is closely in line with the ETSI standards for the cooperative intelligent transport systems (C-ITS). The architecture defines the main types of ITS-Stations involved in the challenge, the communication architecture, as well as the prototyping methods for the vehicle systems. The description of the architecture is generic and stands on a higher level, giving full flexibilities for the participating teams for implementing while at the same fully aligning to the C-ITS standards.

Contents and structure of this document

The scope of this document is to define a protocol for the transition of control, within the i-GAME challenge. The scenarios for this challenge are defined in D1.1 (Didoff, 2014) and will be recapitulated in section 1. The transition of control is typically to be found in starting and stopping of a scenario, and also in case of hazards.

This document consists of an executive summary and the description of the following tasks:

1. Design of a scenario start mechanism
2. Design of a scenario stop mechanism
3. Design of a scenario abort mechanism (including collision avoidance controller)

The start and stop mechanisms are described in the section 1. Details on the abort mechanism are described in section 2. The abort mechanism is based on the hazard analysis, which is performed in section 3. Further possible safety solutions are presented in section 4.

Sections 1 and 2 are intended to be a guideline for the participants of the challenge. Further, in section 3.3 a selection of hazardous events are presented. The participants should have a safety solution for each of these hazards. For the benchmark vehicles the safety solutions for these hazards are described in section 4.

1 Driver interaction

The main task of the driver is to monitor the system. Further, the driver interacts with the system:

- at the start of a scenario,
- at the stop of a scenario,
- during execution of a merging maneuver (here the driver assists the vehicle), and
- in case of a hazard, the driver can abort the system.

The start and stop for each scenario are described in this chapter (section 1.1 and 1.3 describe the highway scenario and section 1.4 and 1.5 describe the crossing scenario). The abort mechanism is described in section 2.1. Further, for the highway scenario, to ensure a safe merging action a confirmation of the driver is required, this interaction is also described in section 1.2.

To recapulate the scenarios, please see Figure 1 for the highway scenario and Figure 2 for the crossing scenario. For further details please see D1.1 (Didoff, 2014).

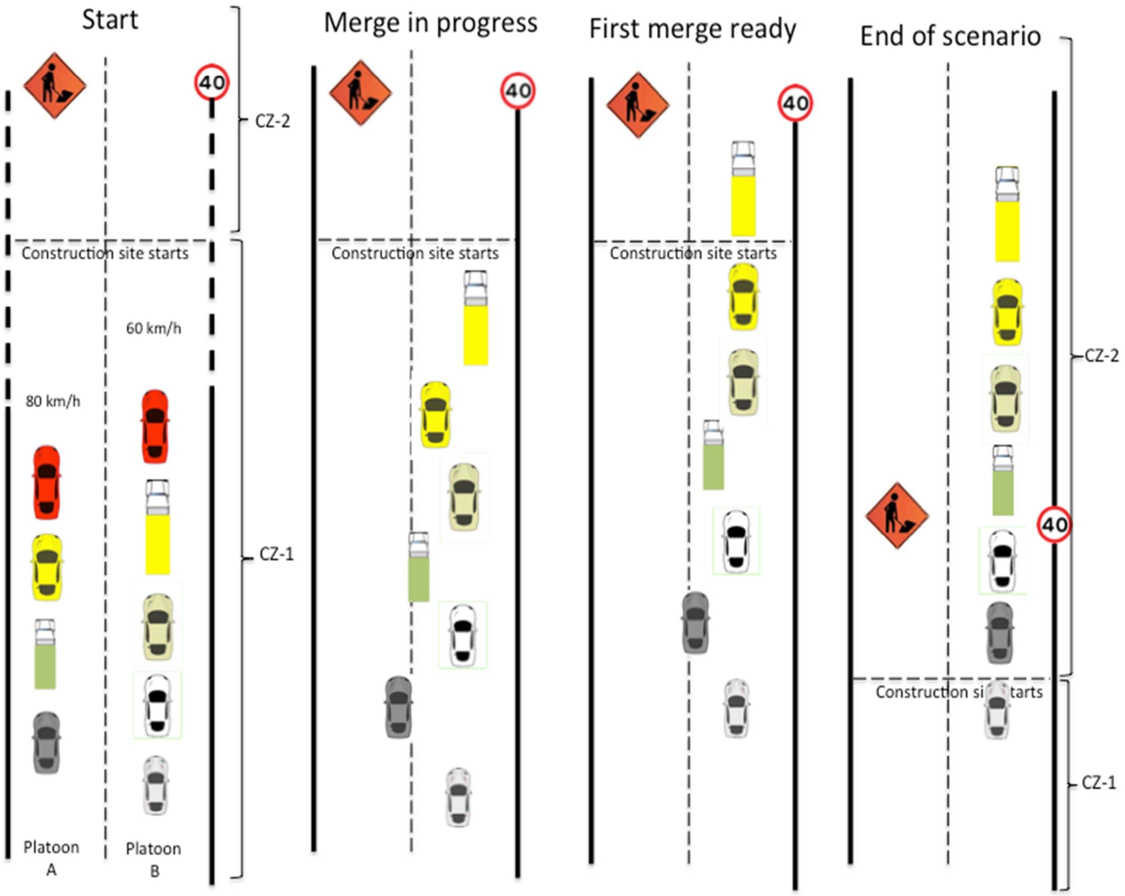


Figure 1: Highway scenario

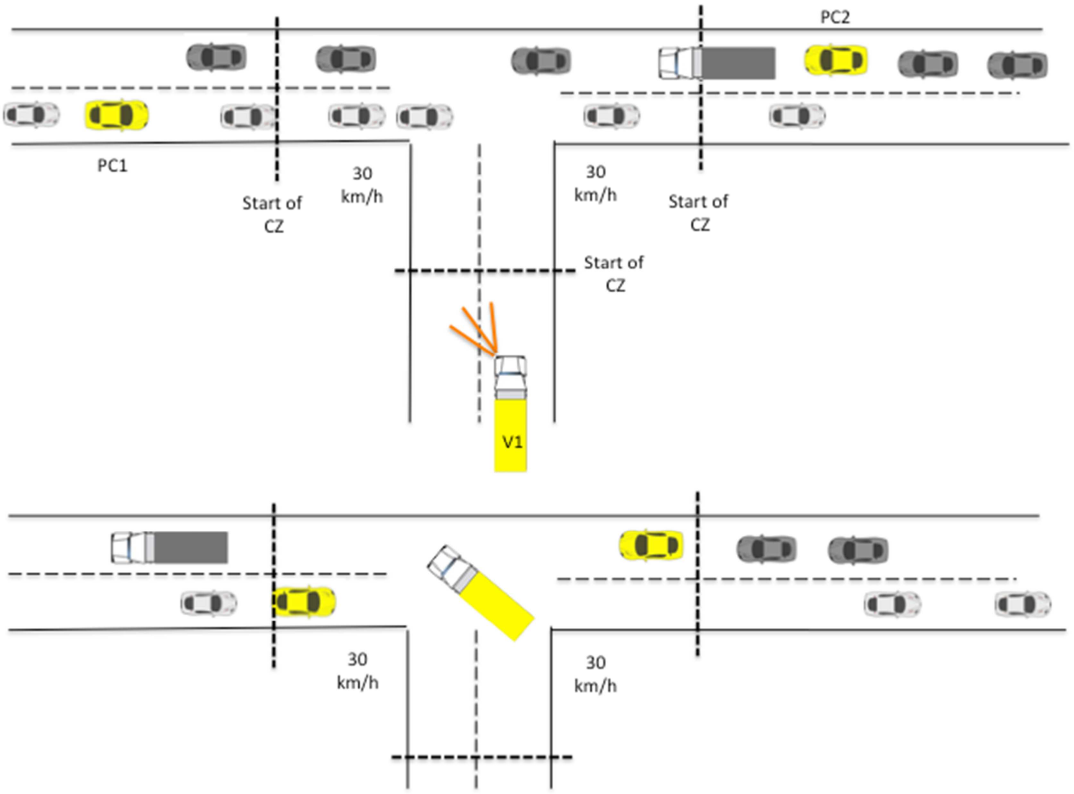


Figure 2: Crossing scenario

To describe the driver interactions, sequence diagrams are used, in which all the relevant actors or systems are presented on the horizontal axis (shown in Figure 3) and the time on the vertical axis. For the longitudinal (and possibly lateral) controlled vehicle the relevant actors and systems are:

- The driver, the person behind the steering wheel.
- The Human Machine Interface (HMI), here we define it to be:
  - a display with touchpad functionality, so it can be used to display information to the driver as well as to obtain information from the driver, and
  - an acoustic means, like a buzzer.
- The control system of the vehicle, which determines the desired actuator setpoints to the vehicle.
- The vehicle itself, including the gateway, which receives V2V and I2V messages.
- The Road Side Unit (RSU), which communicates a start and stop message to the vehicle.

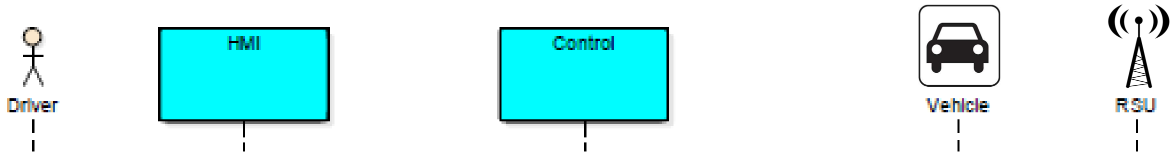


Figure 3: Relevant actors in sequence diagrams.

1.1 Highway scenario start mechanism

The highway scenario starts in standstill. The start mechanism for this scenario is displayed in (the upper part of) Figure 4, and each step can be further detailed as follows:

1. The driver will set the controller to standby by pressing a button on the Human Machine Interface (HMI) display. Also, settings like the desired time gap can be set at the HMI display. This can be done before activation or also be changed when the system is enabled. For the benchmark vehicles, which will drive as leader vehicle, a velocity profile might be pre-programmed and selected.
2. Then, the controller is in standby and will wait for a start-signal from the Road Side Unit (RSU). When this signal is received (AND the driver has enabled the controller) the controller is active.
3. The state of the controller needs to be displayed to the driver, so he/she is aware of the mode of the system.

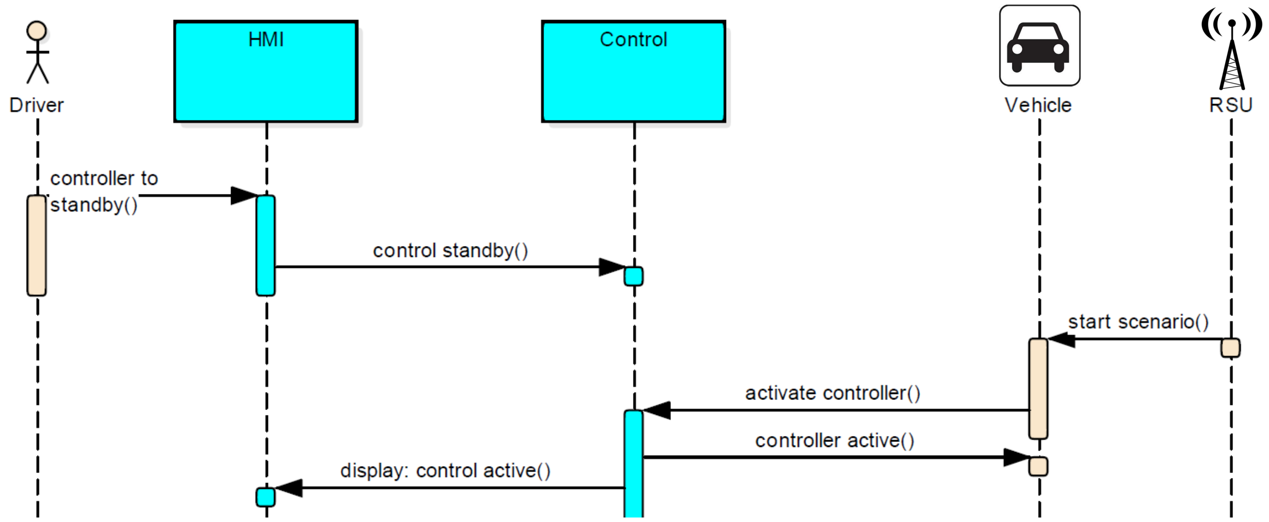


Figure 4: Sequence diagram for start mechanism of highway scenario.

1.2 Highway scenario merging interaction

For this challenge, it is not obliged to have sensors at the side of the vehicle. However, in case a merging action has to be performed a check should be done to ensure there's a free space to merge to. So this merging interaction is only valid for the merging vehicle. Here, the driver should act as a sensor in the situation of a merging vehicle. When the vehicle is laterally controlled, and there are no sensors mounted at the side of the vehicle, the driver is needed to confirm that it's safe to merge. So also here a driver interaction is needed. This part of the driver interaction is depicted in the sequence diagram of Figure 5, and it is described as follows:

1. On the HMI a message is displayed: is it safe to merge?
2. The driver of the merging vehicle has to confirm that it is safe.
3. Only when the confirmation is received, the lateral controller can steer to the right for the merging maneuvre.

