5GAA Automotive Association

Safety Treatment in Connected and Autonomous Driving Functions Report

5GAA Automotive Association
Technichal Reporrt

CONTACT INFORMATION:

Lead Coordinator – Thomas Linget
Email: thomas.linget@5gaa.org

MAILING ADDRESS:

5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	0.93
DATE OF PUBLICATION:	9.12.2019
DOCUMENT TYPE:	Technichal report
CONFIDENTIALITY CLASS:	P (Public use)
REFERENCE 5GAA WORKING GROUP:	Working Group 2
DATE OF APPROVAL BY 5GAA BOARD:	09.03.2021

1 Contents

Foreword

This Technical Report has been produced by 5GAA.

The contents of the present document are subject to continuing work within the Working Groups (WG) and may change following formal WG approval. Should the WG modify the contents of the present document, it will be re-released by the WG with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

(1) This numbering system has six logical elements:

(a) x: a single letter corresponding to the working group:

Where x =

T (Use cases and Technical Requirements)

A (System Architecture and Solution Development)

P (Evaluation, Testbed and Pilots)

S (Standards and Spectrum)

B (Business Models and Go-To-Market Strategies)

(b) nn: two digits to indicate the year. i.e. ,17,18 19, etc

(c) zzzz: unique number of the document

(2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version

(3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

Introduction

This TR documents the findings of the 5GAA STiCAD cross-work item. The purpose of the STiCAD work item has been to determine, propose and evaluate possibilities for telecommunication operators, vendors, and any further identified stakeholders to provide what is necessary in order to enable the car original equipment manufacturers (OEMs) to better treat safety for the new use cases enabled by vehicle-to-anything (V2X) technologies. These new use cases represent scenarios beyond what is handled in the ISO 26262 standard, which assumes that the functional safety approach is limited to a single vehicle and does not consider vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. To achieve this, it was decided to find representative safety requirements for two selected use cases.

The use cases considered are:

- V2N Tele-operated Driving
- V2V Emergency Brake Warning

For each of these use cases there are a number of steps which need to be performed to achieve the required safety treatment.

The approach that has been adopted is to follow the steps outlined in ISO 26262 [1]. These steps are:

- Produce an Item Definition
- Perform an Hazard and Risk Analysis
- Determine Functional Safety Goals

Next steps then include:

- Determine a set of Potential Functional Safety Requirements
- Determine a potential set of solutions to meet the most preferred Potential Functional Safety Requirements
- Determine any changes in standards needed, or other industry level agreements that may be required in order to achieve the Functional Safety Goals

1 Scope

This Technical Report documents the findings of the 5GAA STiCAD cross-work item. The purpose of the STiCAD work item has been to determine, propose and evaluate possibilities for telecommunication operators, vendors, and any further identified stakeholders to provide what is necessary in order to enable the car OEM to better treat safety for systems that exist beyond a single vehicle. To achieve this, it was decided to find representative safety requirements for two selected use cases that cover the V2X scenarios of direct communication and network-based information delivery.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific
- For a specific reference, subsequent revisions do not apply
- For a non-specific reference, the latest version applies

[1] ISO 26262-3 ‘Road vehicles – Functional Safety – Part 3: Concept phase’, First edition 2018-12

[2] ETSI TS 102 637-1 v1.1.1. (2010-09) ‘ITS, Vehicular comms, basic set of applications, Part 1: Functional Requirements’

[3] SAE J2945/1, ‘On-board system requirements for V2V safety communications’, 1 March 2016

[4] 5GAA Tdoc T-180234, ‘Emergency Brake Warning’, Ford, Continental, 5GAA WG1, Conf Call #30, 20 November 2018

[5] ETSI EN 302 637-3 v1.3.1 (2019-04), ‘ITS Vehicular communications, basic set of applications, Part 3: Specifications of Decentralised Environmental Notification Basic Service’

[6] ETSI TS 102 894-2 (2018-08) ‘ITS, Users and applications requirements; Part 2: Applications and facilities layer common data dictionary’

[7] 5GAA TR T-180014 ‘Working group use cases and technical requirements; Day one safety use cases, interim status V3.0’ (Board approved document), 27 February 2018

[8] 5GAA TR T-180014, ‘Working group use cases and technical requirements; Day one safety use cases; Interims status – V3.0’, 27 February 2018

[9] SAE J3016 ‘Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles’

[10] SAE J2735, ‘Dedicated Short Range Communications (DSRC) message set dictionary’, March 2016

[11] ETSI TS 101 539-1 (2013-08) ‘ITS, V2X Applications, Part 1: Road Hazard Signalling (RHS) application requirements specification

[12] SAE J2980, ‘R – Considerations for ISO 26262 ASIL Hazard Classification’, April 2018

[13] ‘Item definition for Emergency Brake Warning V2V use case’, BlackBerry, 11-13 November 2019, Torino, Italy

[14] 'Deliverable D1.1: Use cases, requirements, Performance Evaluation Criteria', Convex project, Version 1.1, 5 October 2017

[15] 'The issue of observance of safe following distance between vehicles in Germany', L. Zemanek, J. Prnka, European scientific journal, August 2015

[16] 'Road traffic estimates: Great Britain 2018', UK Department of Transport, 14 May 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808555/road-traffic-estimates-in-great-britain-2018.pdf

[17] 'Brake response of unsuspecting drivers to high mounted brake lights', Sivak N. et al, Proceedings of human factors society – 24th annual meeting – 1980

[18] 'Field validation of taillights – Report on Phase 1: Pilot testing', Alexandria, Virginia, Prepared for NHTSA, US DoT contract, DOT-HS-7-01756

[19] 'How long does it take to stop? Methodological analysis of driver perception-brake times', Marc Green, Transportation human factors, 2(3), 195-216, 2000

[20] 'Vehicle stopping distance and time', NACTO, https://nacto.org/docs/usdg/vehicle_stopping_distance_and_time_upenn.pdf

[21] 'SUVs account for almost a third of cars on UK roads', https://www.fleetnews.co.uk/news/manufacturer-news/2018/04/16/suvs-account-for-almost-a-third-of-cars-on-uk-roads, 16 April 2018

[22] See file SPE0111, for 2018, https://www.gov.uk/government/statistical-data-sets/vehicle-speed-compliance-statistics-data-tables-spe; UK Government

[23] 'V2X functional and performance test report; Test procedures and results', 5GAA P-190033

[24] 'What's really behind rear-end highway crashes?', University of Minnesota, June 2017, http://www.cts.umn.edu/publications/catalyst/2017/june/highway-crashes

[25] I. Chatterjee, 'Understanding driver contributions to rear-end crashes on congested freeways and their implications for future safety measures', PhD thesis, April 2016

[26] 'Distance behaviour of motorways with regard to active safety – A comparison between adaptive cruise control (ACC) and driver', B. Filzek, B. Breuer, Automotive Engineering dept, Darmstadt University of Technology

[27] 5GAA TR T-180205, Cross Working Group Work Item Tele-Operated Driving ToD Use Cases and technical requirements, 15 July 2020

[28] ISO 26262-6:2018, 'Road vehicles – Functional safety – Part 6: Product development at the software level', 2nd edition

[29] ISO 26262-5:2018, 'Road vehicles – Functional safety – Part 5: Product development at the hardware level', 2nd edition

[30] 'SeVeCom (Secure Vehicular Communication)', EU-funded project, https://sevecom.eu/

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABS	Anti-lock Braking System
ACC	Automatic Cruise Control

AEB	Autonomous Emergency Braking
AF	Application Functions
ALK	Automatic Lane Keeping
AS	Application Server
ASIL	Automotive Safety Integrity Level
AT	Attention
CAM	Cooperative Awareness Message
CC	Control Centre
CN	Core Network
CPM	Collective Perception Message
CV	Controlled Vehicle
DENM	Decentralised Environmental Notification Message
EBW	Emergency Brake Warning
ECU	Electronic Control Unit
EEBL	Emergency Electronic Brake Light
FMEA	Failure Mode and Effect Analysis
FFS	For Further Study
HARA	Hazard And Risk Assessment
HAZOP	HAZard and OPerability study
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
MA	Misbehaviour Authority
MBIM	Mobile Broadband Interface Model
MBR	Misbehaviour Report
MCM	Manoeuvre Control Messages
MNO	Mobile Network Operator
MSM	Mobile Station Modem
NAS	Non-Access Stratum
NAT	Network Address Translation
NB	Northbound
NoC	Network operating Centre
ODD	Operational Design Domain
OS	Operating System
PFSR	Potential Functional Safety Requirements
RAN	Radio Access Network
RHW	Road Hazard Warning
RRS	Radio Resource Control
RS	Roadside Station
RxV	Vehicle that receives the EBW V2V message
SCMS	Security Credential Management System
TxV	Vehicle that transmits the EBW V2V message
UDP	User Datagram Protocol
UE	User Equipment
TCP	Transmission Control Protocol
ToD	Tele-operated Driving
VCC	Vehicle Control Centre

4 Tele-operated Driving V2N Use Case

4.1 Item Definition

This use case represents a scenario where information is exchanged between two end points (in the specific case a Network operating Centre, NoC, and a vehicle) through a telecommunication network.

In this section the items that make up Tele-operated Driving (ToD) from a safety point of view are defined. The aspects considered in describing the item are those provided in [4] (ISO 26262 Part 3) Section 5.

4.1.1 Legal requirements, national and international standards

- Different variants of the ToD use case are described in the first technical report of the 5GAA cross work item 'Tele-operated Driving' (see [27]).

At the time of writing, being there are no known standardisations for the ToD use case. However, there are discussions ongoing at different bodies (e.g. SAE) about needs for standardisation both on the technical as well as the legal and operational sides.

There are some commercial and pre-commercial products existing on the market (e.g. which mainly use proprietary implementations and interfaces. A list of existing solutions can also be found in [27].

Legal requirements are out of scope of this document and might be a potential issue for future work in 5GAA.

4.1.2 The required quality, performance and availability of the functionality, if applicable

An indication of non-functional requirements that may be adequate for our purposes is provided in the 5GAA ToD use case description provided by BMW, in [27]. This information provides non-functional requirements for different variants of ToD.

4.1.3 Potential consequences of behavioural shortfalls including known failure modes and hazards

No potential consequences, shortfalls or failure modes have so far been identified (we will leave this to the risk and hazard analysis phase of our work, as shown in Chapters 4.3 and 4.4).

4.1.4 Capabilities of actuators, or their assumed capabilities

Here, we would like to highlight several important assumptions:

- That there is a partly or fully autonomous driving capable vehicle which is temporarily able to be controlled by a tele-operator
- That the tele-operator has the means (actuators like steering wheel, pedals) to operate the aforementioned vehicle remotely
- That the remotely operated vehicle has sensors whose data can be made accessible to the tele-operator and provide the him/her the information needed to operate the vehicle in a safe way
- That the clocks of remotely operated vehicle sensors and the tele-operator are synchronised, and the sensor data contains the timestamp information allowing the tele-operator to justify/validate the sensor data

4.1.5 Purpose and functionality including operating modes and states

The ToD can be executed in many different operation modes. Due to the extensive list, this exercise does not intend to cover all possible operation implementations. Instead, it demonstrates the modes of operation that require/impose conceptionally different aspects with respect to safety considerations.

4.1.5.1 Direct control of the vehicle from the vehicle control centre

The term 'direct control' indicates that the vehicle is fully controlled by the tele-operator in the vehicle control centre (VCC). In other words, the tele-operator has the means to steer, accelerate and decelerate the vehicle (e.g. a steering wheel that directly affects the angle of the wheels of the car and pedals that directly influence the acceleration or deceleration of the vehicle). The tele-operator mainly responds to information he/she receives from the vehicle sensors via radio communication (e.g. video, radar, Lidar, ultrasonic, audio). There might be some kind of 'direct control' support from the vehicle systems (e.g. the vehicle could overrule commands coming from the tele-operator based on its own sensors and functions, e.g. braking immediately in critical situations). Details of this interaction are part of the detailed safety concepts generated for the different operation modes.

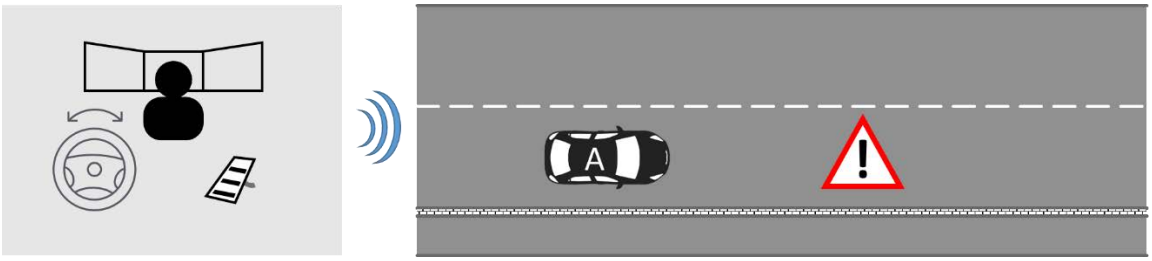

Figure 4-1: ToD direct control

4.1.5.2 Indirect control of the vehicle from the vehicle control centre

Unlike the previous scenario, the ‘indirect mode’ provides no the means for tele-operators to directly control the vehicle’s actuators. In this mode, the vehicle continues using its autonomous driving features. However, the tele-operator helps to overcome situations that cannot be resolved by the vehicles autonomous driving system. Examples of such situations might be blocked roads, known to the autonomous car’s driving system that demand support from the tele-operator who provides alternative driving trajectories (e.g. allows the automated vehicle to drive on the pavement to cross a blocked road). Another situation might be the detection of an obstacle by the vehicle sensors that the system cannot safely classify as non-critical (e.g. a bag lying on the street cannot be safely differentiated from a person by the ‘classifiers’ in the camera sensors), but a human in the VCC can make this distinction and overrule the autonomous car, allowing it to drive over the obstacle. There might be also a variant which takes input from roadside equipment (e.g. cameras) for the remote operator to better judge a certain situation and choose the right actions.