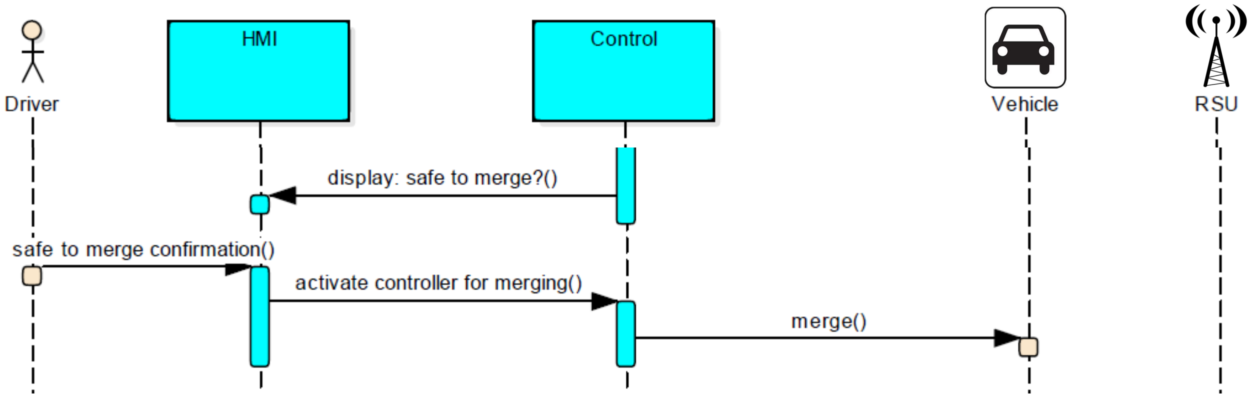

Driver
HMI
Control
Vehicle
RSU
display: safe to merge?()
safe to merge confirmation()
activate controller for merging()
merge()

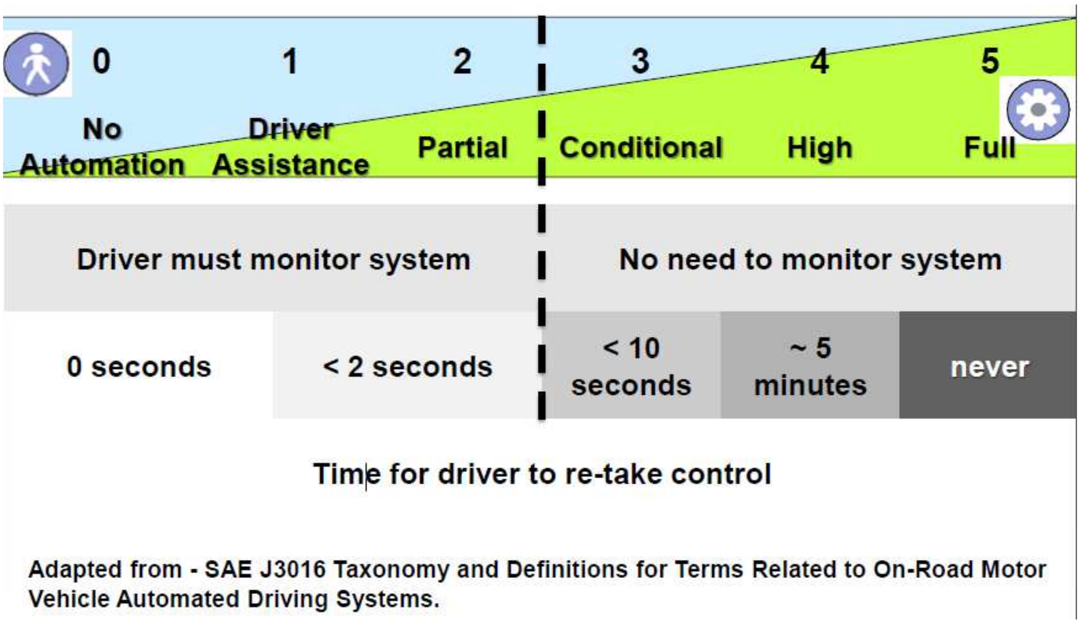
Figure 5: Sequence diagram for merging interaction for the merging vehicle in the highway scenario.

1.3 Highway scenario stop mechanism

For the stop mechanism, there are multiple possibilities considered:

- Stopping in standstill; when the first vehicle will slowly reduce velocity and come to a full stop the system can safely bring the participants to a situation they can easily take over.
- Driver takes over by braking, in case the driver brakes, the system will be disabled (described in section 2.1).
- Driver presses a button to disable the controller, such that the controller can bring the vehicle to a safe state and the driver can easily take over. The safe state in this situation is a higher time gap (e.g. h= 2s) with respect to the preceding vehicle. The reaction times for each level of automation are shown in Figure 6.

Since in the future, the transition from system to driver is likely to follow the procedure mentioned in the last point, (Willemsen D. , Stuiver, Hogema, Kroon, & Sukumar, 2014) (Willemsen, Stuiver, & Hogema, 2014) it is chosen to implement this in the benchmark vehicle.



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

Figure 6: Time for driver to re-take control for each level of automation.

The stop mechanism is only allowed after the merging actions, when the scenario is ended (so not during merging actions). The steps for the stop mechanism are depicted in the sequence diagram in Figure 7, and described as follows:

1. The driver presses a button on the HMI that he/she wants to disable the controller.
2. The controller will increase the time gap to the car in front.
3. When the desired time gap is achieved, the “take over” message will be send to the display and a sound will be used to get the drivers attention.
4. The message ‘take over’ will be displayed via the HMI (display and sound).
5. The driver takes over by using the gas/brake pedal (and steering wheel) and drives manually.
6. The controller is disabled as soon as the driver either steers, presses the brake or presses the gas pedal.
7. The display shows the “controller disabled” state.

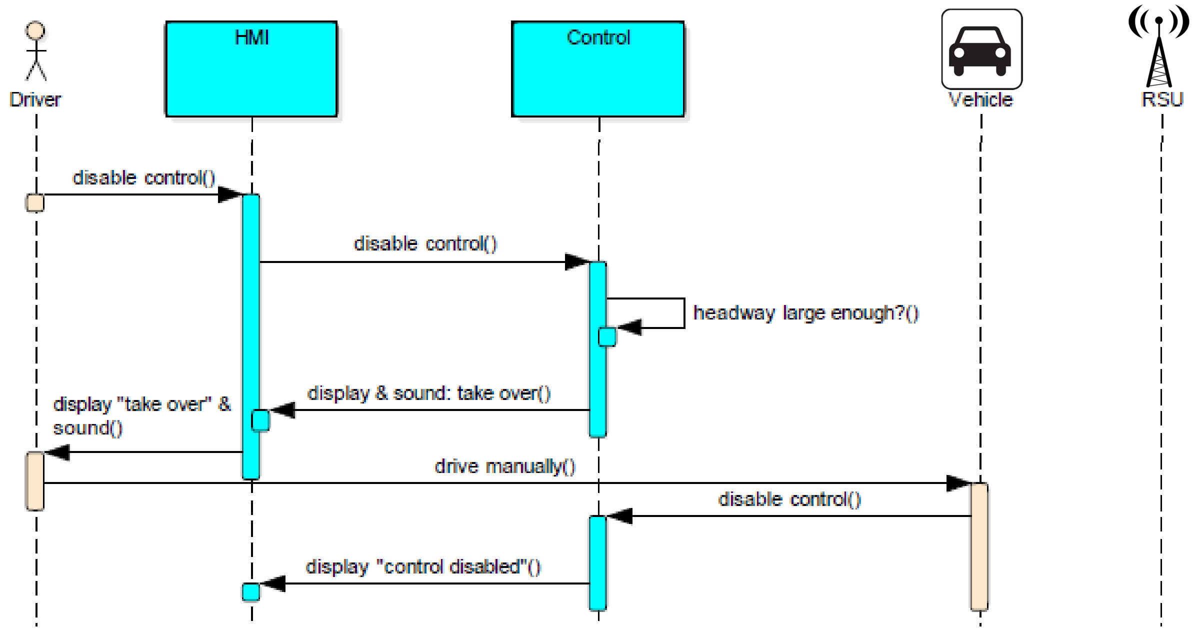


Figure 7: Sequence diagram for stop mechanism of highway scenario.

1.4 Crossing scenario start mechanism

For the crossing scenario the start of the scenario is a little more complex; the vehicles are expected to be at a certain position, and at a certain time with a certain velocity.

To do so, the vehicle needs to be pre-programmed to reach this velocity at this position. From that, the traveled distance, and the time needed to reach that point can be extracted. Let's assume that each vehicle can reach the velocity (of 30 km/h) within a time period of 100 s (which would correspond with an average acceleration of less than 0.1 m/s^2). When the RSU sends a 'start scenario' message, this is used for synchronisation and the time at which the participants receive the message can be defined to correspond to t=-100s. Then, every vehicle has to be at the required position at t=0s, and the scenario starts from there.

Now, the steps for starting the scenario can be described as follows:

1. The driver has to set the following parameters at the HMI display/touchscreen: the desired time (0 s), desired velocity at that time (30 km/h) and the desired location (GPS coordinates). This information is given to the high-level controller which will wait for the driver to enable the system and for the signal of the RSU.
2. The user will set the controller to standby by pressing a button on the HMI.
3. The controller will wait to receive the start of the scenario (t=-100 s), it might be that the system decides to wait before it will accelerate, this will then be displayed to the driver.
4. When it is time to accelerate, the vehicle will accelerate and the controller is active, which again, will be displayed via the HMI display to the driver.
5. Finally, the system evaluates itself and displays to the driver whether or not the desired position and velocity are obtained at the correct timing.

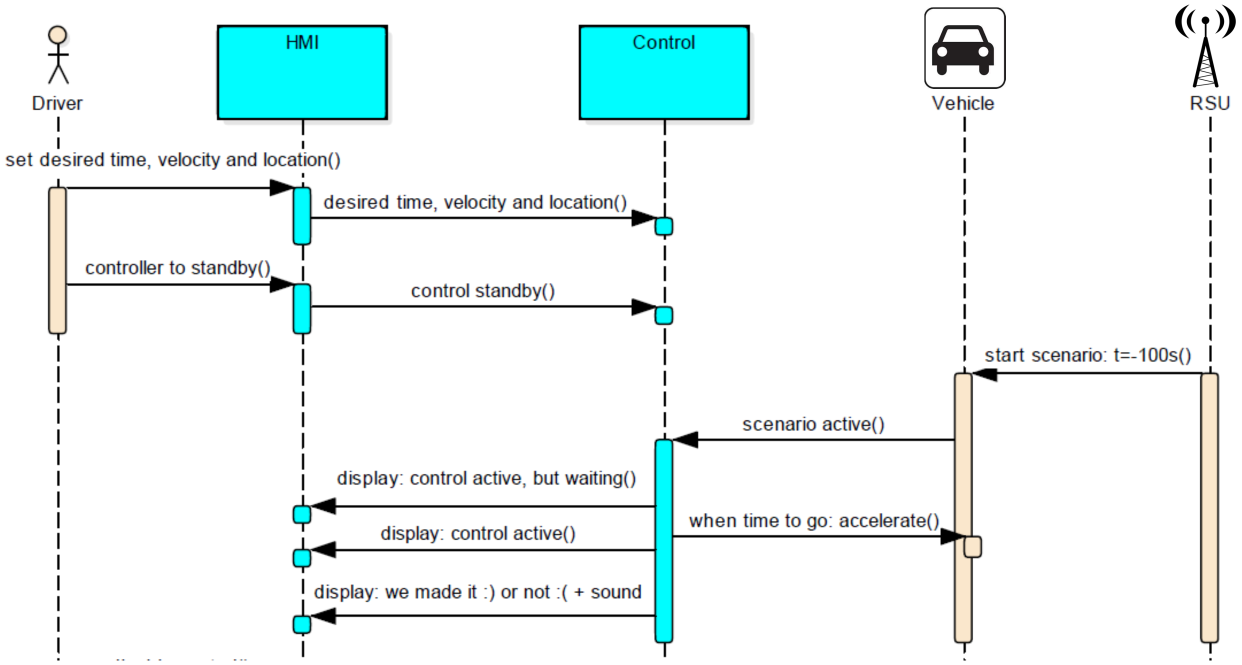

Driver
HMI
Control
Vehicle
RSU
set desired time, velocity and location()
desired time, velocity and location()
controller to standby()
control standby()
start scenario: t=-100s()
scenario active()
display: control active, but waiting()
when time to go: accelerate()
display: control active()
display: we made it :) or not :(+ sound

Figure 8: Sequence diagram for start mechanism of crossing scenario.

1.5 Crossing scenario stop mechanism

The stop mechanism of the crossing scenario is very similar to the stop scenario of the highway scenario, so the system will increase the time gap in case it has a predecessor (Figure 9). In case there's no predecessor, the driver can press gradually the brake and come to a full stop.

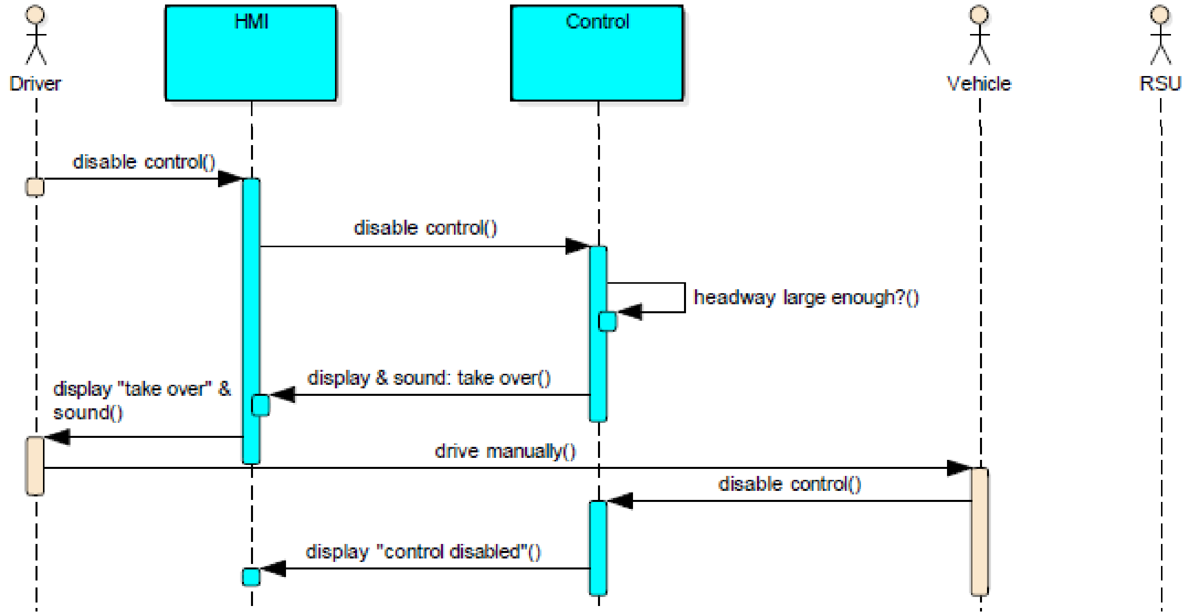


Figure 9: Sequence diagram for stop mechanism of crossing scenario

2 Scenario abort mechanism

In case of a hazardous situation two situations can occur:

- The driver detects the hazardous situation and aborts the scenario execution
- The system detects a hazardous situation and disables itself.

Both situations will be discussed in this chapter.

2.1 Driver aborts

In case the driver detects a hazardous situation himself, there are several means for the driver to take over control and restore the functionallity of a manual driven vehicle:

- By pressing the emergency button which is to be found within reach of the driver: this will disable the low-level (longitudinal and lateral) controller.
- By pressing a button on the HMI: this will disable either the lateral or longitudinal or both controllers.
- By pressing the brake pedal: this will deactive the longitudinal and lateral controller.
- By pressing the gas pedal: this will only be a temporary overrule of the longitudinal controller. The lateral controller will not be disabled.
- By steering: the lateral controller will be disabled. The longitudinal controller will not be disabled.

It will be assumed that there is minimum of 2 persons in the vehicle, such that the driver will not be distracted. The driver should always have a full situation awareness of the traffic situation around him/her and is aware of the state of the system (automated or manual). The passenger will monitor the system in more detail.

The sequence diagram for the above metioned means for the driver to take over control immediately can be found in Figure 10. The threat detection is done by the driver him/herself and is assumed to be the trigger in the sequence diagram.

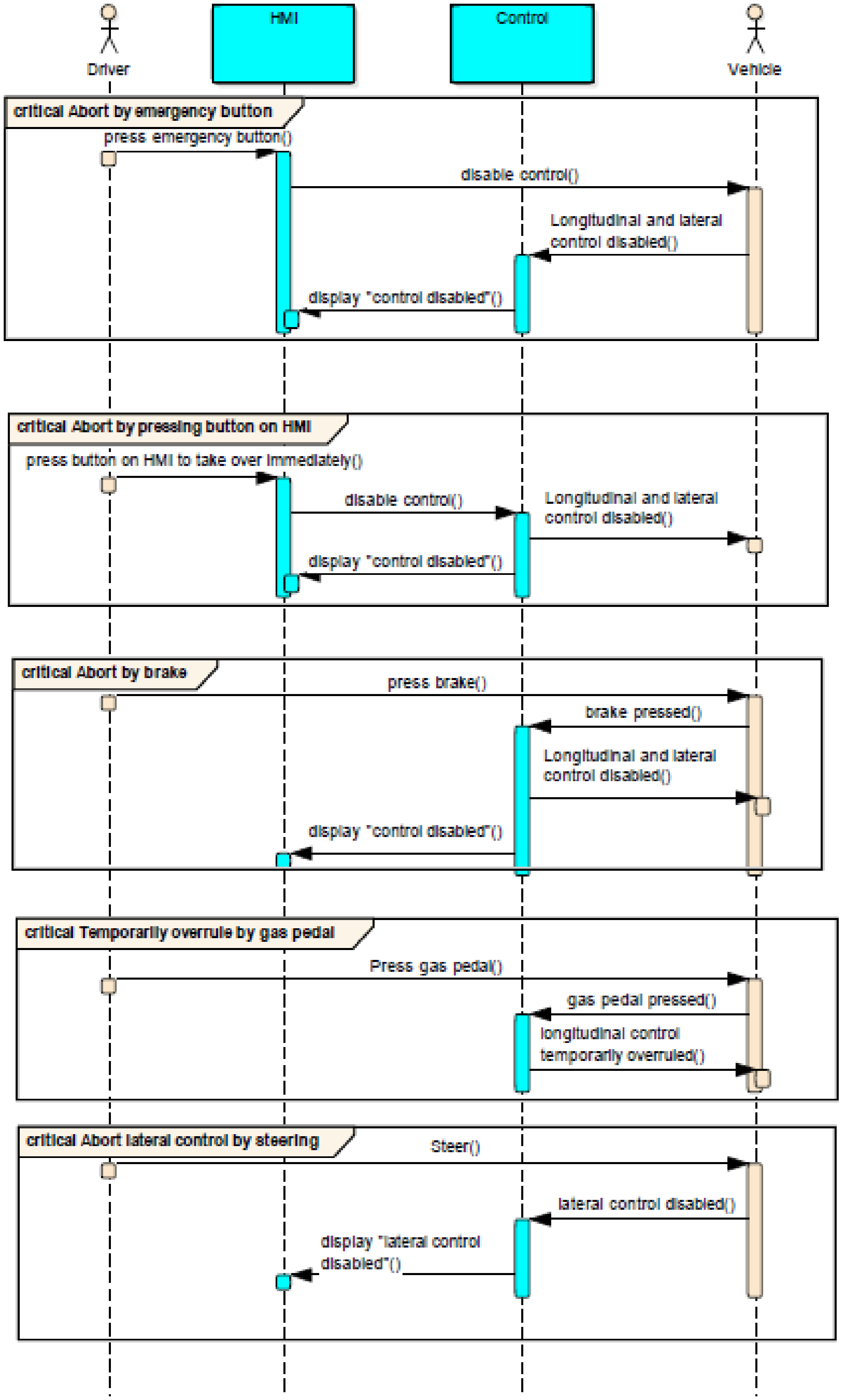

Driver
HMI
Control
Vehicle
critical Abort by emergency button
press emergency button()
disable control()
Longitudinal and lateral control disabled()
display "control disabled"()
critical Abort by pressing button on HMI
press button on HMI to take over immediately()
disable control()
Longitudinal and lateral control disabled()
display "control disabled"()
critical Abort by brake
press brake()
brake pressed()
Longitudinal and lateral control disabled()
display "control disabled"()
critical Temporarily overrule by gas pedal
Press gas pedal()
gas pedal pressed()
longitudinal control temporarily overruled()
critical Abort lateral control by steering
Steer()
lateral control disabled()
display "lateral control disabled"()

Figure 10: Sequence diagram for means for the driver to take over control immediately.

2.2 System aborts

The system can also detect a threat. A threat can be:

- System failure, these can be detected by watch-dogs.
- Sensor failure, these can be detected e.g. by redundancy or plausibility checks.
- Actuator failure, these are however not considered in this project since the actuators of the original vehicle are used and these are not modified.
- Other situations which can lead to a collision. These situations will be the outcome of a HARA (Hazard Analysis and Risk Assessment), which are presented in section 3.2.

The response of the system (how should it come to a safe situation?) will be discussed in section 4.

3 Hazards

3.1 Functional architecture

The functional architecture at which the HARA is based on, is presented in

Figure 11. This architecture is based on Deliverable D1.3 (Englund, 2014).

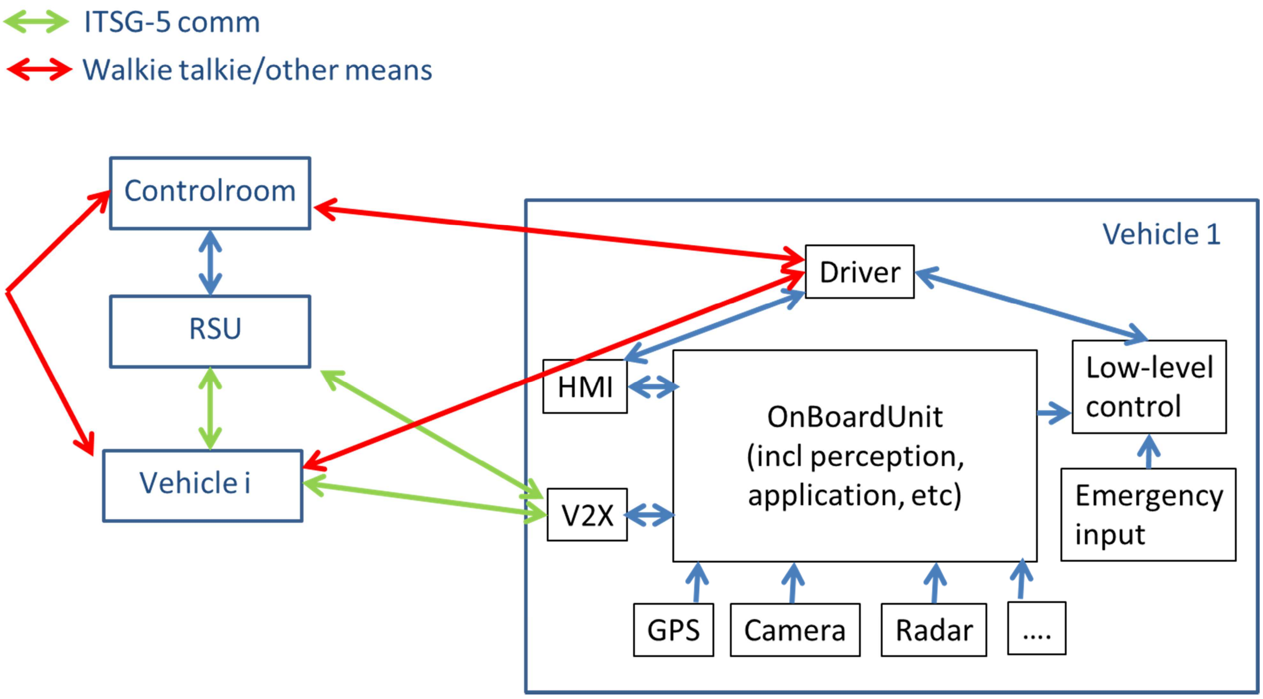


Figure 11: Functional architecture of the total system.

3.2 HARA

The HARA (Hazard Analysis and Risk Assessment) for the different scenarios can be consulted in the Appendix A of this document.

There exist three different HARA's, one for each scenario: Highway, Intersection and Emergency Vehicle scenario. Each scenario performs an specific function:

1- Scenario 1 (Highway): Two vehicle platoonings shall merge in one vehicle platooning.

2- Scenario 2 (Intersection): Three vehicles in the CZ and are approaching a T-intersection (two in the main road on contrary directions (PC1 and PC2) and the third in the intersection (V1)) shall to coordinate and collaborate to allow the third vehicle enter to road.

3- Scenario 3 (Emergency Vehicle): The cooperative vehicles know at which time the EV will be close and act in a cooperative manner to create room for the EV.

Each HARA is structured in seven different parts, which are explained in the subsections 0-3.2.7.

3.2.1 HAZOP (HAZard and OPerability study)

The HAZOP is an study of the deviations of the function performed by each one of the three scenarios at system level. These deviations are the malfunctions of the functions described above about each scenario.

The following Table 1 gives an overview of commonly used guide words and common interpretations of them:

Table 1 – HAZOP guide words

Guideword	Notes
No	Does not happen what is expected.
More	Go beyond the expected maximum value.
Less	Go below the expected minimum value.
As well as	Meets the expectation but unwanted thing happens in addition.
Part of	A part of the expectation happens.
Reverse	What happened is opposite to expectation.
Other than	The expectation happens other than expected.