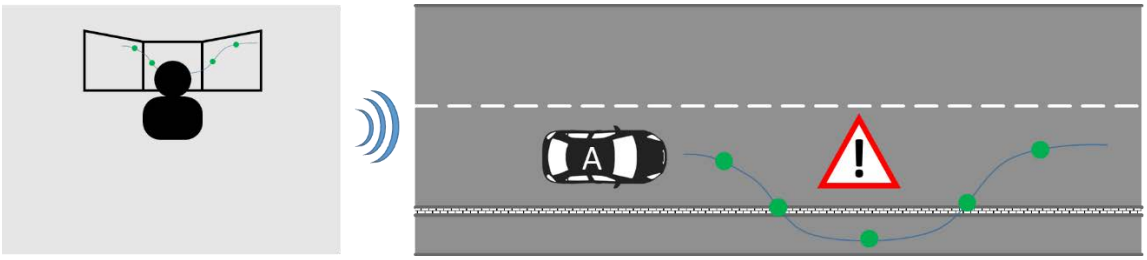

Figure 4-2 ToD indirect control

4.1.6 Elements of the item

The following provides an overview of the overall functional system architecture and serves as a basis for the detailed consideration of the items in subsequent sub-chapters elaborating on direct and indirect control.

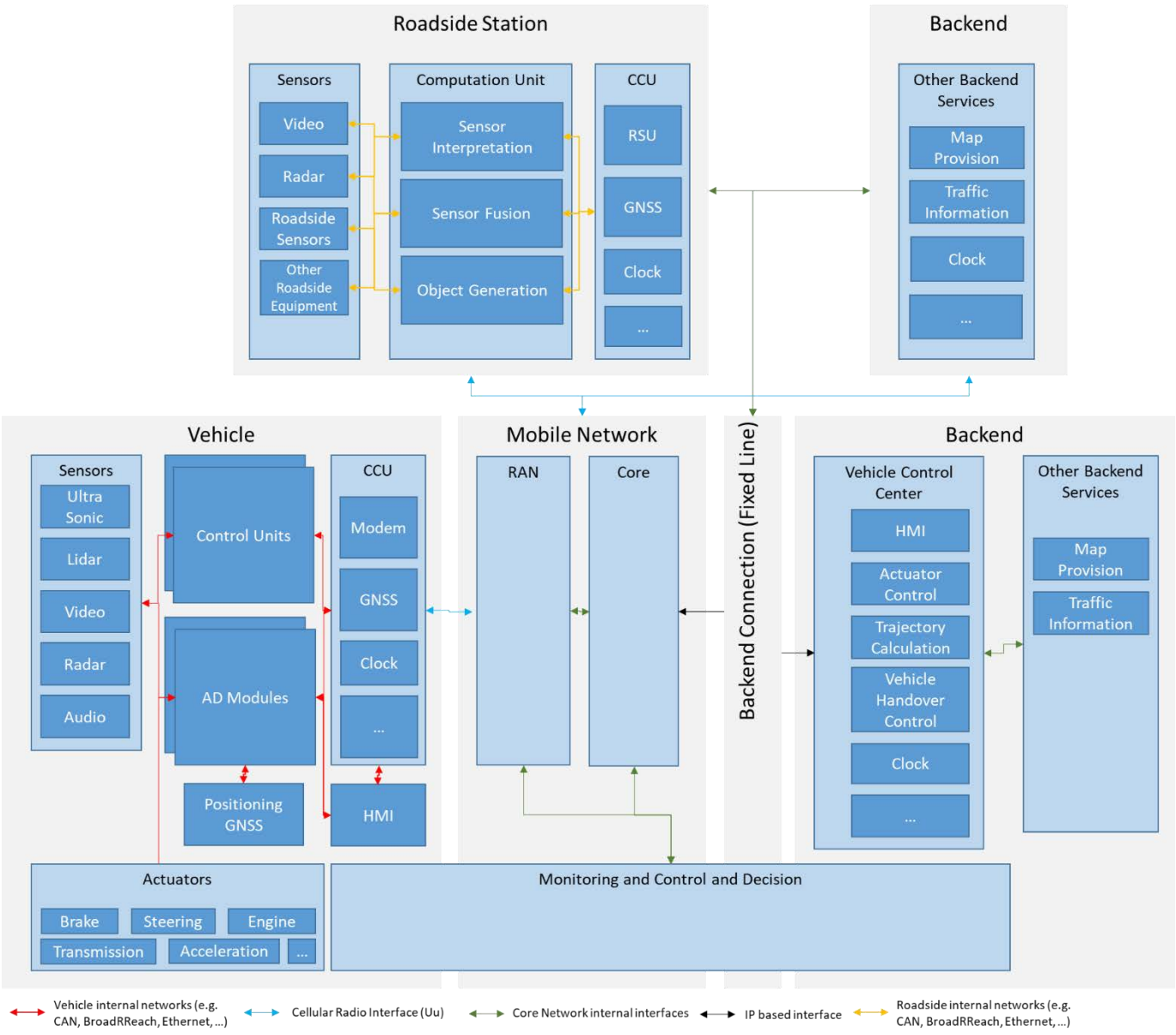

Figure 4-3: ToD overview on architecture items

4.1.6.1 Direct control of the vehicle from the vehicle control centre

In the direct control mode the AD modules of the vehicle might not be involved in the operation and thus will not be part of the items in scope. On the VCC side the trajectory control functions are likely not part of the function and thus will not be part of the item consideration. The involved items thus could be as shown in the following picture in blue.

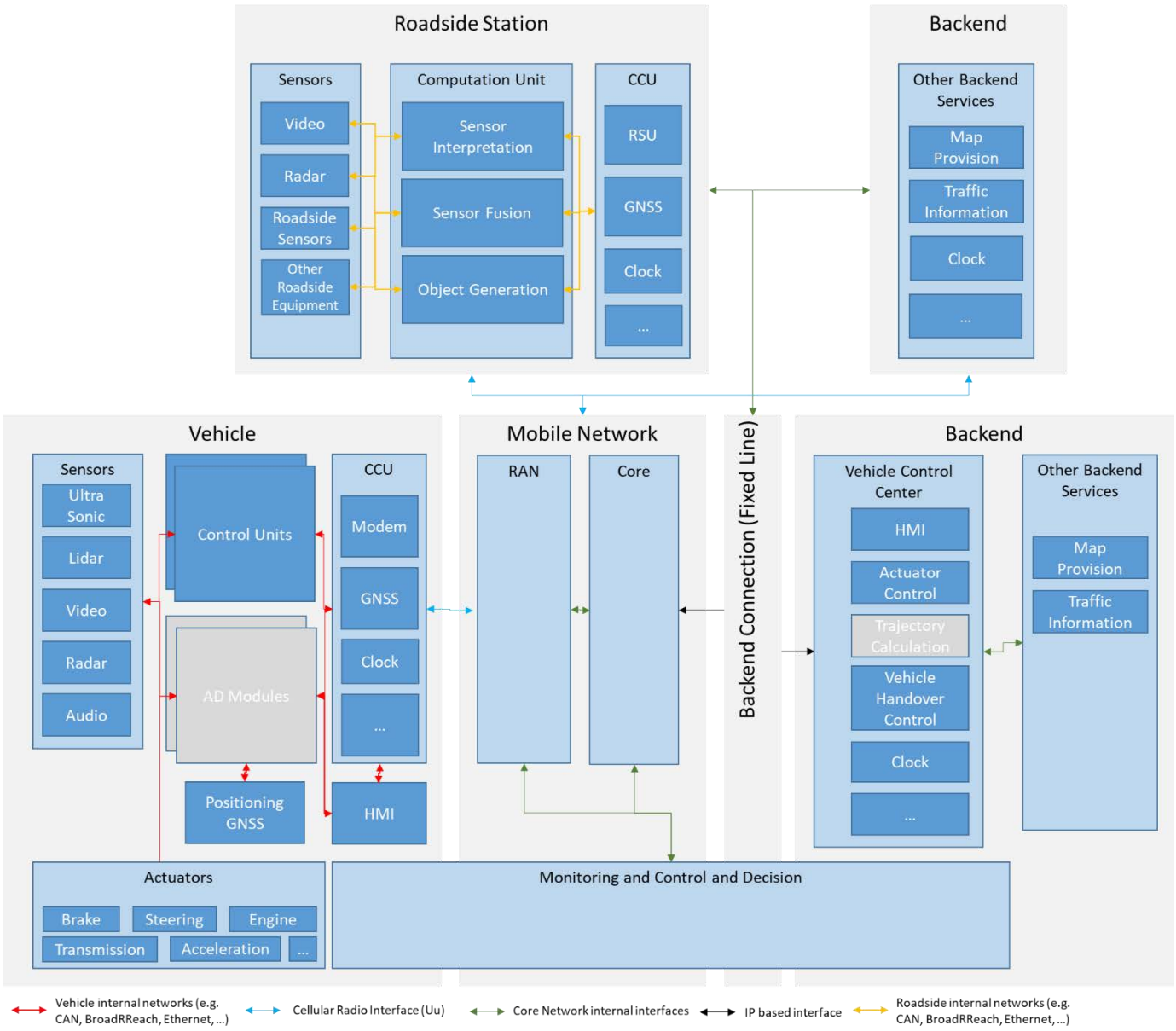

Figure 4-4: ToD direct control items

4.1.6.2 Indirect control of the vehicle from the vehicle control centre

In the indirect mode of operation, the actuators are likely not part of the safety consideration if we assume that the autonomous driving part is treated as being outside the safety analysis done here. Also on the VCC side, the actuator control and the actuator HMI is not part of the consideration, as there is no direct actuator usage. The items involved thus could be as shown in the following figure (in blue).

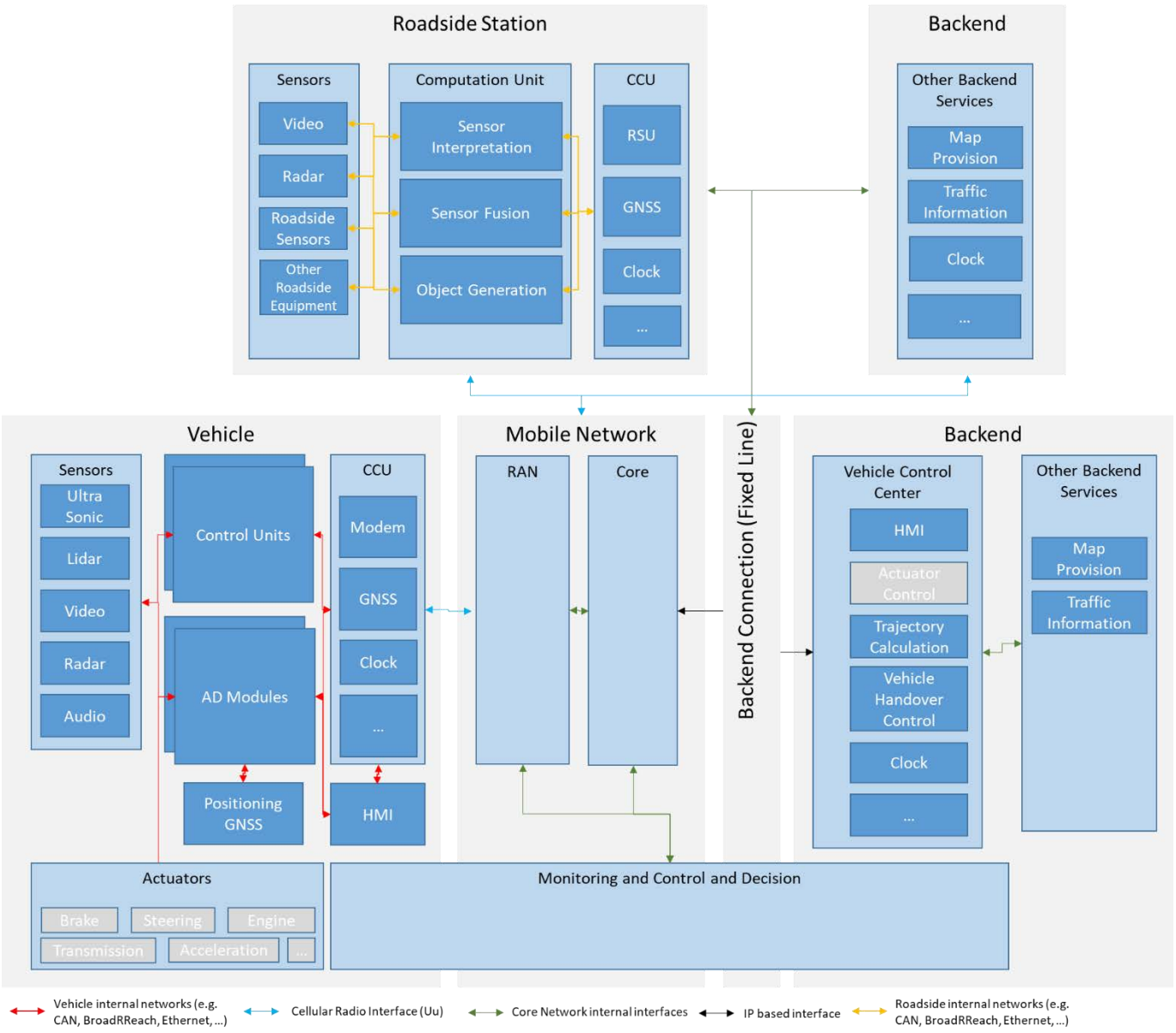

Figure 4-5: ToD indirect control items

4.2 Operational and Environmental Constraints

The following passage defines in detail the constraints with respect to operation of the functions and the environmental conditions to be taken into account.