3.2.2 Situation analysis

In this part of HARA it is indicated where the functions of different scenarios will be performed, and what are the conditions of the road.

It is important to note that the safe conditions in a dry road are better that in a wet road.

3.2.3 Hazard

The different unintended maneuvres are identified and described as hazards provoked by only one vehicle, but take into account that the combination of the unintended maneuvres are also possible.

The different hazards are classified deppending on the type of unnintended manoeuvre.

3.2.4 Hazard events

The combination of hazards and malfuntion behaviours leads to the hazard events. In order to classify the hazard events deppending on their priority, new tables have been created (A.1.4, A.2.4 and A.3.4), but this is not enough, for this reason another tables have been created apart from these, follow with the next chapter, 3.2.5.

3.2.5 ASIL determination

Automotive Safety Integrity Level (ASIL) determination is a function of three parameters: severity (S), exposure (E) and controllability (C), as it is shown below, where (as per ISO International standard 26262):

- Severity (S): estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation.
- Exposure (E): state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis.
- Controllability (C): ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures.

Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior.

Levels range from A to D, with criticality increasing from A to D. Depending on that level, certain rules of development and documentation have to be followed. The class QM (quality management) denotes no requirements to comply with ISO 26262.

For more information related with ASIL, review the deliverable D 4.5.1. Safety analysis of scenarios and requirements

3.2.6 Safety goals

The result of the hazard analysis and risk assessment are four safety goals and their associated ASILs for functions of the escenarios

The safety goals are identified in the deliverable D 4.5. Safety analysis of scenarios and requirements.

3.2.7 Prevention and detection on scenarios

A very important part of HARA consists on the prevention and detection of possibles malfunction behaviours, for this reason, one time each Hazard Events with his malfunction behaviour is detected, paired, the malfunction/s is/are detected.

The most common malfunctions detected here are:

1- Communication degrades/fails.

2- Innacurate sensor inputs.

3- Cut-in.

4- Acceleration.

5- Emergency brake.

Review the Annex of this document for more details.

3.3 Selected hazardous events

The hazardous events are based on individual hazards. In case a platoon fails to merge into the other platoon, this is a result of individual failure(s). So, the focus is on individual hazards.

For the benchmark vehicles a selection of hazardous situations will be considered. This selection is based on the HARA presented in section 3.2. One of the hazardous situations is an emergency brake. An emergency brake of a vehicle is chosen to be defined as follows: the acceleration profile a vehicle performs when it applies its minimum acceleration (or maximal deceleration), starting from a constant velocity towards standstill.

The hazardous situations which lead to ASIL D are often based on a combination of a failure and a hazardous event. These combinations will be shortly discussed below.

<u>For the highway scenario:</u>

1. A communication failure AND at the same time an emergency brake (HE_027, HE_028, HE_030, HE_031, leading to ASIL D). Possible approaches here are:
    a. Increase the nominal time gap to a time gap which is safe for this situation.

    b. Use a redudant communication means, such that the probability of communication failure is very low (because then both means have to fail at the same time).

    c. Use a collision avoidance controller. However, onboard sensors often have a delay of approximately 0.2s, and with an actuator delay of 0.2s, short time gaps become challenging. E.g. in the situation that one would drive with a time gap of 0.3s, tests have showed that, in case the preceding vehicle brakes with -6 m/s^2, the follower vehicle should brake with -4.5 m/s^2 in case a communication failure occurs. However, this leads to high risks of rear-end collisions, so this introduces another hazardous situations which is much more likely to occur.

    d. Make the driver aware of the communication failure (e.g. by a sound) in case the communication failure is longer than the system can handle (which is expected to be in the order of 0.2s), so he can take over in case the preceding vehicle issues an emergency brake at the same time . Meanwhile, the system can increase the time gap. The focus changes then to the situation that the communication fails and a few seconds later the preceding vehicle issues an emergency brake, because this stiuation is more likely to happen during the challenge and does also lead to a high severity.

    So, it is proposed to approach this hazardous situation by focussing on d:
    <u>Communication degrades/fails, some time later, when a safe distance is obtained (which is in the order of 3 s), predecessor issues emergency brake.</u>

2. A communication failure AND cut-in (HE-012, HE-013, HE-015, HE-016, HE-017). Possible approaches are:
    a. Use a redudant communication means, such that the probability of communication failure is very low (because then both means have to fail at the same time).

    b. Make the driver aware of the communication failure (e.g. by a sound), so he can take over in case a vehicle cuts in at the same time. In case of an unexpected cut-in (and communication available) the system should be able to avoid a collision (within reasonable conditions, which are physically feasible).

    So, it's proposed to approach this hazardous situation by foccusing on b:

    <u>Avoid a collision in case of a unexpected cut-in</u>

3. Inaccurate sensor inputs AND cut-in (HE_036, HE_037, HE_039, HE_040, HE_041). Possible approaches are:
    a. Require the accuracy for the sensors to be high enough such that the sensors can detect this situation accurately enough (and fast enough).
    b. Make the driver aware when sensor accuracy (e.g. by a sound) is not sufficient and let him/her take over in case a cut-in happens. Let the system be able to avoid a collision when a cut-in happens (within reasonable conditions).

   So, it's proposed to approach this hazardous situation by focusing on b:

   Cut-in

4. Inaccurate sensor inputs AND emergency brake (HE_051, HE_052, HE_054, HE_055). Possible solutions are:
    a. Require the accuracy for the sensors to be high enough such that the sensors can detect this situation accurately enough (and fast enough).
    b. Use communication only. The desired acceleration of the preceding vehicle is still communicated and can be used as feedforward. In case the driver brakes manually, the system should be able to translate the brakepedal posiiton to an intended acceleration. This situation will not lead to a collision in case communication of the intended acceleration is used.

   So, it's proposed to use the communicated desired acceleration as a feedforward. The intended acceleration must always be communicated by the participants (also in case of manual braking).

For the crossing scenario there's no ASIL D to be found, since it's based on low velocities (30 km/h), so the expected severity in case of a failure is low. Please note, that in case the velocity was chosen higher, there would be higher ASIL levels to be found.
Front-to-side collisions will still be considered, as these are the most dangerous.

So the list of selected hazardous events can be summarized as follows:

- For the highway scenario:
    - Communication degrades/fails, some time later, when a safe distance is obtained (which is in the order of 3 s), predecessor issues emergency brake (related to HE_027, HE_028, HE_030, HE_031)
    - Cut-in (related to HE-012, HE-013, HE-015, HE-016, HE-017)
    - All functional, predecessor issues emergency brake* (related to HE_051, HE_052, HE_054, HE_055).
    - Inaccurate sensor inputs (related to HE_036, HE_037, HE_039, HE_040, HE_041, HE_051, HE_052, HE_054, HE_055).
    - Cut-in AND emergency brake*
    - Driver detects any other unsafe situation and should be able to take over instantly
- For the crossing scenario (additional to the list mentioned above):
    - Front-to-side collisions

Safety solutions for this list of hazards will be designed and implemented in section 4.

4 Safety solutions

First, the global approach will be described in section 4.1. A distinction will be made between fail-safety and fault-tolerance. Fail-safety solutions will be presented for a few of the selected hazardous events in section 4.2 and fault-tolerant solutions for the other selected hazardous events are presented in section 4.3.

4.1 Approach

For a selection of hazardous situations, safety solutions will be proposed. As a first step, the hazardous situations should lead to fail-safety (safety only):

Fail-safety: in the event of a failure, no harm is caused, or at least a minimum of harm, to other devices or danger to personnel.

As a next step the system availability can be increased by fault-tolerance:

Fault-tolerance: the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure.

This stepwise approach is also shown in Figure 12. Automated driving availability increases when threats become acceptable or resolved.

For a selection of hazardous situations (presented in section 3.3), which are derived from the HARA in section 3.2 either a fail-safe or fault-tolerant solution will be presented in respectively sections 4.2 and 4.3.

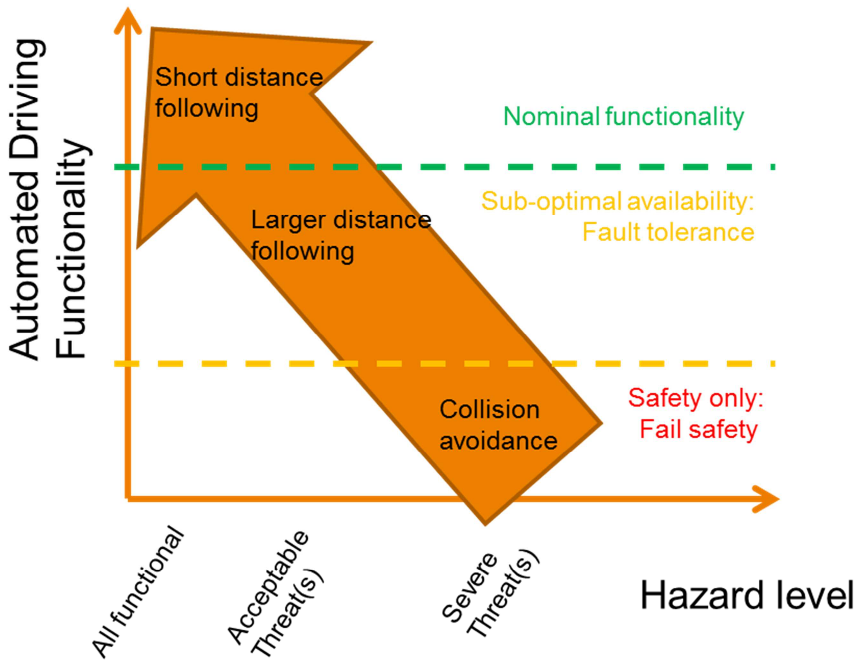


Figure 12: Step wise approach for safety solutions for hazards.

4.2 Fail-safety solutions

For the following hazardous situations a fail-safety approach will be presented:

- Cut-in.
- Driver detects any other unsafe situation and should be able to take over instantly; this is already discussed in section 2.1.
- Front-to-side collisions (crossing scenario).

For a safety approach several steps need to be considered. These steps are also shown in Figure 13. The first step is to perceive its surroundings (environmental perception), e.g. the objects which need to be avoided. When communication is used, more information about the intention of the vehicles can be shared. This enables short following distances for Cooperative Adaptive Cruise Control, as shown in (Ploeg, 2014). The desired acceleration of the preceding vehicle can be used as feedforward for the controller. The feedforward action is added to the feedback action of the controller, which enables a fast response to the acceleration of the predecessor. As feedforward, the current acceleration could be used as well, but the actuator delay causes a later response of the host. Therefore, in this situation larger following distances are needed. So, adding communication to the fail safe strategy can thus be very benificial in order to respond fast. Note that the communication will be time-triggered, at a frequency of at least 10Hz.

The output of the environmental perception serves as input for a collision avoidance controller, which, on its turn can determine the required actuation to avoid a collision. The function of the collision avoidance is hereby defined to avoid a collision for the above mentioned hazardous situations.
The actuation can either be braking or steering or a combination. For each of the situations these three steps will be further discussed (sections 4.2.1-4.2.2). Then, (section 4.2.3), a general safety approach will be proposed which fits all of the above mentioned hazardous situations.

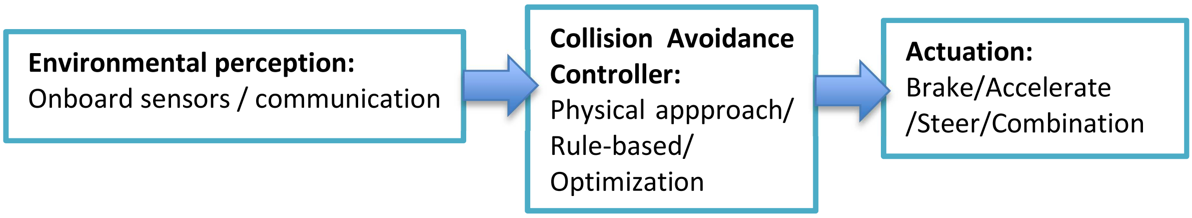

Environmental perception:
Onboard sensors / communication
Collision Avoidance Controller:
Physical appproach/
Rule-based/
Optimization
Actuation:
Brake/Accelerate
/Steer/Combination

Figure 13: Steps in safety approach.

Generally, for collision avoidance there are many approaches possible. An short overview of collision avoidance methods, based on literature is given below:

Physical approach

- The *potential field* approach is suggested by (Khatib, 1986) for the field of Mobile Robots. Also others, like (Gehrig & Stein, 2007) refer to this approach.
- *Elastic bands* are used in (Quinlan & Khatib, 1993) and in (Gehrig & Stein, 2007). In the first reference, so-called bubbles are defined which connect possible points. The radius of these circles are chosen such that the path is collision free.
- *Physical models* like fluid dynamics are proposed, as an alternative to the potential field method, in (Decuyper & Keymeulen, 1991). Fluid dynamics equations are used. The fluid starts at the starting point towards the goal point, and obstacles obstruct the flow. From the resulting flow field, the planned path can be computed.

Rule-based

- Methods based on communication for collision avoidance are compared in (Garcia, 2007), with the goal to improve safety in rail transport. An *agent-based cooperative approach* is also proposed by (Vrba, 2007), here negotiation and goal sharing of agents is proven to be highly efficient for avoiding collisions.
- A *deterministic approach* is proposed by (Lee, Kim, & Huh, 2014). The predicted stopping distance is calculated for an autonomous braking system.
- *Probabilistic risk estimation* is proposed in (van Nunen, van den Broek, Kwakkernaat, & Kotiadis, 2011). Here, probabilitistic models describe the behavior of vulnerable road users and vehicles, based on physical limitations. A risk on collision can then be calculated.

Optimization

- The *game theory* approach is used to analyse safety distances by (Martensson, 2012). Here the evader and pursuer game is formulated as the minimization/maximization of a cost function.
- *Safe set computations* to find safety criteria for vehicles traveling in a platoon are done by (Alam, Gattami, Johansson, & Tomlin, 2014).

The advantages and disadvantages of each method are shown in Table 2. Formal verifications might be possible for the physical approaches, while for optimization the techniques are often complex and therefore would require a large number of rule to completely cover all possible scenarios. Further, optimization methods often require a high calculation time, which makes a real-time implementation more challenging. The physical approach is less calculation time demanding.

Rule-based methods decide upon an action based on a (combination of) rule(s). An example is that a car will brake in case the time to collision is smaller than 1 second. These methods are more sensitive to false positives, since the behavior of other road participants are very dependent on the situation. Hardly all situational aspects can be included, so therefore it's more sensitive to an incorrect prediction, leading to more false positives. When including probability density functions, the realtime calculation time increases as well and thereby it's not necessarily leading to a proper response action (e.g. should one brake when the probability on a collision is higher than 90%?). The rule-based methods are thus less robust than the physical approach. Further, due to its complexity, it's not always possible for an optimization method to prove its robustness.

So, the physical approach seems to be the most suitable method to apply for the collision avoidance challenges defined.

	Formal verification possible	*Calculation-time*	*Robustness*
Physical approach	+	+	+
Rule-based	+	+/-	-
Optimization	-	-	+/-

Table 2: Advantages and disadvantages of collision avoidance methods

4.2.1 Cut-in AND emergency brake

Environmental perception

To detect a cut-in, by the gap-making vehicle, onboard sensors will be used. When the sensors are only positioned at the centre of the front bumper they require a sufficiently large opening angle. Communication is less usefull here, since global positions are likely to be less accurate.

For the emergency brake, communication is very usefull. In case the intention (emergency brake) can be communicated directly the follower vehicle can respond much earlier than when using onboard sensors. In case the emergency brake is initiated by the driver himself, the system should still communicate the intention (e.g. by reading the brake pedal position).

Collision Avoidance controller

The most suitable approach for this situation seems to be the physical approach with feedforward.

Actuation

It's expected that a collision in this situation can be avoided by braking. No steering is required.

4.2.2 Front-to-side collisions

Environmental perception

When the sequence of who goes first is determined (Deliverable D2.1) a model can be used which calculates a expected position. At a certain point in time one vehicle should detect another vehicle by its onboard forward-looking sensors.

For example, in case that the the truck (1) goes first, then the vehicle on the left (2) and then the vehicle on the right (3) as shown in Figure 14. At a certain point in time, vehicle 2 should see the truck (1) and a few moments later vehicle (3) should see the truck. The time at which these events should happen can be calculated based on the expected position model. If this does not happen, an emergency brake should be applied.

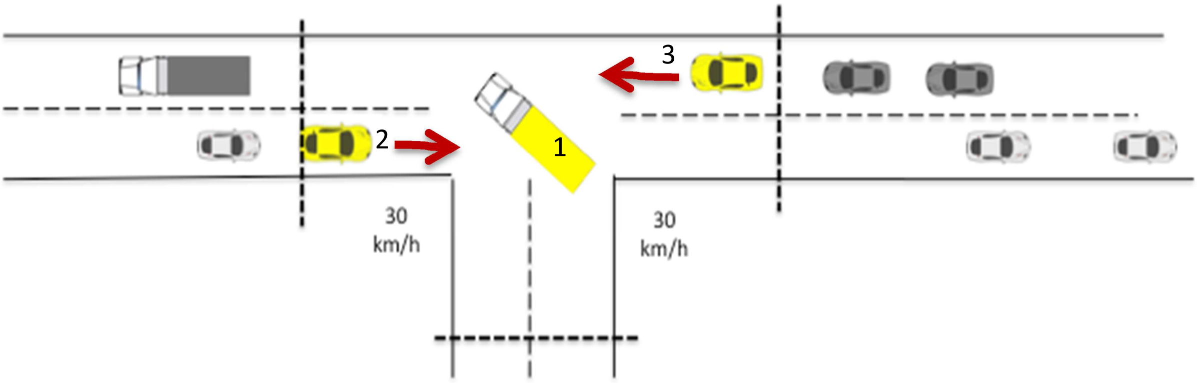


Figure 14: Example of sequence: vehicle 2 should see truck 1 at a certain moment in time, a few moments later vehicle 3 should see truck 1.

Collision Avoidance controller

The collision avoindance controller will thus be rule-based.

Actuation

An open loop brake action will be applied in case the expected behavior does not match reality. One could also consider to use the driver as a backup (who could avoid a collision by steering).

4.2.3 General fail-safety approach

Environmental perception

The environmental perception can be achieved by using communication and on-board forward looking sensors, such as a camera, radar and/or lidar.

Collision Avoidance controller

For the highway: physical approach with feedforward.

For the crossing: rule-based; in case the expectation differs from reality the actuator will be triggered.

Actuation

The actuation will be done by braking. For the highway scenario it will be a closed-loop braking action and for the crossing it will be an open loop braking action.

4.3 Fault tolerance solutions

For the following hazardous situations a fail-safety approach will be presented:

- All systems are functional, the predecessor issues emergency brake.
- All functional, cut-in.
- Communication degrades/fails, some time later the predecessor issues emergency brake.
- Inaccurate sensor inputs.

4.3.1 All functional, the predecessor issues emergency brake

In case communication is functional, the desired acceleration of the predecessor is known and a CACC implementation should be capable to handle this situation safely. However, the predecessor might have different dynamics (a different actuator delay, time constant and/or minimum acceleration). The minimum time gap to ensure that no collision will occur in this situation can be analytically determined, when the dynamics of the predecessor and host are known, as explained in (van Nunen, Ploeg, Morales Medina, & Nijmeijer, 2013).

4.3.2 All functional, cut-in

The CACC design should be such that the vehicle which cuts in is automatically detected as new MIO (most important object) and thus it will be followed instantly.

A vehicle that cuts in can be a vehicle with and without communication (although in the challenge it is expected that all participating vehicles communicate). When it does not communicate, the host should increase its desired time gap. The exact safe desired time gap can be calculated in a similar manner as mentioned within section 4.3.1. Note that the transition phase to this increased time gap is not necessarily safe, but when it has reached its safe time gap it is safe.

4.3.3 Communication degrades/fails, some time later predecessor issues emergency brake

Again, based on the vehicle (and control) characteristics the safe headway (and standstill distance) can be calculated, this is also presented in (van Nunen, Ploeg, Morales Medina, & Nijmeijer, 2013).

4.3.4 Inaccurate sensor inputs

In the calculation of the safe time gap the inaccuracy of the sensors can also be taken into account. This requires additional knowledge on the sensor inaccuracy, the statistical distribution and its properties, (e.g. the standard deviation of the error).

Often a standard normal (Gaussian) distribution for sensor inaccuracies is assumed. However, this is not always valid. Especially when using GPS the error distribution is likely to be non-Gaussian.

For the steering, too inaccurate sensor inputs are not acceptable. The choice of sensors should be such that the probability of leaving a lane is very small (e.g. 1E-5). Depending on the width of the lane, the width of the vehicle, and the curvature an estimation for the standard deviation of the error can be found.

4.3.5 General fault-tolerance approach

In general, the safe spacing policy (in the situation of the benchmark vehicles this is the time gap and standstill distance) can be calculated realtime. Hereby the following should be taken into account:

- Expected acceleration profile of the preceding vehicle, which depends on:
    - The predicted behavior.
    - The vehicle dynamics, such as the minimum acceleration, time constant and actuator delay.
- The host acceleration response, which depends on:
    - The controller implementation.

  - The vehicle dynamics.

- String stability, the ability to dampen out disturbances along a string of vehicles, (Ploeg, 2014). For the benchmark vehicles, the controlled system can become string stable by increasing the time gap. The required time gap for string stability can thus be calculated.
- The brake paths of both vehicles can be calculated real-time, and based on these parameters, the safe spacing policy can be determined.
- Sensor accuracies can be estimated and included to guarantee safety for a certain probability.

The string stability apsect leads to a choice for the desired time gap (this can be done on forehand, by means of a lookup table). Further, the difference in brake distances between the preceding vehicle and the host vehicle will lead to a setting for the standstill distance. So the output of this approach are the settings for the controller (time gap and stand-still distance in the situation of the benchmark vehicles).

Note that in the calculation of brake distances the conditions need to be stable (details are explained in (van Nunen, Ploeg, Morales Medina, & Nijmeijer, 2013). This is not the case when the settings are just changed, since the controller needs some time to reach the new desired spacing. So in the situation that the preceding vehicle issues an emergency stop AND the communication fails, a collision might still happen.

5 Conclusions

For the i-GAME challenge the interactions between the cooperative system and the driver are described in this deliverable.

The goal of this deliverable is to:

1. Design a scenario start mechanism.
2. Design a scenario stop mechanism.
3. Design a scenario abort mechanism (including collision avoidance controller).

Design of the scenario start and stop mechanism

The main task of the driver is to always have a full situation awareness of the traffic situation around him/her and to be aware of the state of the system (automated or manual). The passenger will monitor the system in more detail. Further, the driver interacts with the system:

- at the start of a scenario,
- at the stop of a scenario,
- during execution of a merging maneuver, and
- in case of a hazard, the driver can abort the system.

For each situation the steps are explained by means of sequence diagrams.

Design of the scenario abort mechanism

A Hazard Assessment by Risk Analysis (HARA) is done to show which hazardous situations should be adressed. The solutions for these hazardous situations can be provided by either the system or by the driver. For a selection of hazardous situations software solutions are proposed. These solutions are approached from a fail-safe perspective (in the event of failure, no harm is caused, or at least a minimum of harm, to other devices or danger to personnel) and as a next step system availability is increased by fault-tolerance (the property that enables a system to continue operating properly in the event of a failure).

Possible fail-safety solutions are presented based on a short literature overview on collision avoidance. There are several approaches possible for collision avoidance; physical approach, optimization approach and rule-based approaches.

Based on the realtime calculation time and the verification possiblities, the physical approach seems to be the most suitable method to apply for the collision avoidance in the highway challenge. For the crossing scenario the rule-based approach seems most feasible.

The proposed fault tolerant approach is mainly based on the calculation of brake distances of the preceding vehicle and the host vehicle. Hereby the behavior of the preceding vehicle has to be predicted, which will be based on assumptions. Further, the response of the host to the preceding vehicle can be described analytically and also string stability and sensor inaccuracies can be taken into account (when assuming these to be gaussian distributed). This approach will define safe controller settings (spacing policy).

6 Works Cited

Alam, A., Gattami, A., Johansson, K. H., & Tomlin, C. J. (2014). Guaranteeing safety for heavy duty vehicle platooning: Safe set computations and experimental evaluations. *Control Engineering Practice*, 33-41.

Albaker, B., & Rahim, N. (2009). A Survey of Collision Avoidance Approaches for Unmanned Aerial Vehicles.

Decuyper, J., & Keymeulen, D. (1991). A reactive robot navigation system based on a fluid dynamics metaphor. *Proc. Conf. Parallel Problem Solving Nature.*

Didoff, J. (2014). *DEL140331_i-GAME_D1.1 Specification of Scenarios.*

Englund, C. (2014). DEL140730_i-GAME_D1.3 Functional architecture.

Garcia, C. (2007). Comparison of Collision Avoidance Systems and Applicatbility to Rail Transport.

Gehrig, S. K., & Stein, F. J. (2007). Collision Avoidance for Vehicle-Following Systems. *IEEE transactions on Intelligent transportation systems.*

Khatib, O. (1986). Real-Time Obstacle Avoidance for Manipulators and Mobile Robots.

Lee, D., Kim, K., & Huh, K. (2014). Development of an autonomous braking system using the predicted stopping distance.

Martensson, J. (2012). Evalutation of Safety Distance in Vehicle Platoons by Combined Braking and Steering.