For safety considerations relating to a certain function, it is important to define the so-called Operational Design Domain (ODD). The ODD defines conditions and constraints under which the considered function is intended to work in a safe manner. The ODD considers different types or classes of defined conditions, limitations and circumstances (e.g. on which type of roads the function will be allowed to work or under which weather conditions it might be used). As part of the safety concept, the underlying system providing the function needs to be able to safely detect, at any time, whether the conditions defining the ODD are met or not. If conditions are met, the function is allowed to be active and vice versa. If the system leaves the ODD, while being active, the respective actions defined in the safety concept (e.g. safe stop) need to be safely performed. There might also be a variant which takes input from roadside equipment (e.g. cameras) to help the remote operator better judge a certain situation and choose the right actions.

4.3 Hazard and Risk Analysis

A full and complete Hazard and Risk Analysis for the ToD use case is not intended here and would go beyond the scope of this document. Instead, some considerations are presented in order to find representative hazards that could provide a first view on the possible Automotive Safety Integrity Level (ASIL) to be considered.

4.3.1 Operational situation

The following figure provides an overview of different possible classes serving as a definition of the ODD for ToD. There will be different ODD definitions for the two operation modes previously outlined.

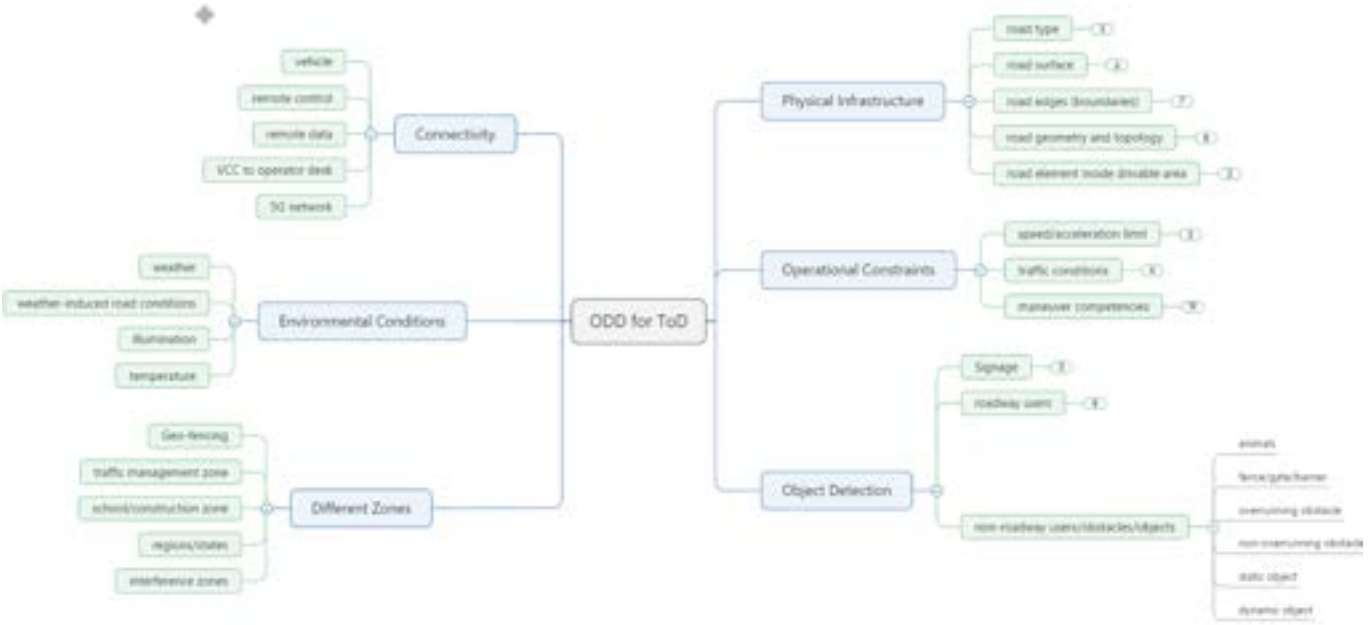

Figure 4-6: Potential ODD structure

As the safety considerations in this document and in 5GAA's STiCAD work item mainly concentrate on the communication part of the overall system, the ODD definition mentioned below is just focusing on those parts of the system related to communication, and do not pretend to be exhaustive.

Class	ODD elements	Considered (Y/N/Limited)	Function behaviour	Impact on safety analysis
Roadway Type	Highway	No		
	Urban	Limited	Assist autonomous vehicle to judge traffic	Lots of traffic surrounded
	Off-road (e.g. agricultural, construction site, mining)	No		
Roadway surface	Grass	Yes		
	Paved	Yes		
	Dry	Yes		

	Wet	Yes		
	Gravel	Yes		
Roadway boundaries	Side wall	Yes		
	Curb stone	Yes		
	Grass	Yes		
	Walkway	Yes		
	Sign	Yes		
	Pole	Yes		
	Guardrail	Yes		
Roadway geometry and topology	Curve	Yes		
	Downhill	Yes		
	Uphill	Yes		
	Uneven road	Yes		
	Brick road	Yes		
	Narrow road	Yes		
	Merging	Yes		
	Branching	Yes		
	Pothole	Yes		
Roadway elements	Oncoming traffic	Yes		
	Barriers	Yes		
	Temporal modification	Yes		
Vehicle dynamics	Speed limit	Yes		
	Acceleration limit	Yes		
Traffic conditions	Intersection	Yes		
	Traffic circle	Yes		
	Traffic jam	Yes		
	Crossover (zebra crossing)	Yes		
Manoeuvre competencies	Forward/backward driving	Yes		
	Perform lane change	Yes		
	Low/High-speed merge	Yes		
	Leaving the travel lane and park	Yes		
	Detect and respond to encroaching oncoming traffics	Yes		

	Perform car following (‘stop & go’)	Yes		
	Evade the static obstacles in the driving path	Yes		
	Manoeuvring in intersections	Yes		
	Perform turns (right, left, complete)	Yes		
	Manoeuvring in roundabouts	Yes		
	Manoeuvring in a parking lot	Limited		
	Follow police control (overriding)	Yes		
	Detect and respond to emergency vehicles	Yes		
	Stop for pedestrians, cyclist at intersections and crosswalks	Yes		
	Keep safe distance from vehicle, pedestrians, cyclist on side of the road	Yes		
	Manoeuvring off-road	No		
	With/without leading vehicle	Yes		
	Sudden traversing	Yes		
	Passing by a vehicle (or bicycle, motorcycle…)	Yes		
Detection	Signage	Yes		
Roadway users	Passenger Cars	Yes		
	Trucks	Yes		
	Bicycle	Yes		
	Motorcycle	Yes		
	Pedestrian	Yes		
	Trailing vehicle	Yes		
	Miscellaneous (e.g. skateboards, roller skates, e-scooters)	Yes		
Non-roadway users	Fence	Yes		
	Gates	Yes		
	Barriers	Yes		
	Animals	Yes		

	Railway	Yes		

Communication to other	Vehicles	No		
	Remote control	Yes		
	Remote data	Yes		
Weather	Rainy	Yes		
	Cloudy	Yes		
	Snow	Yes		
	Fog	Yes		
	Hail	Yes		
	Sleet	Yes		
	Smoke	Yes		
Illumination	Oncoming vehicle light	Yes		
	Early morning	Yes		
	Daytime	Yes		
	Evening	Yes		
	Night time	Yes		
Temperature		Yes		
Special zones	Geo-fencing	No		
	Traffic management zone	Yes		
	School	Yes		
	Construction	Yes		
	Regions/States	Yes		
	Garage	Yes		
	Tunnel	Limited		

4.4 Identification of Hazards

4.4.1 Hazards identified for direct control mode

Guide word	ID	Application of guide word	Hazard event and its consequences
NO OR NOT	H#1	Control message (CM) is not sent for a certain time period by control centre (CC) to the controlled vehicle (CV)	• CV is staying at a dangerous place causing an obstacle or danger for other road users • Another driver is not able to react in time to the obstacle and thus collides with the CV
	H#2	CM does not contain necessary fields for control (e.g. position, acceleration, speed, …)	• As H#1
	H#3	Fields in CM are not correct	• CV performs driving manoeuvres that are not as intended by the CC (e.g. driving with wrong speed or wrong steering angle) • CV causes an accident to other road users (e.g. hits a pedestrian or crashes into another vehicle)
	H#4	Fields in CM are inconsistent	• As H#3
	H#5	Video information is not sent from CV (or optional roadside station, RS) to CC for a certain time period	• Operator at CC cannot judge the traffic situation anymore and thus has to stop operating the vehicle • -> same as H#1
	H#6	Video information from CV (or optional RS) sent to CC is not detailed enough or the image is distorted	• As H#2
	H#7	Sensor information is not sent from CV (or optional RS) to CC for a certain time period	• As H#1
	H#8	Sensor information from CV (or optional RS) sent to CC is not detailed enough or disturbed	• As H#3

	H#9	CV stops responding to the CM; maybe due to broken communication channels between CV and CC, or loss of control to actuators in CV	• CV does not act as directed by CC • As H#3
	H#10	Inconsistent data received at CC, cannot be correlated, may be sabotaged (e.g. prior positioning data too far off the last update)	• Jammed/sabotaged user • As H#3
	H#11	Misinterpretation of CM messages at CV – due to data corruption	• CV does not act as directed by CC • As H#3
MORE		TBC	TBC
LESS		TBC	TBC
AS WELL AS	H#12	Interference caused by other functions in the CV	Wrong localisation or cascading failure at CV
PART OF		TBC	TBC
REVERSE		TBC	TBC
OTHER THAN/ INSTEAD		TBC	TBC
EARLY		TBC	TBC
LATE		Commands from CC to CV are delayed and reach it too late	• Reaction to the commands does not fit the traffic situation any more • CV causes an accident to other road users (e.g. hits a pedestrian or crashes into another vehicle)
		Video information from CV (or optional RS) to CC is delayed and reaches it too late	• Reaction of CC operator is not able to be performed in time • Reaction of CC operator results in CV causing an accident with other road users (e.g. hits a pedestrian or crashes into another vehicle)
BEFORE		TBC	TBC
AFTER		TBC	TBC

4.4.2 Hazards identified for indirect control mode

Guide word	ID	Application of guide word	Hazard event and its consequences
NO OR NOT	H#1	CM with new trajectory sent from CC does not contain necessary fields	• CV cannot perform necessary driving manoeuvre and thus causes an obstacle or danger for other road users • Another driver is not able to react in time to the obstacle and thus collides with the CV
	H#2	CM contains all fields but information is not correct	• CV performs a manoeuvre different from the intended one by the CC operator • CV causes an accident with other road users (e.g. hits a pedestrian or crashes into another vehicle)
	H#3	Fields in CM are inconsistent	• As H#2
	H#4	Situation information (video or sensor information) is not sent from CV (or optional RS) to CC for a certain time period	• As H#1
	H#5	Situation information (video or sensor information) from CV (or optional RS) sent to CC is not detailed enough or the image is distorted	• CC operator makes wrong decision due to unclear information and thus generates wrong driving manoeuvre information • CV causes an accident with other road users (e.g. hits a pedestrian or crashes into another vehicle)
	H#6	CV stops responding to the CM; maybe due to broken communication channels between CV and CC, or loss of control to actuators in CV	• CV does not act as directed by CC • As H#3
	H#7	Inconsistent data received at CC, cannot be correlated, may be sabotaged (e.g. prior positioning data too far off the last update)	• Jammed/sabotaged user • As H#3
	H#8	Misinterpretation of CM messages at CV – due to data corruption	• CV does not act as directed by CC • As H#3
MORE		TBC	TBC
LESS		TBC	TBC