Ploeg, J. (2014). *Analysis and design of controllers for cooperative automated driving.*

Quinlan, S., & Khatib, O. (1993). Elastic Bands: Connecting Path Planning and Control.

van Nunen, E., Ploeg, J., Medina, A. M., & Nijmeijer, H. (2013). Fault Tolerancy in Cooperative Adaptive Cruise Control. *Proceedings of the 16th International IEEE Annual Conference on.*

van Nunen, E., Ploeg, J., Morales Medina, A., & Nijmeijer, H. (2013). Fault Tolerancy in Cooperative Adaptive Cruise Control. *Proceedings of the 16th International IEEE Annual Conference on.* The Hague, The Netherlands.

van Nunen, E., van den Broek, T., Kwakkernaat, M., & Kotiadis, D. (2011). Implementation of Probabilistic Risk Estimation for VRU Safety. *WIT conference.*

Vrba, P. (2007). Collision Avoidance Algorithms: Multi-agent Approach.

Willemsen, D., Stuiver, A., & Hogema, J. (2014). Transition of Control: automation giving back control to the driver. *Proceedings of the 5th International Conference on Applied Human Factors and Ergonomics (AHFE).*

Willemsen, D., Stuiver, A., Hogema, J., Kroon, L., & Sukumar, P. (2014). Towards Guidelines for Transition of Control. *Fisita World Automotive Congress.*

Appendix A HARA (Hazard Analysis and Risk Assessment)

A.1 Highway Scenario

A.1.1 HAZOP (HAZard and Operability study)

Attribute/Parameter	Guideword	Malfunction/Deviation	Malfunction behavior on system/Consequences	Hazard	Priority	Comments
Vehicle platooning and merging of platoons	No	The platooning is not performed, the vehicles continue in two platoonings, no vehicles performs the merge.	**MF_01**: Communication problem (communication degrades/fails) (platoonings don't see each other) between all the systems installed, the vehicles continue in two platoonings. **MF_02**: There is not communication problem (platoonings recognize each other) but none of the maneuvers have been performed due to inaccurate sensor inputs or something like that.	**HAZARD_01**: Continuous in two platoonings instead of one platooning.	Low	As a safety point of view the platooning merging is not initiated at all. We consider 'low' because the system is not working and it can be identified 'easily' (stop execution of the scenario 'X' meters before reaching road obstacle: visual monitoring).
	More	Not Applicable				
	Less	The platooning is not performed because only some vehicles perform the merge but not all of them.	**MF_03**: Communication problem (communication degrades/fails) (protocol problem source) between systems installed on different vehicles, some vehicles merge, others not. **MF_04**: There is not communication problem (no protocol issues, issues on maneuver decision) but	**HAZARD_02:** Less vehicles than expected (at least one of them) have performed the merging. The platooning is not performed.	Medium	As a safety point of view many situations can occur, most of them dangerous for the occupants of the vehicles. However, there are no unexpected/unintended vehicles maneuvers.

			some vehicles do not perform the expected maneuver (longitudinal/lateral)*			
	As well as	Not Applicable				
	Part of	Not Applicable				
	Reverse	Not Applicable				
	Other than	The platooning is not performed since there are unintended maneuvers (predecessor issues emergency brake/merge when no gap has been created /cut-in/emergency brake / cut-in / acceleration)	**MF_05:** Communication problem (communication degrades/fails) (protocol problem source) between systems installed on different vehicles, a/some vehicle/s may move unexpected **MF_06:** There is not communication problem (no protocol issues, issues on maneuver decision) but some vehicles do not perform the expected maneuver (longitudinal/lateral)*	**HAZARD_03:** Vehicles, at some point of the merging execution, may go in unexpected behavior.	High	Vehicles may behave unexpected due to unintended maneuvers and, therefore, severity of that situation is high.

* Due to a malfunction of any mechanical part and/or innacurate sensor(s) input(s).

A.1.2 Situation analysis

Location	Characteristics	Remarks
Urban area	Max speed:30 Km/h	To be further discussed (originally it's defined to be 80 Km/h and 60 Km/h going towards 40 km/h… this might be too fast).
Highway	Max speed: 60 km/h	

Road conditions	Characteristics	Remarks
Paved dry road	Normal road friction	Vehicle "validation" will be done at dry road, so it's not sure whether the vehicle will behave safe in wet road conditions.
Paved wet road	Low road friction	

A.1.3 Hazard

Assumptions for hazard decomposition events:	Only one vehicle behaves unintendedly; combination of the unintended maneuvers are also possible
	Only one unintended maneuver is considered; vehicle may maneuver as a combination of lateral and longitudinal unintended maneuvers

ID	Description	
HAZARD_01	**HAZARD_01:** Continuous in two platoonings instead of one platooning.	
HAZARD_02	Less vehicles than expected (at least one of them) have performed the merging. The platooning is not performed.	**HAZARD_02_01:** There is space for merging in Platoon B, but merging is not performed at least for one of them due to no possible lateral maneuver (right) (although vehicle (Platoon A) is aligned with gap (Platoon B)). **HAZARD_02_02:** There is space for merging in Platoon B, but merging is not performed at least for one of them because vehicle in Platton A cannot align its position with space gap at Platoon B. **HAZARD_02_03:** There is no enough space gap for merging in Platoon B due to vehicle/s in Platoon B cannot keep space gap constant .
HAZARD_03	Vehicles, at some point of the merging execution, may go in unexpected behavior.	**See below table for different HAZARD situations**

Unintended maneuver / Vehicle Position	Head Vehicle Platoon A	Middle positions Platoon A	Last vehicle Platoon A	Head vehicle Platoon B	Middle positions Platoon B	Last vehicle Platoon B
Lateral (Left)	Hazard_03_01	Hazard_03_02	Hazard_03_03	Hazard_03_04	Hazard_03_05	Hazard_03_06
Lateral (Right)	Hazard_03_07	Hazard_03_08	Hazard_03_09	Hazard_03_10	Hazard_03_11	Hazard_03_12
Acceleration	Hazard_03_13	Hazard_03_14	Hazard_03_15	Hazard_03_16	Hazard_03_17	Hazard_03_18
Deceleration	Hazard_03_19	Hazard_03_20	Hazard_03_21	Hazard_03_22	Hazard_03_23	Hazard_03_24

A.1.4 Hazard events

ID	Location	Road conditions	Malfunctioning Behavior	Hazard	Priority
HE_001	Any	Any	MF_01	HAZARD_01	Low
HE_002	Any	Any	MF_02	HAZARD_01	Low
HE_003	Any	Any	MF_03	HAZARD_02_01	Medium
HE_004	Any	Any	MF_03	HAZARD_02_02	Medium
HE_005	Any	Any	MF_03	HAZARD_02_03	Medium
HE_006	Any	Any	MF_04	HAZARD_02_01	Medium
HE_007	Any	Any	MF_04	HAZARD_02_02	Medium
HE_008	Any	Any	MF_04	HAZARD_02_03	Medium
HE_009	Any	Any	MF_05	HAZARD_03_01	High
HE_010	Any	Any	MF_05	HAZARD_03_02	High
HE_011	Any	Any	MF_05	HAZARD_03_03	High
HE_012	Any	Any	MF_05	HAZARD_03_04	High
HE_013	Any	Any	MF_05	HAZARD_03_05	High
HE_014	Any	Any	MF_05	HAZARD_03_06	High
HE_015	Any	Any	MF_05	HAZARD_03_07	High
HE_016	Any	Any	MF_05	HAZARD_03_08	High
HE_017	Any	Any	MF_05	HAZARD_03_09	High
HE_018	Any	Any	MF_05	HAZARD_03_10	High
HE_019	Any	Any	MF_05	HAZARD_03_11	High
HE_020	Any	Any	MF_05	HAZARD_03_12	High

HE_021	Any	Any	MF_05	HAZARD_03_13	High
HE_022	Any	Any	MF_05	HAZARD_03_14	High
HE_023	Any	Any	MF_05	HAZARD_03_15	High
HE_024	Any	Any	MF_05	HAZARD_03_16	High
HE_025	Any	Any	MF_05	HAZARD_03_17	High
HE_026	Any	Any	MF_05	HAZARD_03_18	High
HE_027	Any	Any	MF_05	HAZARD_03_19	High
HE_028	Any	Any	MF_05	HAZARD_03_20	High
HE_029	Any	Any	MF_05	HAZARD_03_21	High
HE_030	Any	Any	MF_05	HAZARD_03_22	High
HE_031	Any	Any	MF_05	HAZARD_03_23	High
HE_032	Any	Any	MF_05	HAZARD_03_24	High
HE_033	Any	Any	MF_06	HAZARD_03_01	High
HE_034	Any	Any	MF_06	HAZARD_03_02	High
HE_035	Any	Any	MF_06	HAZARD_03_03	High
HE_036	Any	Any	MF_06	HAZARD_03_04	High
HE_037	Any	Any	MF_06	HAZARD_03_05	High
HE_038	Any	Any	MF_06	HAZARD_03_06	High
HE_039	Any	Any	MF_06	HAZARD_03_07	High
HE_040	Any	Any	MF_06	HAZARD_03_08	High
HE_041	Any	Any	MF_06	HAZARD_03_09	High
HE_042	Any	Any	MF_06	HAZARD_03_10	High
HE_043	Any	Any	MF_06	HAZARD_03_11	High
HE_044	Any	Any	MF_06	HAZARD_03_12	High
HE_045	Any	Any	MF_06	HAZARD_03_13	High
HE_046	Any	Any	MF_06	HAZARD_03_14	High
HE_047	Any	Any	MF_06	HAZARD_03_15	High
HE_048	Any	Any	MF_06	HAZARD_03_16	High
HE_049	Any	Any	MF_06	HAZARD_03_17	High

HE_050	Any	Any	MF_06	HAZARD_03_18	High
HE_051	Any	Any	MF_06	HAZARD_03_19	High
HE_052	Any	Any	MF_06	HAZARD_03_20	High
HE_053	Any	Any	MF_06	HAZARD_03_21	High
HE_054	Any	Any	MF_06	HAZARD_03_22	High
HE_055	Any	Any	MF_06	HAZARD_03_23	High
HE_056	Any	Any	MF_06	HAZARD_03_24	High

A.1.5 ASIL determination

Assumption	Exposure: Safe margin: **E4** for Hazard_03_XX (any vehicle may provoke the situation).
	Controllability: **C3** for Hazard_03_XX(the platoon cannot control easily this situation).

The orange boxes indicate the highest ASIL determination assigned in the table.

ID	Severity	Exposure	Controllability	ASIL	Malfunction/Deviation
HE_001	S1	E3	C1	QM	Communication degrades / fails
HE_002	S1	E3	C1	QM	Inaccurate sensor inputs
HE_003	S1	E3	C1	QM	Communication degrades / fails
HE_004	S1	E3	C1	QM	Communication degrades / fails
HE_005	S2	E3	C2	A	Communication degrades / fails
HE_006	S1	E3	C1	QM	Inaccurate sensor inputs
HE_007	S1	E3	C1	QM	Inaccurate sensor inputs
HE_008	S2	E3	C2	A	Inaccurate sensor inputs
HE_009	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_010	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_011	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_012	S3	E4	C3	D	Communication degrades / fails & Cut-in
HE_013	S3	E4	C3	D	Communication degrades / fails & Cut-in
HE_014	S1	E4	C3	B	Communication degrades / fails & Cut-in

HE_015	S3	E4	C3	D	Communication degrades / fails & Cut-in
HE_016	S3	E4	C3	D	Communication degrades / fails & Cut-in
HE_017	S3	E4	C3	D	Communication degrades / fails & Cut-in
HE_018	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_019	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_020	S1	E4	C3	B	Communication degrades / fails & Cut-in
HE_021	S1	E4	C3	B	Communication degrades / fails & Acceleration
HE_022	S2	E4	C3	C	Communication degrades / fails & Acceleration
HE_023	S2	E4	C3	C	Communication degrades / fails & Acceleration
HE_024	S1	E4	C3	B	Communication degrades / fails & Acceleration
HE_025	S2	E4	C3	C	Communication degrades / fails & Acceleration
HE_026	S2	E4	C3	C	Communication degrades / fails & Acceleration
HE_027	S2	E4	C3	D	Communication degrades / fails & Emergency brake
HE_028	S2	E4	C3	D	Communication degrades / fails & Emergency brake
HE_029	S1	E4	C3	B	Communication degrades / fails & Emergency brake
HE_030	S2	E4	C3	D	Communication degrades / fails & Emergency brake
HE_031	S2	E4	C3	D	Communication degrades / fails & Emergency brake
HE_032	S1	E4	C3	B	Communication degrades / fails & Emergency brake
HE_033	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_034	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_035	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_036	S3	E4	C3	D	Inaccurate sensor inputs / fails & Cut-in
HE_037	S3	E4	C3	D	Inaccurate sensor inputs / fails & Cut-in
HE_038	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_039	S3	E4	C3	D	Inaccurate sensor inputs / fails & Cut-in
HE_040	S3	E4	C3	D	Inaccurate sensor inputs / fails & Cut-in
HE_041	S3	E4	C3	D	Inaccurate sensor inputs / fails & Cut-in
HE_042	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_043	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in