AS WELL AS	H#9	Interference caused by other functions in the CV	Wrong localisation or cascading failure at CV
PART OF		TBC	TBC
REVERSE		TBC	TBC
OTHER THAN/ INSTEAD		TBC	TBC
EARLY		TBC	TBC
LATE		Situation information (video or sensor information) from CV (or optional RS) to CC is delayed and reaches it too late	• Reaction to the commands no longer fit the traffic situation • CV causes an accident with other road users (e.g. hits a pedestrian or crashes into another vehicle)
		CC commands from CC to CV are delayed and reach it too late	• Reaction to the commands no longer fit the situation • CV causes an accident with other road users (e.g. hits a pedestrian or crashes into another vehicle)
BEFORE		TBC	TBC
AFTER		TBC	TBC

4.5 Safety Goals

Hazardous event and associated risk	**Safety Goal**	**Possible ASIL ratings for selected hazardous events**
CV causes an accident by receiving wrong or late information from CC and thus causes a severe accident	SG1: Avoid wrong control information being received by the CV SG2: Avoid late control information being received by the CV	• If vehicle's autonomous sensors are still functioning the incorrect information could be checked and therefore accidents due to wrong information can be avoided -> QM • If vehicle's autonomous sensors are no longer functioning or they are degraded (e.g. because CC commands put vehicle outside ODD) -> ASIL D

		• If vehicle's autonomous sensors are still functioning, and the CV detects the control information is late with synchronised clocks between CC and CV, then CV can ignore the control information -> ASIL C
CV becomes an obstacle to other vehicles which might cause accidents	SG1: Avoid wrong control information being received by the CV SG2: Avoid late control information being received by the CV	• Drivers of other vehicles are still capable of avoiding crashes as in normal traffic situations, hard braking can be avoided due to still-functioning CV vehicle autonomous sensors -> QM to ASIL B • The reaction of the CV is unforeseeable by other traffic participants and thus normal reaction times cannot avoid accidents -> ASIL B to ASIL D • If vehicle's autonomous sensors are still functioning, and the CV detects the control information is late with synchronised clocks between CC and CV, then CV can ignore the control information -> ASIL C
CV causes an accident because the operator at CC gets wrong sensor information and thus provides wrong information to the vehicle or performs dangerous driving manoeuvres at the CV	SG3: Avoid wrong sensor information being received by the CC SG4: Avoid late information being received by the CC	• If vehicle's autonomous sensors are still functioning the incorrect information could be checked and accidents avoided -> QM • If vehicle's autonomous sensors are not functioning any more or are degraded (e.g. because CC commands put vehicle outside ODD) ASIL D • If vehicle's autonomous sensors are still functioning, and the CV detects the control information is late with synchronised clocks between CC and CV, then CV can ignore the control information. • ASIL C
CV becomes an obstacle to other vehicles which might cause accidents due to this obstacle due to wrong commands generated by the CC or late reaction	SG3: Avoid wrong information being received by the CC SG4: Avoid late information being received by the CC	• Drivers of other vehicles are still capable of avoiding crashes as in normal traffic situations, hard braking can be avoided due to still-functioning CV vehicle autonomous sensors -> QM to ASIL B • The reaction of the CV is unforeseeable by other traffic participants and thus normal reaction times cannot avoid accidents -> ASIL B to ASIL D

		• If vehicle's autonomous sensors are still functioning, and the CV detects the control information is late with synchronised clocks between CC and CV, then CV can ignore the control information -> ASIL C
CV may cause an accident or become an obstacle to other vehicles; CC may also make incorrect decisions	SG5: Avoid misbehaviour at CV and wrong reaction at CC; identify spurious and rogue clients and malware injection and avoid reaction	• Signal the misbehaviour and build challenge/authorisation mechanisms -> ASIL B to ASIL D

4.6 Functional Safety Requirements

4.6.1 Potential functional safety requirements for Safety Goal #1 (SG1)

SG1: Avoid wrong information being received by the CV.

Note: ISO 26262 Part 3, Section 7.4.2.3 [1] lists a number of strategies that can be considered in determining functional safety requirements: Fault avoidance, fault detection and control of faults, transitioning to safe state, fault tolerance, degradation of functionality, driver warnings, avoidance or mitigation of hazardous event, etc. Potential Functional Safety Requirements (PFSR) are organised in the tables below according to the category of fault and the strategy deployed to deal with that fault.

Fault location	**Fault Category (FC)**	**Potential Functional Safety Requirements (PFSR)**	**Comment**
CC	**FC1:** CC does not generate control messages when it should	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC1-1 (Requirement on CC)**: CC shall implement a watchdog that assures that regular control messages are available • **PFSR-FC1-2 (Requirement on CC)**: A real-time supervision system shall be implemented at CC that cares for regular message generation and sending **<u>Strategies for fault detection and mitigation:</u>**	

		• **PFSR-FC1-3 (Requirement on CC)**: CC shall inform the operator about messages sent and provide a warning if interval reaches certain maximum value **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC1-4 (Requirement on CV)**: CV shall monitor time since last control message received and, if certain threshold has been exceeded, either move to fail operational state (e.g. reduce speed) or, in case another higher maximum value has been reached, enter safe stop based on 'ego-sensors'	
CC	**FC2:** CC generates faulty or inaccurate control messages	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC2-1 (Requirement on CC)**: CC shall implement a concept and the means to validate control messages sent to the CV; validation might be done using plausibility checks to avoid unrealistic control messages • **PFSR-FC2-2 (Requirement on CC)**: CC shall implement a concept and the means to validate control messages sent to the CV; validation is based on knowledge of the capabilities of the vehicle (e.g. maximum/minimum speed, acceleration, steering angle, vehicle size) **<u>Strategies for fault detection and mitigation:</u>** none **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC2-3 (Requirement on CV)**: CV shall check the control messages received from CC for message correctness ('checksum') and for message authenticity (see PFSR-FC2-4); for this the CV has to hold e.g. public keys of all certified CCs	
NW	**FC3:** Messages correctly generated by CC are lost during	**<u>Strategies for fault avoidance:</u>**	

	transmission to the CV	• **PFSR-FC3-1 (Requirement on NW)**: NW shall provide the means to guarantee high quality of service for the transmitted messages on the complete chain from CC exit to CV entry (CCU – CCU) • **PFSR-FC3-2 (Requirement on NW)**: NW shall provide the means to predict quality of service on the complete chain from CC exit to CV entry (CCU – CCU) and allow CC and CV to regularly get this QoS **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC3-3 (Requirement on NW)**: NW shall provide the means to safely detect connection loss or degradation on both sides (CC and CV) • **PFSR-FC3-4 (Requirement on CC)**: CC shall continuously monitor communication state, using the means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. stop generating control messages based on potential outdated information) • **PFSR-FC3-5 (Requirement on CV)**: CV shall continuously monitor communication state, using the means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. move to fail operational state or enter safe stop) **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC3-6 (Requirement on CV)**: CV shall continuously monitor communication state, using the means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. move to fail operational state or enter safe stop)	
NW	**FC4:** Messages correctly generated by CC are corrupted during transmission to the CV	**<u>Strategies for fault avoidance:</u>** None **<u>Strategies for fault detection and mitigation:</u>**	

		• **PFSR-FC4-1 (Requirement on CC)**: To ensure message consistency, each message shall contain a 'checksum' at each point in the communication chain to see if the message is still consistent and has not been changed • **PFSR-FC4-2 (Requirement on CC)**: To ensure message authenticity, CC shall add a 'hash value' generated taking into account a certificate provided by an independent authentication control entity and that proves the CC is a registered and authorised control instance **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC4-3 (Requirement on CV)**: To ensure that no corrupted or otherwise faulty messages are used for manoeuvring the CV, the CV shall calculate a 'checksum' in the same way as the CC and, if there is a difference, the CV shall ignore such messages. If ignored messages are necessary for further operation (e.g. because of timing, etc.), the CV should enter 'safe state' or 'degrade function' • **PFSR-FC4-4 (Requirement on CV)**: The CV shall check the message 'hashes' against its own knowledge of certified users and ignore all messages that do not have proven authenticity or come from a trusted CC. If ignored messages are necessary for further operation (e.g. because of timing, etc.) the CV should enter 'safe state' or 'degrade function'	
CV	**FC5:** Control messages are correctly received by the CV but cannot be processed correctly by the application	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC5-1 (Requirement on CC)**: CC and CV shall have the same set of semantic rules for the control messages; the CC shall assure that only semantically correct messages are generated and transmitted **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC5-2 (Requirement on CV)**: The receiving CV should check the contents of all correctly received messages (all syntax checks successful) against semantic mistakes (e.g. non-performable manoeuvres) and shall ignore the semantically incorrect messages	

		<u>Strategies for fault detection and transition to safe state:</u> • **PFSR-FC5-3 (Requirement on CV)**: If ignored messages are necessary for further operation (e.g. because of timing, etc.), the CV should enter 'safe state' or 'degrade function'	
CV	**FC6:** Information received by the CV application is not consistent with the ego sensor information of the CV	**<u>Strategies for fault avoidance:</u>** None **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC6-1 (Requirement on CC)**: The CC shall add a confidence level indication at each message; the confidence level shall reflect how much trust the CC has in the contents of this message • **PFSR-FC6-2 (Requirement on CV)**: The CV shall keep a confidence level for each of its internal sensors; if the messages are not consistent, a reasonable decision shall be made on the usage of those messages in controlling the vehicle; the decision shall take into account the confidence levels in a reasonable way **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC6-3 (Requirement on CV)**: If the decision on the usage of the 'ego sensor' and or external information cannot be made with a high enough confidence level the vehicle should enter 'safe state' or 'degrade function'	
CC/CV			There are many other possibilities that might cause errors in this direction, e.g. the CV application could wrongly react to correct messages or actuators. There could also be other issues on the CC side, e.g. errors in control devices on the CC side could cause problems. However, those cases are not relevant for the

			considerations here, which deal with connectivity and related safety issues.

4.6.2 Potential functional safety requirements for Safety Goal #2 (SG2)

SG2: Avoid late information being received by the CV.

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)	Comment
CC	**FC7:** CC takes too long to produce the message and prepare it for sending	**Strategies for fault avoidance:** • **PFSR-FC7-1 (Requirement on CC)**: CC is allowed to monitor processing calculation and transmission times inside the CC thanks to a real-time capable computation system architecture **Strategies for fault detection and mitigation:** • **PFSR-FC7-2 (Requirement on CC)**: The CC shall constantly monitor the calculation capabilities available and detect bottlenecks or serious delays in real time **Strategies for fault detection and transition to safe state:** • **PFSR-FC7-3 (Requirement on CC)**: If the CC detects a problem in its calculation chain that prevents it from doing calculations in time, it shall inform the CV immediately • **PFSR-FC7-4 (Requirement on CV)**: The CV shall, on reception of the information about timing problems from the CC, enter 'safe state' or 'degrade function'	
NW	**FC8:** Transmission of the messages from	**Strategies for fault avoidance:**	

	the CC to the CV takes too long.	• **PFSR-FC8-1 (Requirement on NW)**: The network shall be able to fulfil transmission times given by a certain QoS as the basis for the communication; if the required transmission time cannot be kept, the NW should immediately inform the CV and the CC • **PFSR-FC8-2 (Requirement on CC)**: The CC shall provide the means for monitoring CC internal message transmission times **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC8-3 (Requirement on NW)**: The network shall provide the means for monitoring transmission times in real time • **PFSR-FC8-4 (Requirement on CC)**: The CC shall provide the means for monitoring CC internal message transmission times • **PFSR-FC8-5 (Requirement on CV)**: CV shall implement a monitoring function that keeps track of the transmission times currently available and detects if a message that should arrive is late **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC8-6 (Requirement on CV)**: When the monitoring is proving that transmission times are too long, the CV should enter 'safe state' or 'degrade function'	
CV	**FC9:** Processing of the messages at the CV takes too long	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC9-1 (Requirement on CV)**: The CV shall implement a real-time capable computation system including monitoring of the current computation performance **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC9-2 (Requirement on CV)**: The CV shall constantly monitor the computation performance of its real-time computation system **<u>Strategies for fault detection and transition to safe state:</u>**	

		• **PFSR-FC9-3 (Requirement on CV)**: If the real-time requirements of the application can no longer be assured, the CV should enter 'safe state' or 'degrade function'	
CC/CV			There are many other possibilities that might cause errors in this direction, e.g. the CV application could wrongly react to correct messages or actuators. There could also be other issues on the CC side, e.g. errors on the CC's control devices could cause problems. However, those cases are not relevant for the considerations here, which deal with connectivity and related safety issues.

4.6.3 Potential functional safety requirements for Safety Goal #3 (SG3)

SG3: Avoid wrong information being received by the CC.

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)	Comment
CV	**FC10:** Sensor at the CV (or optional RS) does not generate data	**Strategies for fault avoidance:** • **PFSR-FC10-1 (Requirement on CV (or optional RS))**: Sensors used in CV and/or RS should have a suitable ASIL grade **Strategies for fault detection and mitigation:** • **PFSR-FC10-2 (Requirement on CV (or optional RS))**: The health of the sensors shall be monitored in real time; monitoring needs to be implemented according to the suitable ASIL grade **Strategies for fault detection and transition to safe state:**	

		• **PFSR-FC10-3 (Requirement on CV (or optional RS))**: If a problem is detected with the sensors by the monitoring function, all relevant system parts (CC, receiving CV) should be informed; and the receiving CV(s) should enter 'safe state' or 'degrade function'	
CV	**FC11** Sensor at the CV (or optional RS) is generating wrong or inaccurate data	**Strategies for fault avoidance:** • **PFSR-FC11-1 (Requirement on CV (or optional RS))**: Sensors used in CV and/or RS should have a suitable ASIL grade **Strategies for fault detection and mitigation:** • **PFSR-FC11-2 (Requirement on CV (or optional RS))**: The health of the sensors shall be monitored in real time; monitoring needs to be implemented according to the suitable ASIL grade • **PFSR-FC11-3 (Requirement on CC)**: The CC shall perform plausibility checks between the received information and other information available at the CC (including judgement by operator); implausible data shall not be used for serious decisions **Strategies for fault detection and transition to safe state:** • **PFSR-FC11-4 (Requirement on CV (or optional RS))**: If a problem is detected with the sensors by the monitoring function, all relevant system parts (CC, receiving CV) should be informed; the receiving CV(s) should enter 'safe state' or 'degrade function'	
CV	**FC12:** Sensor at the CV (or optional RS) is generating correct data but information is interrupted or degraded when preparing it for	**Strategies for fault avoidance:** • **PFSR-FC12-1 (Requirement on CV (or optional RS))**: Software and hardware used for sensor processing (e.g. video encoding) shall have a suitable ASIL grade **Strategies for fault detection and mitigation:**	

	sending (e.g. at video encoding)	• **PFSR-FC12-2 (Requirement on CC)**: The CC shall perform plausibility checks between the received information and other information available at the CC (including judgement by operator); implausible data shall not be used for serious decisions **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC12-3 (Requirement on CC)**: If plausibility checks are showing severe problems, the CV should be informed about this state • **PFSR-FC12-4 (Requirement on CV)**: If sensor plausibility problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
NW	**FC13:** Sensor information is lost in transmission during the network	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC13-1 (Requirement on NW)**: NW shall provide the means to guarantee a high quality of service for the transmitted messages on the complete chain from CC exit to CV entry (CCU – CCU) • **PFSR-FC13-2 (Requirement on NW)**: NW shall provide the means to predict quality of service on the complete chain from CC exit to CV entry (CCU – CCU) and allow CC and CV to regularly get this QoS **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC13-3 (Requirement on NW)**: NW shall provide the means to safely detect connection loss or degradation on both sides (CC and CV) • **PFSR-FC13-4 (Requirement on CV (or optional RS))**: CV (or optional RS) shall continuously monitor the communication state using the means from PFSR-FC13-3, and implement strategies to cope with network errors or degradation (e.g. inform receiving system elements (CC, CV) about the network problems) • **PFSR-FC13-5 (Requirement on CV)**: CV shall continuously monitor communication state using the means from PFSR-FC13-3 and implement strategies to cope with network errors or degradation (e.g.	

		inform CV to about failure and cause CV to enter fail operational state or enter safe stop) **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC13-6 (Requirement on CV)**: If network problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
Network	**FC14:** Sensor information is corrupted during transmission over the CV (or optional RS)	**<u>Strategies for fault avoidance:</u>** None **<u>Strategies for fault detection and mitigation :</u>** • **PFSR-FC14-1 (Requirement on CV (or optional RS))**: To ensure message consistency, each message shall contain a 'checksum' at each point in the communication chain to be sure the message is still consistent and has not been changed • **PFSR-FC14-2 (Requirement on CV (or optional RS))**: To ensure message authenticity, CC shall add a 'hash' value generated taking into account a certificate provided by an independent authentication control entity that proves the CC is a registered and authorised control instance **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC14-3 (Requirement on CC)**: To ensure that no corrupted or otherwise faulty messages are used for manoeuvring the CV, the CC shall calculate a 'checksum' in the same way as the CC and, if there is a difference in the calculated and received checksum, the CV shall ignore such messages, but if these messages are necessary for further operation (e.g. because of timing, etc.) the CV should enter 'safe state' or 'degrade function' • **PFSR-FC14-4 (Requirement on CC)**: The CC shall check the message 'hashes' against its own knowledge of certified users and shall ignore all	

		messages that do not have proven authenticity that come from a trusted CC; and if these messages are necessary for further operation (e.g. because of timing, etc.) the CV shall be informed • **PFSR-FC14-5 (Requirement on CV)**: If network problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
CC	**FC15:** Sensor information is received at CC but incorrectly decoded	**Strategies for fault avoidance:** • **PFSR-FC15-1 (Requirement on CC)**: The hardware and software used to decode the sensor information shall have the suitable ASIL grade **Strategies for fault detection and mitigation:** • **PFSR-FC15-2 (Requirement on CC)**: The CC shall perform plausibility checks between the received information and other information available at the CC (including judgement by operator); implausible data shall not be used for serious decisions **Strategies for fault detection and transition to safe state:** • **PFSR-FC15-3 (Requirement on CC)**: If plausibility checks are showing severe problems, the CV should be informed about this state • **PFSR-FC15-4 (Requirement on CV)**: If sensor plausibility problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
CC/CV			There are many other possibilities that might cause errors in this direction, e.g. the CV application could wrongly react to correct messages or actuators. There could also be other issues on the CC side, e.g. errors on the control devices could cause problems. However, those cases are not relevant for the considerations here, which

			deal with connectivity and related safety issues.

4.6.4 Potential functional safety requirements for Safety Goal #4 (SG4)

SG4: Avoid late information being received by the CC.

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)	Comment
CV	**FC16:** CV (or optional RS) sensors take too long to generate the data	**Strategies for fault avoidance:** • **PFSR-FC16-1 (Requirement on CV (or optional RS))**: CV (or optional RS) shall be allowed to monitor processing calculation and transmission times inside of the CV/RS by real-time capable computation system architecture **Strategies for fault detection and mitigation:** • **PFSR-FC16-2 (Requirement on CV (or optional RS))**: The CV (or optional RS) shall constantly monitor the calculation capabilities available and detect bottlenecks or serious delays in real time **Strategies for fault detection and transition to safe state:** • **PFSR-FC16-3 (Requirement on CV (or optional RS))**: If the CV (or optional RS) detects a problem in its calculation chain that prevents it from doing calculations in time, it shall inform the CC immediately • **PFSR-FC16-4 (Requirement on CC)**: The CC shall on reception of the information about timing problems from the CV (or optional RS) inform the controlled CV(s) • **PFSR-FC16-5 (Requirement on CV)**: If calculation problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	

CV	**FC17:** Coding of the sensor information for transmission takes too long	**Strategies for fault avoidance:** • **PFSR-FC17-1 (Requirement on CV (or optional RS))**: Coding of the sensor information shall be performed by a powerful and real-time capable calculation hardware and software • **PFSR-FC17-2 (Requirement on CV (or optional RS))**: CV (or optional RS) shall be allowed to monitor coding calculation and transmission times inside of the CV/RS by real-time capable computation system architecture **Strategies for fault detection and mitigation:** • **PFSR-FC17-3 (Requirement on CV (or optional RS))**: CV (or optional RS) shall constantly monitor coding calculation and transmission times inside of the CV/RS **Strategies for fault detection and transition to safe state:** • **PFSR-FC17-4 (Requirement on CV (or optional RS))**: If the CV (or optional RS) detects a problem in its calculation chain that prevents it from doing calculations in time, it shall inform the CC immediately • **PFSR-FC17-5 (Requirement on CC)**: The CC shall on reception of the information about timing problems from the CV (or optional RS) inform the controlled CV(s) • **PFSR-FC17-6 (Requirement on CV)**: If calculation problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
NW	**FC18:** Transmission time over the network takes too long	**Strategies for fault avoidance:** • **PFSR-FC8-1 (Requirement on NW)**: The network shall be able to fulfil transmission times given by a certain QoS as the basis for the communication; if the required transmission time cannot be kept, the NW should immediately inform the CC and the CV (or optional RS)	

		• **PFSR-FC8-2 (Requirement on CV (or optional RS))**: The CV (or optional RS) shall provide the means for monitoring CV (or optional RS) internal message transmission times **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC18-3 (Requirement on NW)**: The network shall provide the means for monitoring transmission times in real time • **PFSR-FC18-4 (Requirement on CV (or optional RS))**: The CV (or optional RS) shall provide the means for monitoring CV (or optional RS) internal message transmission times • **PFSR-FC18-5 (Requirement on CC)**: CC shall implement a monitoring function that keeps track of the transmission times currently available and detects if a message that should arrive is late **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC18-6 (Requirement on CC)**: When the monitoring is proving that transmission times are too long, the CC shall immediately inform the CV about this • **PFSR-FC18-7 (Requirement on CV)**: If timing problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
CC	**FC19:** Decoding and displaying the sensor information at the CC takes too long	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC19-1 (Requirement on CC)**: The CC shall implement a real-time capable computation system including a monitoring function of the current computation performance **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC19-2 (Requirement on CC)**: The CV shall constantly monitor the computation performance of its real-time computation system	

		<u>Strategies for fault detection and transition to safe state:</u> • **PFSR-FC19-3 (Requirement on CC)**: If the real-time requirements of the application can no longer be assured, the CV shall immediately inform the CV about this • **PFSR-FC19-4 (Requirement on CV)**: If decoding problems are reported by the CC, the receiving CV(s) should enter 'safe state' or 'degrade function'	
CC/CV			There are many other possibilities that might cause errors in this direction, e.g. the CV application could wrongly react to correct messages or actuators. There could also be other issues on the CC side, e.g. errors on the control devices could cause problems. However, those cases are not relevant for the considerations here, which deal with connectivity and related safety issues.

5 Emergency Brake Warning V2V Use Case

5.1 Item Definition

This use case represents a scenario where information is exchanged between two end points (in the specific case two vehicles) through direct communication.

In this section the item is defined. The aspects considered in describing the item are those provided in or inspired by [1] (ISO 26262 Part 3) Section 5.

As per [1] the objectives of producing an item definition are:

a) to define and describe the item, its functionality, dependencies on and interaction with, the driver, the environment and other items at the vehicle level; and
b) to support an adequate understanding of the item so that the activities in subsequent phases can be performed.

Two Emergency Brake Warning (EBW) scenarios are considered:

- **EBW Scenario 1 (Human acts on message)**
  - The EBW message results in a human receiving a warning who may then act upon (SAE level 0 [9]) it
- **EBW Scenario 2 (Hybrid: Human and/or robot acts on message)**
  - The EBW message is acted upon by a human and/or an Autonomous Emergency Braking (AEB) system (SAE level 0 [9])

5.1.1 Legal requirements, national and international standards

- ETSI 102 637 [2] defines an Emergency Electronic Brake Light use case (reproduced in Appendix of [13]).
  - Requirements of this use case have been reproduced in Appendix A
- SAE J2945/1 [3], Section 4.2.3 also describes an 'Emergency Electronic Brake Light' use case
  - Functionality described includes the receiving vehicle determining which vehicles have sent the message and the position of those vehicles, and then determining the relative distance to them (for those vehicles that are broadly ahead) and if this distance is less than a certain implementation threshold. A threat level is then allocated and a warning is provided to the driver accordingly.