HE_044	S1	E4	C3	B	Inaccurate sensor inputs / fails & Cut-in
HE_045	S1	E4	C3	B	Inaccurate sensor inputs / fails & Acceleration
HE_046	S2	E4	C3	C	Inaccurate sensor inputs / fails & Acceleration
HE_047	S2	E4	C3	C	Inaccurate sensor inputs / fails & Acceleration
HE_048	S1	E4	C3	B	Inaccurate sensor inputs / fails & Acceleration
HE_049	S2	E4	C3	C	Inaccurate sensor inputs / fails & Acceleration
HE_050	S2	E4	C3	C	Inaccurate sensor inputs / fails & Acceleration
HE_051	S2	E4	C3	D	Inaccurate sensor inputs / fails & Emergency brake
HE_052	S2	E4	C3	D	Inaccurate sensor inputs / fails & Emergency brake
HE_053	S1	E4	C3	B	Inaccurate sensor inputs / fails & Emergency brake
HE_054	S2	E4	C3	D	Inaccurate sensor inputs / fails & Emergency brake
HE_055	S2	E4	C3	D	Inaccurate sensor inputs / fails & Emergency brake
HE_056	S1	E4	C3	B	Inaccurate sensor inputs / fails & Emergency brake

A.1.6 Safety goals

Safety goal 1 (SG1): No sudden unintended full acceleration
Safety goal 2 (SG2): No sudden unintended full braking in highway/intersection
Safety goal 3 (SG3): No fast transversal vehicle movement when not requested
Safety goal 4 (SG4): Minimize inconsistency in system state perception among all vehicles, leading to unintended action in vehicle/s

A.1.7 Prevention and detection on scenarios

ID	Malfunctioning Behavior	Prevention	Detection	Malfunction/Deviation
HE_001	MF_01	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching road obstacle: system monitoring	Communication degrades / fails
HE_002	MF_02	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Stop execution of the scenario 'X' meters before reaching road obstacle: visual monitoring	Inaccurate sensor inputs
HE_003	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Monitor how long the space gap has been created; if vehicle from Platoon A don't move to gap in 'X' seconds, then abort scenario	Communication degrades / fails
HE_004	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Monitor how long the space gap has been created; if vehicle from Platoon A don't move to gap in 'X' seconds, then abort scenario	Communication degrades / fails
HE_005	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Monitor stability of space gap; if stability is intermittent, then abort the scenario	Communication degrades / fails
HE_006	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Monitor how long the space gap has been created; if vehicle from Platoon A don't move to gap in 'X' seconds, then abort scenario	Inaccurate sensor inputs

HE_007	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Monitor how long the space gap has been created; if vehicle from Platoon A don't move to gap in 'X' seconds, then abort scenario	Inaccurate sensor inputs
HE_008	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Monitor stability of space gap; if stability is intermittent, then abort the scenario	Inaccurate sensor inputs
HE_009	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon A shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in
HE_010	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon A shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in
HE_011	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon A shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in

HE_012	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in
HE_013	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in
HE_014	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to left, only tolerances)	Communication degrades / fails & Cut-in
HE_015	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to merge' is not given)	Communication degrades / fails & Cut-in
HE_016	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to merge' is not given)	Communication degrades / fails & Cut-in

HE_017	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to merge' is not given)	Communication degrades / fails & Cut-in
HE_018	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to right, only tolerances)	Communication degrades / fails & Cut-in
HE_019	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to right, only tolerances)	Communication degrades / fails & Cut-in
HE_020	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement to right, only tolerances)	Communication degrades / fails & Cut-in
HE_021	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration

HE_022	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_023	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_024	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_025	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_026	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_027	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_028	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake

HE_029	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_030	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_031	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_032	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_033	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon A shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_034	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon A shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in

HE_035	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon A shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_036	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_037	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_038	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_039	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about lateral movement and check if this lateral movement is allowed (2) Driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to	Inaccurate sensor inputs / fails & Cut-in

			merge' is not given)	
HE_040	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about lateral movement and check if this lateral movement is allowed (2) Driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to merge' is not given)	Inaccurate sensor inputs / fails & Cut-in
HE_041	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about lateral movement and check if this lateral movement is allowed (2) Driver/passenger detection, then communicate via radio to other participants (vehicles on Platoon B shall not have lateral movement if space gap is not created and 'OK to merge' is not given)	Inaccurate sensor inputs / fails & Cut-in
HE_042	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in

HE_043	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_044	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle lateral information: vehicles on Platoon B shall not have lateral movement (only tolerances) to right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Cut-in
HE_045	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_046	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_047	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration

HE_048	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_049	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_050	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle acceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_051	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_052	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake

HE_053	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_054	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_055	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information and monitor probability of collision (via radar for example) (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_056	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about vehicle deceleration information (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake

A.2 Intersection Scenario

A.2.1 HAZOP (HAZard and Operability study)

Attribute/Parameter	Guideword	Malfunction/Deviation	Malfunction behavior on system/Consequences	Hazard	Priority	Comments
Three vehicles (two in the main road) are approaching to T-intersection shall to coordinate and collaborate to allow the V1 vehicle enter to main road.	No	Entry of the V1 on the main road is not performed due to any vehicle, no vehicle performs the properly maneuvers.	**MF_01:** Communication problem (communication degrades/fails) (vehicles don't see each other) between all the systems installed, the two vehicles on the main road (PC1 and PC2) continue normally driving and the third (V1) turns left when arrives on the intersection. **MF_02:** There is not communication problem (the vehicles coordinate and collaborate them) but none of the maneuvers have been performed in order to allow the V1 to enter the main road due to inaccurate sensor inputs or something like that.	**HAZARD_01:** The V1 cannot enter to the main road.	Low	As a safety point of view three vehicles approaching a T-intersection and they are not communicating, we consider low because the V1 cannot cause any injury accident due to the vehicle not enter on the main road according with the OBU, it doesn't receive any message from others systems. Stop the execution of the scenario if after 'X' meters to stay in the CZ there isn't communication between the vehicles of the scenario.
	More	Not Applicable				

	Less	Entry of the V1 on the main road is not performed due to some vehicle, some vehicle does not perform the properly maneuver.	**MF_03:** Communication problem (communication degrades/fails) (protocol problem source) between systems installed on different vehicles, some vehicle performs the correct maneuver, others not. **MF_04:** There is not communication problem (no protocol issues, issues on maneuver decision) but some vehicles do not perform the expected maneuver (longitudinal/turn left)*	**HAZARD_02:** It is probably that the V1 cannot enter to the main road.	Medium	As a safety point of view many situations can occur, most of them dangerous for the occupants of the vehicles. However, there are no unexpected/unintended vehicles maneuvers. Stop the execution of the scenario if after 'X' meters to stay in the CZ there isn't communication between some of the vehicles of the scenario.
	As well as	Not Applicable				
	Part of	Not Applicable				
	Reverse	Not Applicable				
	Other than	There are unintended maneuvers (emergency brake/lane change) which provoque that the V1 doesn't enter to the main road and/or an accident along to the intersection.	**MF_05:** Communication problem (communication degrades/fails) (protocol problem source) between systems installed on different vehicles, a/some vehicle/s may move unexpected. **MF_06:** There is not communication problem (no protocol issues, issues on maneuver decision) but some vehicles do not perform the expected maneuver (longitudinal/turn left)*	**HAZARD_03:** Vehicles, at some point of the intersection communication / collaboration, may go in unexpected behavior.	High	Vehicles may behave unexpected due to unintended maneuvers and, therefore, severity of that situation is high.

* Due to a malfunction of any mechanical part and/or innacurate sensor(s) input(s).

A.2.2 Situation analysis

Location	Characteristics
Country road or a street in a city	Max speed: 30 Km/h

Road conditions	Characteristics	Remarks
Paved dry road	Normal road friction	Vehicle "validation" will be done at dry road, so it's not sure whether the vehicle will behave safe in wet road conditions.
Paved wet road	Low road friction	

A.2.3 Hazard

Assumptions for hazard decomposition events:	Only one vehicle behaves unintendedly; combination of the unintended maneuvers are also possible
	Only one unintended maneuver is considered; vehicle may maneuver as a combination of longitudinal and turn left or right unintended maneuvers

ID	Description	
HAZARD_01	**HAZARD_01:** The V1 cannot enter to the main road.	
HAZARD_02	It is probably that the V1 cannot enter to the main road.	**HAZARD_02_01:** The vehicle PC1 decelerates in order to permit enter to the road the vehicle V1, but PC2 continues driving. There is not enough space. **HAZARD_02_02:** The vehicle PC2 decelerates in order to permit enter to the road the vehicle V1, but PC1 continues driving. There is not enough space. **HAZARD_02_03:** The vehicles PC1 and PC2 decelerate but V1 not enter to the main road.
HAZARD_03	Vehicles, at some point of the intersection communication / collaboration, may go in unexpected behavior.	**See below table for different HAZARD situations**

Unintended maneuver / Vehicle Position	Vehicle PC1	Vehicle PC2	Vehicle V1
Acceleration	HAZARD_03_01	HAZARD_03_02	HAZARD_03_03
Deceleration	HAZARD_03_04	HAZARD_03_05	HAZARD_03_06
Turn left	HAZARD_03_07	HAZARD_03_08	HAZARD_03_09
Turn right	HAZARD_03_10	HAZARD_03_11	HAZARD_03_12

A.2.4 Hazard events

ID	Location	Road conditions	Malfunctioning Behaviour	Hazard	Priority
HE_001	Any	Any	MF_01	HAZARD_01	Low
HE_002	Any	Any	MF_02	HAZARD_01	Low
HE_003	Any	Any	MF_03	HAZARD_02_01	Medium
HE_004	Any	Any	MF_03	HAZARD_02_02	Medium
HE_005	Any	Any	MF_03	HAZARD_02_03	Medium
HE_006	Any	Any	MF_04	HAZARD_02_01	Medium
HE_007	Any	Any	MF_04	HAZARD_02_02	Medium
HE_008	Any	Any	MF_04	HAZARD_02_03	Medium
HE_009	Any	Any	MF_05	HAZARD_03_01	High
HE_010	Any	Any	MF_05	HAZARD_03_02	High
HE_011	Any	Any	MF_05	HAZARD_03_03	High
HE_012	Any	Any	MF_05	HAZARD_03_04	Low
HE_013	Any	Any	MF_05	HAZARD_03_05	Low
HE_014	Any	Any	MF_05	HAZARD_03_06	High
HE_015	Any	Any	MF_05	HAZARD_03_07	High
HE_016	Any	Any	MF_05	HAZARD_03_08	High
HE_017	Any	Any	MF_05	HAZARD_03_09	High
HE_018	Any	Any	MF_05	HAZARD_03_10	Medium

HE_019	Any	Any	MF_05	HAZARD_03_11	Medium
HE_020	Any	Any	MF_05	HAZARD_03_12	High
HE_021	Any	Any	MF_06	HAZARD_03_01	High
HE_022	Any	Any	MF_06	HAZARD_03_02	High
HE_023	Any	Any	MF_06	HAZARD_03_03	High
HE_024	Any	Any	MF_06	HAZARD_03_04	Low
HE_025	Any	Any	MF_06	HAZARD_03_05	Low
HE_026	Any	Any	MF_06	HAZARD_03_06	High
HE_027	Any	Any	MF_06	HAZARD_03_07	High
HE_028	Any	Any	MF_06	HAZARD_03_08	High
HE_029	Any	Any	MF_06	HAZARD_03_09	High
HE_030	Any	Any	MF_06	HAZARD_03_10	Medium
HE_031	Any	Any	MF_06	HAZARD_03_11	Medium
HE_032	Any	Any	MF_06	HAZARD_03_12	High

A.2.5 ASIL determination

Assumption	Exposure: Safe margin: **E4** for Hazard_03_XX (any vehicle may provoke the situation).
	Controllability: **C3** for Hazard_03_XX(the platoon cannot control easily this situation).

The orange boxes indicate the highest ASIL determination assigned in the table.