Though not standards, the following documents provide use case descriptions:
- 5GAA has defined an 'Emergency Brake Warning' use case [8] (original document submission: [4])
- An EEBL use case was described by the Convex project [14]

5.1.2 The functional behaviour at the vehicle level including the operating modes or states

5.1.2.1 Human acts on message (SAE level 0)

Expected functional behaviour:

- Step 1) TxV (i.e. the vehicle which transmits the EBW message) detects an emergency braking event (e.g. measured rate of deceleration exceeds a threshold) and transmits an EBW V2V message
- Step 2) RxV (i.e. the vehicle which receives the EBW message) receives EBW message
- Step 3) RxV determines whether any messages received are from a vehicle that is within a certain distance and direction such that the human driver should be alerted
- Step 4) Human driver is alerted, through audio (e.g. voice message or chime) or through vibration (e.g. of steering wheel or seat) or through visual (e.g. warning on heads-up display), or through some combination of these methods
- Step 5) Human driver becomes alert and takes action:

- Intended action is that the human driver reduces speed rapidly, e.g. by braking hard, even in the absence of other corroborating evidence of an emergency braking event (thus benefitting from the non-line-of-sight messaging capability of V2X)
- Action taken could also include any of (or combination of)
  - Reduce speed action (brake, foot off accelerator, depress clutch, gear down)
  - Abort lane change
  - Abort acceleration
  - Abort other manoeuvre
  - Change lane
- Human driver is not expected to check surroundings (e.g. whether there are cars following closely behind) before taking action

5.1.2.2 Hybrid: Human and/or robot act on message (SAE level 0)

Expected functional behaviour:

- Steps 1-5 as above, then:
- **If human driver does not take action within a specific time** and EBW message is still current (e.g. has been retransmitted/not cancelled/is still within its validity time/danger is still imminent) then the car initiates AEB and applies brakes:
  - The force with which brakes are applied may depend on
    - Deceleration needed in order to avoid collision with the vehicle ahead undertaking the emergency braking
    - Proximity of following vehicles; whether following vehicles are known to be V2X equipped (and may therefore also have received the message from TxV)
- **If human takes action within a specific time but braking force applied is less than optimal** and EBW message is still current (e.g. has been retransmitted/not cancelled/is still within its validity time/danger is still imminent) then car takes action
  - Vehicle may apply Emergency Brake Assist to increase the force with which the brakes are applied

5.1.3 The required quality, performance and availability of the functionality, if applicable

An indication of non-functional requirements that may be adequate for our purposes is provided in the 5GAA Emergency Brake Warning use case description provided by Ford and Continental in [4]. This information provides non-functional requirements for two different 'user stories'. The most relevant requirements have been reproduced in Appendix B of [13].

5.1.4 Constraints, functional dependencies, dependencies on other items, and the operating environment

Human acts on message:

- Human may take into account numerous factors in building situational awareness used in determining what action to take (e.g. how hard to apply brakes) when receiving an EBW message:
  - Current and historic proximity, position, speed, direction of other vehicles
  - Assumptions on behaviour of other motorists
  - Knowledge of road layout
  - Road conditions
  - Visual or audio evidence of emergency braking event (corroborating evidence)

Hybrid: Human and/or robot act on message:

- Human driver may take into account the environmental information listed above
- If human driver fails to activate brakes, or fails to activate them with sufficient force then a robot may intervene taking numerous environmental factors into account in deciding what action to take:
  - Local dynamic map info
    - From network (RSU/internet)

- Road conditions:
  - From V2X, or from ego-sensors (e.g. windscreen water sensors, vehicle light activation)

5.1.5 Potential consequences of behavioural shortfalls including known failure modes and hazards

- None so far identified (this is dealt with in the risk and hazard analysis phase of our work)

5.1.6 Capabilities of actuators, or their assumed capabilities

- Assume that brakes are activated promptly in response to signals (foot depression of human driver) or electronic signal (robot), and that there is adequate granularity to allow a variety of braking forces to be applied
- Assume Anti-lock Braking System (ABS) is available:
  - Feature manages wheel lock up and enables the vehicle to be steered effectively even as it is braking hard
- Electronic brake force distribution:
  - Enables appropriate braking forces to be applied to each wheel with the intention of preventing wheel lock-up (inclusion in study is FFS)
- Emergency Brake Assist
  - Enables the vehicle to detect that braking action applied by the human driver corresponds to an emergency braking manoeuvre, and in this case the vehicle may apply additional braking force in case the human driver is not applying as much force as the vehicle is capable of handling

5.1.7 Elements of the item

A high-level description of the item is shown in Figure 5-1-1. More detailed descriptions are shown for each of the two EBW scenarios in the sub-sections.

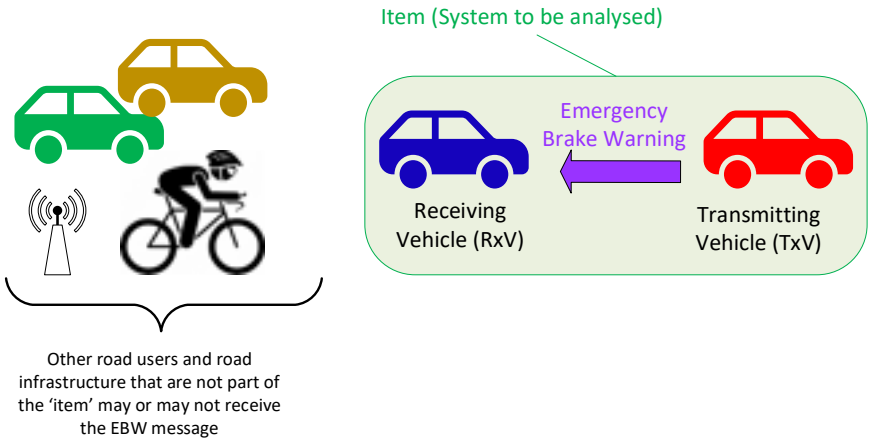

Figure 5-1-1: Item definition for emergency brake warning (simple view)

Note that it is assumed that the communications between TxV and RxV are direct and use the PC5 interface. For this use case it is assumed that the network is not involved, and that there is no scheduling of access to the PC5 connection by the cellular network.

5.1.7.1 EBW Scenario 1: Human acts on message

Figure 5-1-2 shows the functional architecture of the item for EBW Scenario 1 in which a human acts on the V2V message. This architecture was partly inspired by information provided in ETSI and SAE specifications [2, 3, 5] (and reproduced in Appendixes A, C, D and E of [13]).

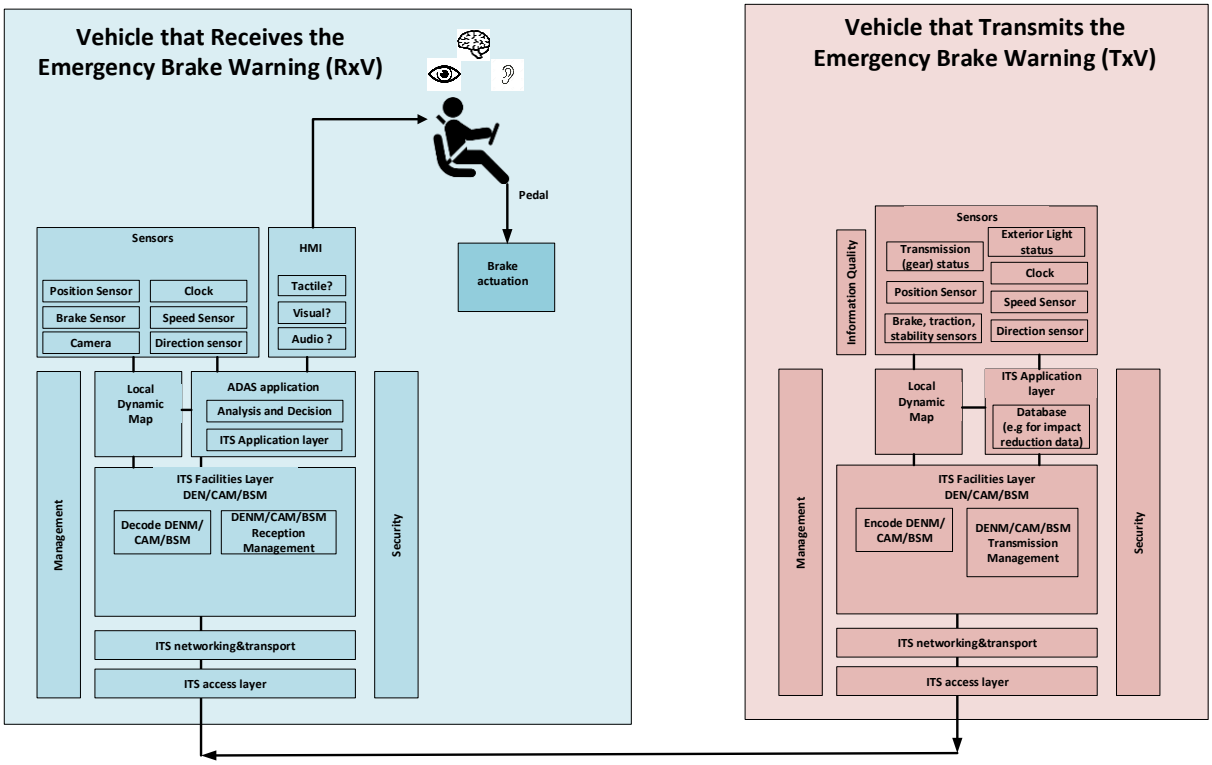

Figure 5-1-2: Functional architecture of 'item' for EBW Scenario 1: Human acts on message

ETSI supports the use of relaying DENM messages. However, for simplicity we consider an item description where relaying between a transmitting ITS station and a Receiving ITS station does not occur.

Comments on functional architecture: Vehicle that transmits the V2V message (TxV)

- Sensors detect whether an emergency braking event is occurring, and this could be achieved in a number of ways:
  - Measurements made within the brake actuators
  - Measurements made by brake pedal sensors
  - Speed-based measurements of deceleration
    - Change in wheel revolutions with time
    - Change in GPS position vs time
- Sensors provide information needed for populating EBW DENM, or SAE EEBL BSM message:
  - Timestamp (clock)
  - Position (GPS)
  - Direction (GPS)
  - Speed (GPS, wheel revolution counter, clock)
    - Also calculates acceleration, deceleration
  - Transmission status (gear sensor)
  - Exterior lights (e.g. hazard warning light sensor)
  - Brake, transmission and stability control status sensors
  - Vehicle type (car, truck, freight truck …)
- Information quality:
  - In the ETSI DENM message this takes values 0…7 and is supposed to be an indication of the probability that the event actually exists at the indicated event position [5]
    - It is unclear from the ETSI specs how this should be set. Ref [6] states that the 'definition of quality level is out of the scope of the present document'
  - SAE defines confidence levels for DF_PathPrediction and DF_PositionalAccuracy
- Local dynamic map:
  - May be needed for indicating lane position (FFS)
  - There is the following ETSI requirement [2]: 'The vehicle ITS stations shall be able to verify whether the "emergency electronic brake lights" event may be a risk to other vehicles.'

        - It is unclear what the vehicle should do if it finds a risk/does not find a risk (FFS)
- ITS application layer database:
    - Impact reduction data provides information about TxV that a RxV may use in managing how to act on the message (whether this may be included in an EBW message is yet to be determined)
- Transmission management:
    - For ETSI DENM messages, a cancellation message may be sent when the event is terminated (according to ETSI requirements [2], Appendix A)
    - Transmit EBW continuously with dynamic data will help RxV to track the TxV state such as vehicle spinning, running into road shoulder, etc.

Comments on functional architecture: Vehicle that receives the V2V message (RxV)

- ITS facilities layer:
    - Both DENM and CAM are mentioned because although in ETSI's design the EBW message is sent using DENM, in [2] it is stated that information provided in CAMs may also be taken into account by the vehicle that receives the DENM
- ITS application layer: analysis and decision:
    - The ETSI specification [2] states (see also reproduction in Appendix A) that: 'The RHW [Road Hazard Warning] application shall decide whether an *"*emergency electronic brake lights*"* warning information should be provided to user via HMI.*'* (SAE J2945/1 [3] has a similar statement)
        - One set of criteria to be taken into account in making this decision will be the relative position of the car that generated the message (TxV) compared to its RxV, for example
            - If the car that generated the message is on the carriageway that goes in the opposite direction then the message could be ignored (in this case no warning need be provided via the HMI)
            - If TxV is behind RxV then the message could be ignored (in this case no warning need be provided via the HMI)
            - If TxV and RxV are on a multi-lane highway, and even if they are moving in the same direction, then RxV may decide not to create a warning via the HMI if TxV and RxV are a sufficient number of lanes distance from one another (SAE J2945/1 [3] states that warnings are only provided to the driver if the vehicle undertaking the emergency braking is in the same lane, next lane to the left or next lane to the right, with dependency also on how far in front the braking vehicle is)
            - Hence RxV will need access to its own position (GPS), direction (GPS) and lane information (local dynamic map, camera)
        - RxV will also take into account the time that the message was generated
            - The ETSI specification [3] states: 'The originating vehicle ITS station shall add an estimated valid time to the *"*emergency electronic brake lights*"* DENM.*'*
            - RxV may choose not to generate a message on HMI if the validity time has passed
            - For this feature the clock will be required in RxV
        - The EBW may choose not to send a message over HMI if the human driver is already applying the brakes (requires brake sensor) and/or if speed is low (speed sensor)
- HMI:
    - The human machine interface over which the warning is provided could take many forms
        - Tactile (e.g. vibration of steering wheel or seat)
        - Audio (e.g. warning alarm, chime, replay of audio file of human voice saying e.g. 'brake now')
        - Visual (e.g. symbol displayed on heads up display)
        - Dynamic TxV state (position, direction, brake data, etc.)
        - Or some combination of the above
- Human driver:
    - As has already been noted, the human driver plays a critical role in this control loop and in implementing a reaction to the warning (hence brain, eyes and ears are shown in the figure)
- Brake actuation:
    - The human driver applies the brake pedals and this sends either an electrical or hydraulic 'signal' to the brakes

5.1.7.2 EBW Scenario 2 Hybrid: Human and/or robot acts on message

Figure 5-1-3 shows the functional architecture for EBW scenario 2 where a human and/or robot acts on the message. Differences compared to Figure 5-1-2 are highlighted in the addition of the new (green) line which enables the ITS application (robot) to automatically actuate the brakes.

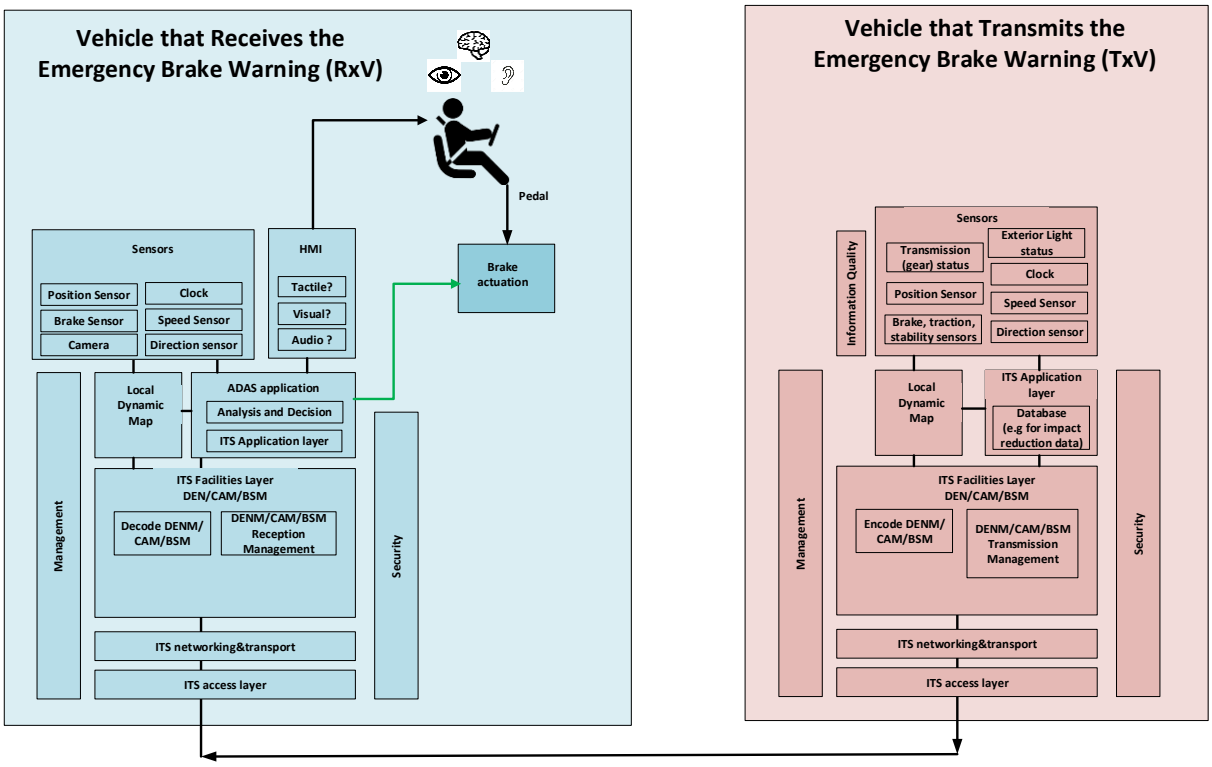

Figure 5-1-3: Functional architecture of 'item' for EBW Scenario 2: Human and/or robot acts on message

Vehicle that transmits the V2V message (TxV): Comments on functional architecture

- Same as for EBW Scenario 1

Vehicle that receives the V2V message (RxV): Comments on functional architecture

- Similar to EBW Scenario 1, with the following differences: the ADAS application itself will be different to the ADAS application of EBW Scenario 1, because there is additional information to process, and additional 'analysis and decision' processes associated with whether and by how much to apply the brakes in the event that the human driver does not apply them or applies them with too little force

5.1.8 Assumptions concerning the effects of the item's behaviour on the vehicles in the item

ISO 26262 [1] has a similar but different 'heading' to the above heading which is inspired by ISO 26262. ISO 26262 has an item definition category: 'Assumpti*ons concerning the effects of the item's behaviour on the vehicle'*. However, this ISO 26262 'heading' does not reflect very well the new V2V scenario we are considering in this study where the 'item' actually consists of two vehicles.

It is assumed that the effect of the item's behaviour on the vehicles in the item will be:

- RxV brakes (loses speed) when a vehicle that is further up the road signals an emergency brake warning message
- To reduce the chance that a following vehicle (which could be RxV) will collide with ('rear-end') a leading vehicle (TxV) and thereby reduce adverse impacts for the cars and the car occupants

- Reduce the chance that a vehicle that is following RxV will collide with ('rear-end') RxV

5.1.9 The functionality of the item under consideration required by other items and elements

No requirements identified.

5.1.10 The functionality of other items and elements required by the item under consideration

No new functionality required that has not already been described above.

5.1.11 The allocation and distribution of functions among the involved systems and elements

This has already been described with reference to the detailed diagrams above.

5.1.12 The operational scenarios which impact the functionality of the item

Assume the feature operates at all speeds (including high speeds).

There are a large number of operational scenarios that may affect the functionality of the 'item'.

- Variable factors within the 'item' definition:
  - Distance between TxV and RxV
  - Speed and direction of TxV and RxV
  - Whether other vehicles are positioned between TxV and RxV
  - Impacts: Likelihood that collision can be avoided
- State of the driver in RxV:
  - Driver might be fatigued or distracted
  - Driver might never have received the warning message before
  - Warning message might be conveyed in a different manner to what the driver has been familiar with in the past with other vehicles
  - Driver may not have been taught what they are supposed to do when receiving a warning message
  - Driver may not understand that an EBW event could have been received from a car that is out of the line of sight (e.g. may have come from a car in front of the truck that the car is travelling behind)
  - Impacts: Delay in reacting to EBW; applying too little/too much brake force in reaction to EBW; cognitive confusion when receiving the EBW over HMI results in reduction not increase in situational awareness; the above may result in increased likelihood of collision
- Availability of visible or audible evidence of the emergency braking event (from the perspective of the driver of RxV):
  - Driver may be unable to see the vehicle that issued the EBW.
  - Driver may be unable to hear the braking of the vehicle that generated the EBW.
  - Impacts: driver does not take action or delays taking action (pending corroborating visible or audible evidence), even though the event is real
- Road type/layout:
  - Multi-lane highway
  - Country lane
  - Intersection
  - Slip road
  - Car park
  - Impacts: Use of EBW on high-speed roads (highways) may make severity of injury greater; use of the feature in lower speed environments may mean vulnerable road users are present, which again could impact upon the severity and controllability of collision

- Road conditions/weather:
    - Ice, snow, rain, blinding sun
    - Poor traction, e.g. caused by weather, road surface material
    - Impacts: Unusual conditions affect efficacy of human driver and/or car systems, potentially increasing likelihood of collision
- Vehicle conditions:
    - Braking efficiency
    - Condition and type of tyres
- Vehicle state/driving manoeuvres:
    - Making lane change
    - Accelerating
    - Creeping
    - Impacts: Driver attention is elsewhere (making manoeuvre) at the time the EBW alert is received; acceleration the means time to stop may be longer; available actions to driver could be increased (e.g. stop accelerating is a possible response to the EBW)
- Capabilities of other road users in the environment:
    - Support or not for autonomy (at various SAE levels) and ADAS features, including
        - Automatic cruise control (ACC)
        - Automatic emergency braking (AEB)
        - Automatic lane keeping (ALK)
    - Ability of other vehicles to receive EBW V2X messages
    - State of driver in other vehicles (see above list for 'driver state')
    - Impacts: How other vehicles and drivers of those vehicles around the item react (e.g. timeliness of reaction, appropriateness of braking force applied, etc.)
- Positions of other road users in the environment:
    - Distance and direction with respect to RxV, TxV
    - Impacts: Collision into rear end of RxV more likely if following car is travelling close behind (with low or inadequate braking distance)
- Density of other road users in the environment:
    - Highly congested, low congestion
    - Traffic jam
    - Impacts: Higher number of cars may increase probability of some cars colliding; visibility is restricted (as already mentioned above)
- Types of road users:
    - Cars, trucks, pedestrians, cyclists, motorcyclists
    - Impacts: Pedestrians, motorcyclists or cyclists in the vicinity may mean the severity of injury in any collisions could be higher; driver awareness of such VRUs may be less (since they are smaller than a car or truck); trucks may limit visibility of the source of emergency braking

5.2 Hazard and Risk Analysis

5.2.1 Operational Situations

In performing a HARA, one or more operational situations need to be specified; ISO 26262 [1] states:

> *'The operational situations and operating modes in which an item's malfunctioning behaviour will* result in a hazardous event shall be described; both when the vehicle is correctly used and when it is incorrectly used in a reasonably foreseeable way.*'*

Note 1: Operational situations describe conditions within which the item is assumed to behave in a safe manner.

Note 2: Hazards resulting only from the item behaviour, in the absence of any item failure, are outside the scope of this document.

There are many operational situations that we could consider, and many potentially relevant operational dimensions are provided in Section 5.1. One straightforward and commonly occurring operational situation is described below, to get the discussion started.

Operational situation	**Description**
1	• Highway: Fast road on which vehicles are allowed to travel at 60mph or greater • Drivers of RxV and any vehicle following RxV have a typical level of alertness • Driver of RxV has experienced the EBW alert before • Driver of RxV understands that the alert may come from a vehicle that is out of their line of sight • RxV is being driven along the highway at a constant speed, no manoeuvres are being undertaken • Road conditions and weather are good • Highway is busy, with mixture of motorised 4 (or more) wheeled vehicles, some of which are V2X equipped and some of which are not • Further details of this operational situation, e.g. distance between vehicles are described within the section that provides the detailed ASIL determination
2	……

Table 5-2-1: Operational situations

Note: SAE J2980 [12], Section F.5 considers a slightly different use case to ours where a malfunction results in a car applying its parking brakes when travelling at speed. This specification [12] states that for their (parking brake) scenario, in order to properly evaluate the risk, several factors may be included in the analysis: deceleration dynamics of vehicles, driver reaction times, exposure rates for different distances between the two vehicles at different speeds, exposure rates for different types of vehicle if this leads to different severity impacts (e.g. if the following vehicle is a truck then the speed at impact could be greater and severity of injury could be greater, but exposure, i.e. probability of being followed by a truck is lower). Whether we will need to get into a comparable level of detail for our study is yet to be determined.

5.2.2 Identification of Hazards

ISO 26262 [1] states: *'The hazards shall be determined systematically based on possible malfunctioning of the item.'*

Note 1: FMEA approaches and HAZOP are suitable to support hazard identification at the item level. These can be supported by brainstorming, checklists, quality history and field studies.

5.2.2.1 Hazards identified for Operational Situation #1, EBW Scenario 1

In the following table we apply the HAZOP guide words to the V2V DENM EBW message. (Note that this HARA is not intended to be exhaustive.)

Guide word	ID	Application of guide word	Hazard event and its consequences
NO OR NOT	H#1	EBW message is not sent by TxV	• Human driver of RxV does not receive an EBW notification • Hence the driver has to wait for other indications of emergency braking, e.g. the driver has to wait until they can see with their own eyes the vehicle in front suddenly braking hard, therefore the time for the driver of RxV to react is reduced compared to what would have been the case if they had received the EBW warning as intended • Under certain conditions of speed and distance between TxV and RxV a crash might therefore result • Either RxV crashes into the rear of a vehicle in front or a vehicle following RxV crashes into RxV
	H#2	EBW message is not received by RxV	As H#1
	H#3	EBW message is received by RxV but is not processable by the application	As H#1
	H#4.1	Field within EBW message is not present or is not accurate: *eventPosition* [5]	Consider first the case where RxV receives an EBW message which states a location for the emergency braking event (*eventPosition*: location of TxV) which is incorrect: • RxV uses the information, and in some circumstances, determines that the braking vehicle is in the same lane and a relatively short distance in front of it (even though in actual fact the braking vehicle is elsewhere) • The emergency brake warning is provided to the human driver via the HMI. • The human driver of RxV applies the brakes hard • A following Vehicle (FV), which is not V2X equipped, crashes into the rear end of RxV
	H#4.2	Field within EBW message is not present or is not accurate: *eventPosition* [5]	Consider the case where the location information is not present: • In this case, RxV may reject the message since eventPosition is a mandatory information element • Outcomes are then similar to H#3 (similar to H#1)

	H#5	Field within EBW message is not present or is not accurate: *relevanceTrafficDirection* [5]	To be completed
	H#6	Field within EBW message is not present or is not accurate: *eventSpeed* [5]	To be completed
	H#7	Field within DENM message is not present or is not accurate: *eventType* [5] (i.e. *Dangerous Situation -> Electronic Emergency Brake Lights* [5])	Consider the case where a DENM message is received, and the cause code indicates an emergency brake warning event, even though the trigger / cause for the DENM message was another less critical event. Impact: • RxV receives the message and determines that there is an EBW event • The emergency brake warning is provided to the human driver via the HMI • The human driver of RxV applies the brakes hard • A following Vehicle (FV), which is not V2X equipped, crashes into the rear end of RxV
	H#8	Field within EBW message is not present or is not accurate: *detectionTime* [5]	To be completed
	H#9	Field within EBW message is not present or is not accurate: *informationQuality* [5]	To be completed
	H#10	Field within EBW message is not present or is not accurate: *stationType* [5] (what sort of vehicle generated the EBW message)	Consider the case where the value is not accurate and is set to a value corresponding to a station type that could not send an emergency brake warning, for example if *stationType* is set to *roadSideUnit* or *Pedestrian* RxV rejects the message and impacts are similar to those of H#3
MORE	H#11	TxV sends a correctly formatted EBW message even though it is not actually undergoing an emergency braking event. (more)	• RxV receives the message and determines that there is an EBW event • The emergency warning is provided to the human driver via the HMI • The human driver of RxV applies the brakes sharply • A following Vehicle (FV), which is not V2X equipped, crashes into the rear end of RxV
LESS	H#12	To be completed	To be completed
AS WELL AS	H#13	To be completed	To be completed
PART OF	H#14	To be completed	To be completed
REVERSE	H#15	To be completed	To be completed

OTHER THAN / INSTEAD	H#16	To be completed	To be completed
EARLY	H#17	To be completed	To be completed
LATE	H#18	Message is sent too late to provide any value (the V2X EBW use case only provides value if it is provided before the human driver can see the emergency braking event with their own eyes)	As H#1
BEFORE	H#19	To be completed	To be completed
AFTER	H#20	To be completed	To be completed

Table 5-2-2: Hazards identified for Operational Situation #1, EBW Scenario 1

Similar tables to that produced above may be produced for other Operational Situations and also for EBW Scenario 2.