ID	Severity	Exposure	Controllability	ASIL	Malfunction/Deviation
HE_001	S1	E3	C1	QM	Communication degrades / fails
HE_002	S1	E3	C1	QM	Inaccurate sensor inputs
HE_003	S2	E3	C2	A	Communication degrades / fails
HE_004	S2	E3	C2	A	Communication degrades / fails
HE_005	S1	E3	C2	QM	Communication degrades / fails
HE_006	S2	E3	C2	A	Inaccurate sensor inputs

HE_007	S2	E3	C2	A	Inaccurate sensor inputs
HE_008	S1	E3	C2	QM	Inaccurate sensor inputs
HE_009	S2	E3	C3	B	Communication degrades / fails & Acceleration
HE_010	S2	E3	C3	B	Communication degrades / fails & Acceleration
HE_011	S2	E3	C3	B	Communication degrades / fails & Acceleration
HE_012	S1	E2	C3	QM	Communication degrades / fails & Emergency brake
HE_013	S1	E2	C3	QM	Communication degrades / fails & Emergency brake
HE_014	S2	E3	C3	B	Communication degrades / fails & Emergency brake
HE_015	S2	E3	C3	B	Communication degrades / fails & Lane change
HE_016	S2	E3	C3	B	Communication degrades / fails & Lane change
HE_017	S2	E3	C3	B	Communication degrades / fails & Lane change
HE_018	S1	E3	C3	A	Communication degrades / fails & Lane change
HE_019	S1	E3	C3	A	Communication degrades / fails & Lane change
HE_020	S2	E3	C3	A	Communication degrades / fails & Lane change
HE_021	S2	E3	C3	B	Inaccurate sensor inputs / fails & Acceleration
HE_022	S2	E3	C3	B	Inaccurate sensor inputs / fails & Acceleration
HE_023	S2	E3	C3	B	Inaccurate sensor inputs / fails & Acceleration
HE_024	S1	E2	C3	QM	Inaccurate sensor inputs / fails & Emergency brake
HE_025	S1	E2	C3	QM	Inaccurate sensor inputs / fails & Emergency brake
HE_026	S2	E3	C3	B	Inaccurate sensor inputs / fails & Emergency brake
HE_027	S2	E3	C3	B	Inaccurate sensor inputs / fails & Lane change
HE_028	S2	E3	C3	B	Inaccurate sensor inputs / fails & Lane change
HE_029	S2	E3	C3	B	Inaccurate sensor inputs / fails & Lane change
HE_030	S1	E3	C3	A	Inaccurate sensor inputs / fails & Lane change
HE_031	S1	E3	C3	A	Inaccurate sensor inputs / fails & Lane change
HE_032	S2	E3	C3	A	Inaccurate sensor inputs / fails & Lane change

A.2.6 Safety goals

Safety goal 1 (SG1): No sudden unintended full acceleration
Safety goal 2 (SG2): No sudden unintended full braking in highway/intersection
Safety goal 3 (SG3): No fast transversal vehicle movement when not requested
Safety goal 4 (SG4): Minimize inconsistency in system state perception among all vehicles, leading to unintended action in vehicle/s

A.2.7 Prevention and detection on scenarios

ID	Malfunctioning Behavior	Prevention	Detection	Malfunction/Deviation
HE_001	MF_01	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario after 'X' meters to stay in the CZ: system monitoring	Communication degrades / fails
HE_002	MF_02	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Stop execution of the scenario after 'X' meters to stay in the CZ: visual monitoring	Inaccurate sensor inputs
HE_003	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario after 'X' meters to stay in the CZ: system monitoring	Communication degrades / fails
HE_004	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario after 'X' meters to stay in the CZ: system monitoring	Communication degrades / fails
HE_005	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario after 'X' meters to stay in the CZ: system monitoring	Communication degrades / fails

HE_006	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Stop execution of the scenario after 'X' meters to stay in the CZ: visual monitoring	Inaccurate sensor inputs
HE_007	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Stop execution of the scenario after 'X' meters to stay in the CZ: visual monitoring	Inaccurate sensor inputs
HE_008	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	Stop execution of the scenario after 'X' meters to stay in the CZ: visual monitoring	Inaccurate sensor inputs
HE_009	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_010	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration

HE_011	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Acceleration
HE_012	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_013	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_014	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Emergency brake
HE_015	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change
HE_016	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change
HE_017	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change

HE_018	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change
HE_019	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change
HE_020	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Communication degrades / fails & Lane change
HE_021	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC1: unintended acceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_022	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC2: unintended acceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration
HE_023	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in	(1) Monitor message about V1: unintended acceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Acceleration

		charge of making maneuver decisions.		
HE_024	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC1: unintended deceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_025	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC2: unintended deceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_026	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about V1: unintended deceleration (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Emergency brake
HE_027	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC1: unintended turn left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change

HE_028	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC2: unintended turn left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change
HE_029	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about V1: unintended turn left (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change
HE_030	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC1: unintended turn right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change
HE_031	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about PC2: unintended turn right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change
HE_032	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the control unit which is in charge of making maneuver decisions.	(1) Monitor message about V1: unintended turn right (2) Driver/passenger detection, then communicate via radio to other participants (this could be add on participants rules)	Inaccurate sensor inputs / fails & Lane change

A.3 Emergency Vehicle Scenario (Demonstrator)

A.3.1 HAZOP (HAZard and Operability study)

Attribute/Parameter	Guideword	Malfunction/Deviation	Malfunction behavior on system/Consequences	Hazard	Priority	Comments
The vehicles from two different lanes make room in order to the EV can pass between them.	No	The EV cannot pass between the other vehicles of the road.	**MF_01:** Communication problem (communication degrades/fails) (vehicles don't see the EV) between all the systems installed, the vehicles continue driving by their lane. **MF_02:** There is not communication problem (vehicles see the EV) but none of the maneuvers have been performed.	**HAZARD_01:** The EV cannot pass between the other vehicles of the road.	Low	As a safety point of view the EV trying pass between the other vehicles of the road is not initiated at all. We consider 'low' because the system is not working and it can be identified 'easily' (stop execution of the scenario 'X' meters before reaching to the last vehicles of the road: visual monitoring).
	More	Not Applicable				
	Less	The EV cannot pass between all the other vehicles of the road, only some of them.	**MF_03:** Communication problem (communication degrades/fails)(protocol problem source) between systems installed on different vehicles, some vehicle performs the correct maneuver, others not. **MF_04:** There is not communication problem (no protocol issues, issues on maneuver decision) but some vehicles do not perform the expected maneuver (lateral left / lateral right)	**HAZARD_02:** It is highly probably that the EV cannot pass between the other vehicles of the road.	Medium	As a safety point of view many situations can occur, most of them dangerous for the occupants of the vehicles. However, there are no unexpected/unintended vehicles maneuvers.
	As well as	Not Applicable				

	Part of	Not Applicable				
	Reverse	Not Applicable				
	Other than	There are unintended maneuvers which provoque that the EV doesn't pass between the other vehicles of the road.	**MF_05:** Communication problem (protocol problem source) between systems installed on different vehicles, a/some vehicle/s may move unexpected. **MF_06:** There is not communication problem (no protocol issues, issues on maneuver decision) but some vehicles do not perform the expected maneuver (lateral left / lateral right)	**HAZARD_03:** Vehicles, at some point of permission to EV to pass between them may go in unexpected behavior.	High	Vehicles may behave unexpected due to unintended maneuvers and, therefore, severity of that situation is high.

A.3.2 Situation analysis

Location	Characteristics
Country road or a street in a city	EV: Max speed: 80 Km/h Other vehicles: Max speed: 50 Km/h

Road conditions	Characteristics	Remarks
Paved dry road	Normal road friction	Vehicle "validation" will be done at dry road, so it's not sure whether the vehicle will behave safe in wet road conditions.
Paved wet road	Low road friction	

A.3.3 Hazard

Assumptions for hazard decomposition events:	Only one vehicle behaves unintendedly; combination of the unintended maneuvers are also possible
	Only one unintended maneuver is considered; vehicle may maneuver as a combination of longitudinal and turn left or right unintended maneuvers

ID	Description	
HAZARD_01	**HAZARD_01:** The EV cannot pass between the other vehicles of the road.	
HAZARD_02	It is highly probably that the EV cannot pass between the other vehicles of the road.	**HAZARD_02_01:** Only the vehicles from the left lane receive the signal from the EV and send the message forward to other vehicles. **HAZARD_02_02:** Only the vehicles from the right lane receive the signal from the EV and send the messages forward o other vehicles. **HAZARD_02_03:** Only some vehicles have received the signal. **HAZARD_02_04:** All vehicles receive the signal from the EV but none of them performs none maneuver.
HAZARD_03	Vehicles, at some point of permission to EV to pass between them may go in unexpected behavior.	**See below table for different HAZARD situations**

Unintented maneuver / Vehicle Position	Last Vehicle Lane A	Middle or Head Vehicle Lane A	Last Vehicle Lane B	Middle or Head Vehicle Lane B
Lateral left	HAZARD_03_01	HAZARD_03_02	HAZARD_03_03	HAZARD_03_04
Lateral right	HAZARD_03_05	HAZARD_03_06	HAZARD_03_07	HAZARD_03_08

A.3.4 Hazard events

ID	Location	Road conditions	Malfunctioning Behavior	Hazard	Priority
HE_001	Any	Any	MF_01	HAZARD_01	Low
HE_002	Any	Any	MF_02	HAZARD_01	Low
HE_003	Any	Any	MF_03	HAZARD_02_01	Medium
HE_004	Any	Any	MF_03	HAZARD_02_02	Medium
HE_005	Any	Any	MF_03	HAZARD_02_03	Medium
HE_006	Any	Any	MF_03	HAZARD_02_04	Medium
HE_007	Any	Any	MF_04	HAZARD_02_01	Medium
HE_008	Any	Any	MF_04	HAZARD_02_02	Medium

HE_009	Any	Any	MF_04	HAZARD_02_03	Medium
HE_010	Any	Any	MF_04	HAZARD_02_04	Medium
HE_011	Any	Any	MF_05	HAZARD_03_01	High
HE_012	Any	Any	MF_05	HAZARD_03_02	High
HE_013	Any	Any	MF_05	HAZARD_03_03	High
HE_014	Any	Any	MF_05	HAZARD_03_04	High
HE_015	Any	Any	MF_05	HAZARD_03_05	High
HE_016	Any	Any	MF_05	HAZARD_03_06	High
HE_017	Any	Any	MF_05	HAZARD_03_07	High
HE_018	Any	Any	MF_05	HAZARD_03_08	High
HE_019	Any	Any	MF_06	HAZARD_03_01	High
HE_020	Any	Any	MF_06	HAZARD_03_02	High
HE_021	Any	Any	MF_06	HAZARD_03_03	High
HE_022	Any	Any	MF_06	HAZARD_03_04	High
HE_023	Any	Any	MF_06	HAZARD_03_05	High
HE_024	Any	Any	MF_06	HAZARD_03_06	High
HE_025	Any	Any	MF_06	HAZARD_03_07	High
HE_026	Any	Any	MF_06	HAZARD_03_08	High

A.3.5 ASIL determination

Assumption	Exposure: Safe margin: **E4** for Hazard_03_XX (any vehicle may provoke the situation).
	Controllability: **C3** for Hazard_03_XX (the platoon cannot control easily this situation).

The orange boxes indicate the highest ASIL determination assigned in the table.

ID	Severity	Exposure	Controllability	ASIL	Malfunction/Deviation
HE_001	S1	E3	C2	QM	Communication degrades / fails
HE_002	S1	E3	C2	QM	Others

HE_003	S2	E3	C2	A	Communication degrades / fails
HE_004	S2	E3	C2	A	Communication degrades / fails
HE_005	S2	E3	C2	A	Communication degrades / fails
HE_006	S2	E3	C2	A	Communication degrades / fails
HE_007	S2	E3	C2	A	Others
HE_008	S2	E3	C2	A	Others
HE_009	S2	E3	C2	A	Others
HE_010	S2	E3	C2	A	Others
HE_011	S2	E3	C3	B	Communication degrades / fails
HE_012	S2	E3	C3	B	Communication degrades / fails
HE_013	S3	E3	C3	C	Communication degrades / fails
HE_014	S3	E3	C3	C	Communication degrades / fails
HE_015	S3	E3	C3	C	Communication degrades / fails
HE_016	S3	E3	C3	C	Communication degrades / fails
HE_017	S2	E3	C3	B	Communication degrades / fails
HE_018	S2	E3	C3	B	Communication degrades / fails
HE_019	S2	E3	C3	B	Others
HE_020	S2	E3	C3	B	Others
HE_021	S3	E3	C3	C	Others
HE_022	S3	E3	C3	C	Others
HE_023	S3	E3	C3	C	Others
HE_024	S3	E3	C3	C	Others
HE_025	S2	E3	C3	B	Others
HE_026	S2	E3	C3	B	Others

A.3.6 Safety goals

Safety goal 1 (SG1): No sudden unintended full acceleration

Safety goal 2 (SG2): No sudden unintended full braking in highway/intersection
Safety goal 3 (SG3): No fast transversal vehicle movement when not requested
Safety goal 4 (SG4): Minimize inconsistency in system state perception among all vehicles, leading to unintended action in vehicle/s

A.3.7 Prevention and detection on scenarios

ID	Malfunctioning Behavior	Prevention	Detection	Malfunction/Deviation
HE_001	MF_01	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_002	MF_02	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_003	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_004	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_005	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_006	MF_03	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails

HE_007	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_008	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_009	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_010	MF_04	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_011	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_012	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_013	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails

HE_014	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_015	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_016	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_017	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_018	MF_05	Qualify vehicle from communication point of view: design a robust test plan (normal mode and failure mode)	Stop execution of the scenario 'X' meters before reaching the last vehicles of the lanes visual monitoring	Communication degrades / fails
HE_019	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_020	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_021	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others

HE_022	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_023	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_024	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_025	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others
HE_026	MF_06	Vehicle will be qualified through different scenarios at workshops (some maneuvers will be executed, we request teams to present a complete functional check (and vehicle states in case of failure) for the manual control of the vehicle.	Since there is a malfunction on communications, we shall look for another detection mechanism: we may probably rely on driver/passenger detection, then communicate via radio to other participants	Others