5.2.2.2 Classification of hazards: Operational Situation #1, EBW Scenario 1

In the table below, the right-hand column gives an estimate of both the lowest possible ASIL rating and the highest possible ASIL rating. From this, a range of possible ASIL values is determined. The specific ASIL rating for a particular hazard may require more analysis and discussion than has been provided here, and/or there may be dependencies on the details of the Operational Situation, such as TxV and RxV speed and the distance between TxV and RxV at the time of the emergency braking event. In classifying exposure, severity and controllability, the guidelines provided in [12] have been applied.

Hazard	**Hazard Category**	**Exposure**	**Severity**	**Controllability**	**ASIL rating (possible range)**
H#1	Message not sent when should be sent	• Highway driving at relatively high speed in busy traffic occurs > 10% of time • Cars following relatively closely behind occurs > 10% of time • But emergency brake events are rare (assume less than once a year, or a few times a year) • Classification: Exposure is low: E1-E2	• Rear-ending on a highway could cause life-threatening injuries, or worse • Classification: S2-S3 (depends on speed of impact, see Table B.1 [1])	• Human drivers have to rely on their own senses, which the means that the emergency braking of vehicles in front must be visible. Given that Operational Scenario #1 is one where the highway is assumed to be busy, this the means controllability will be limited	QM→B E1-S2-C3=QM E2-S3-C3=B (Indicative values. Further and deeper analysis needed to

				• Assume C3 (10% or more of drivers find it difficult to control, or uncontrollable).	establish confidence)
H#4.1	Content of message inaccurate	• Highway driving at relatively high speed in busy traffic occurs > 10% of time • Cars following relatively closely behind occurs > 10% of time • Likelihood that a vehicle following RxV is not V2X equipped is high, especially during early years of roll-out • However, receiving an emergency brake warning message is a rare event (less than once a year, or a few times a year) • Classification: Exposure is low, E1-E2	• Rear-ending on a highway could cause severe and life-threatening injuries, or worse • Classification: S2-S3	• Drivers of RxV will come to trust the warning messages; if the driver receives an EBW message, and they know that they need to react to it by braking hard, (e.g. because the HMI is a replay of an audio recording saying 'brake hard') then most drivers will do so; hence we can assume that at least 10% or more of RxV drivers are unable to avoid the specified harm (a following vehicle crashing into them). • Similarly cars following RxV, which are assumed to be <u>not</u> V2X equipped, may get no other indication that the car immediately in front is about to brake hard due to the nature of the failure (TxV location information being inaccurate), since the actual vehicle that is undertaking the emergency braking may be nowhere in visual sight (e.g. may be far ahead, in a different lane, or even travelling in a different direction); this means that controllability for the driver of the following vehicle is also poor if the driver of RxV does decide to apply the brakes hard • Classification: C3	QM→B E1-S2-C3=QM E2-S3-C3=B (Indicative values; further and deeper analysis needed to establish confidence)
H#7.1	Content of	• See Appendix F for the detailed computation)	• See Appendix F for the detailed computation)	• See Appendix F for the detailed computation)	B E4-S2-C2=B

	message inaccurate				(See Appendix F for the detailed computation)
H#11	Message sent when should not be sent	• Highway driving at relatively high speed in busy traffic occurs > 10% of time • Cars following relatively closely behind occurs > 10% of time • Likelihood that a vehicle following RxV is not V2X equipped is high, especially during early years of roll-out • Classification: Exposure is high: E4	• Rear-ending on a highway could cause severe and life-threatening injuries, or worse • Classification: S2-S3	• Classification: C3 • Explanation for this rating is as for H#4.1	C→D E4-S2-C3=C E4-S3-C3=D (Indicative values; further and deeper analysis needed to establish confidence)
H#18	Message not sent at right time	• Classification: Exposure is low: E1-E2 • Reasons as per H#1	• Classification: S2-S3 • Reasons as per H#1	• Assume C3 (difficult to control, or uncontrollable) • Reasons as per H#1	QM→B E1-S2-C3=QM E2-S3-C3=B (Indicative values; further and deeper analysis needed to establish confidence)

Table 5-2-3: Classification of hazards identified for Operational Situation #1, EBW Scenario 1

Note: A question that arises is whether an error in the cause code alone could be interpreted as an EBW event, or whether the presence or absence of other data elements in the 'host' DENM message might rather cause RxV to reject the message. In this regard according to [11] the only mandatory data element (other than cause code) that has to be passed from the EBW application to the DEN basic service layer is EventSpeed. Which should be interpreted by RxV as 'Speed of the hard-braking vehicle when the event is detected'. The EBW message shall also include 'relevance area' information (distance and direction). It can be seen from inspection of [11] that therefore the format of the EBW

message is very similar to that of the 'traffic condition' warning message, which also has, EventSpeed (intended to indicate 'moving speed of the traffic jam endpoint' to the receiving ITS station) as its only mandatory data element that needs to be passed down from the application to the DEN basic service layer. The traffic condition message, like that of EBW shall also include 'relevance area' information. 'Traffic condition' is likely to be a very frequently encountered DENM message, since it can be used to indicate traffic jams and changes in traffic jam conditions. Other than in cause code, it appears that the only other difference between mandated fields in the messages is that the sub-cause code value has 8 possible values (0-7) in the EBW message and 9 values (0-8) for the 'traffic condition' message. This example illustrates the plausibility for a corruption or incorrect setting of cause code (or the ASN.1 coding thereof) of a 'traffic condition' message to result in a commonly occurring and potentially non-critical 'traffic condition' DENM message being interpreted by RxV as an EBW message, with potential for serious adverse consequences.

5.2.2.3 Classification of hazards: Operational Situation #1, EBW Scenario 2

Hazard	Hazard category	Exposure	Severity	Controllability	ASIL rating (possible range)
H#7.1	Content of message inaccurate	See Appendix F	See Appendix F	See Appendix F	C E4-S2-C3=C (Detailed analysis provided in Appendix F)

Table 5.2.4) Classification of hazards identified for Operational Situation #1, EBW scenario #2

Similar tables to that produced above may be produced for other operational scenarios.

5.3 Safety Goals

5.3.1 Functional Safety Concept: EBW Scenario 1, Operational Situation 1

Table 5-3-1 shows the safety goals and Tables 5-4-1 and 5-4-2 show Potential Functional Safety Requirements (PFSR). The PFSR are inspired by the HARA analysis of Section 5.2. The Functional Safety Requirements are marked as being 'potential', because there may be multiple ways of meeting a safety goal, and the most preferred way is addressed in Section 5.5. Since the objective of this work is to capture the key classes of issue that need to be considered, some requirements are described using terms from ETSI message definitions, while others may be described in terms of SAE message definitions.

5.3.1.1 Safety Goals

Hazardous event and associated risk	Safety Goal	Possible ASIL ratings for selected hazardous events

Unintended braking of the car RxV that receives a V2X message causes a vehicle that is following RxV to crash into RxV	**SG1**: Avoid or mitigate unintended braking if there are following vehicles	H#4.1 (see Table 5-2-3): • Somewhere in range QM→B H#7.1, H#11 (see Table 5-2-3): • Somewhere in range C→D
Car does not brake early enough due to EBW message not being received, or being received but being unactionable for some reason, thus causing a following vehicle to crash into the car or for the car to crash into a vehicle that is in front of it	**SG2**: Avoid or mitigate the situation where a car does not brake when it should	H#1 (see Table 5-2-3): • Somewhere in range QM→B H#18 (see Table 5-2-3): • Somewhere in range QM→B

Table 5-3-1: Safety goals for EBW Scenario 1, Operational situation 1

5.4 Functional Safety Requirements

5.4.1 Potential Functional Safety Requirements for Safety Goal #1 (SG1)

SG1: Avoid or mitigate unintended braking if there are following vehicles.

Note: ISO 26262 Part 3, Section 7.4.2.3 [1] lists a number of strategies that can be considered in determining Functional Safety Requirements: fault avoidance, fault detection and control of faults, transitioning to safe state, fault tolerance, degradation of functionality, driver warnings, avoidance or mitigation of hazardous event, etc. PFSR are organised in the tables below according to the category of fault and the strategy deployed to deal with that fault.

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)	Comment

TxV	**FC1:** EBW message transmitted when it should not have been	**Strategies for fault avoidance:**
		• **PFSR-FC1-1 (Requirement on TxV)**: Information that is used by the V2X application in triggering the creation and sending of an EBW message shall be accurate
		• **PFSR-FC1-2 (Requirement on TxV):** Content of messages created as a result of other triggering conditions shall be accurate (such that they do not provide a mechanism for creating 'false' EBW messages – e.g. an error in *eventType* could result in a 'traffic condition' warning message being transmitted as an EBW message)
		
		Strategies for fault detection and mitigation:
		• **PFSR-FC1-3 (Requirement on RxV):** Corroborate the validity of the emergency braking event through other the means in RxV and do not raise a warning to the human driver over HMI until sufficient corroboration is available.
		  • **PFSR-FC1-3-1 (Requirement on RxV):** Corroborate the validity of the emergency braking event through use of ego-sensors in the RxV, e.g. radar, lidar etc.
		  • **PFSR-FC1-3-2: (Requirement on: All vehicles, RxV):** Corroborate the validity of the emergency braking event through information received over V2X from other vehicles, either:
		  o i) EBW V2X messages received from other vehicles (e.g. if the road is congested, then other vehicles in the vicinity of the braking vehicle might also be expected to create EBW messages)
		  o ii) Content of CAM/BSM messages transmitted by other vehicles (which might e.g. indicate rapid deceleration)
		
		Strategies for fault detection and transition to safe state:
			See Hazard H#11 (Table 5-2-3).
			
			PFSR-FC1-3: Corroboration is not always possible (e.g. position given by TxV in the EBW message may be out of line of sight of other RxV ego-sensors, V2X info from other vehicles may be unavailable etc.)
			
			Another issue is that if RxV waits for corroborating information then time to react could be lessened, thereby increasing the potential of a collision on occasions where there is a genuine EBW event
			
			PFSR-FC1-4: The control loop is very slow, a CRL may get published and distributed very infrequently

		• **PFSR-FC1-4 (Requirement on: All vehicles, TxV, MA):** Cars that receive an EBW message from a car that is not undergoing emergency braking may raise a Misbehaviour Report (MBR) to a Misbehaviour Authority (MA). The MA may include indication of TxV's certificates on a CRL. When TxV learns that it has been placed on a CRL, TxV shall cease transmitting messages using the V2X service. In addition, cars receiving messages from TxV can ignore them • **PFSR-FC1-5 (Requirement on TxV):** A simple monitor function that is separate from the main V2X application, shall perform a plausibility test before allowing an EBW message to be transmitted. Such a 'simple' monitor function may for example include its own in-built accelerometer. If the plausibility test is not passed TxV may (tbd) prevent itself from transmitting future EBW V2X messages and thereby move itself to a 'safe state'	
TxV	**FC2:** Content of transmitted EBW message not accurate	The following PFSR's apply for informational content inaccuracies in any of the following: • Location (*eventPosition*): values for: longitude, latitude, altitude with confidence ellipse values x, y, z • Traffic direction (*relevanceTrafficDirection*): values upstream, downstream, opposite • Cause (*eventType*): many values, e.g. traffic condition, accident, roadworks, weather, dangerous situation etc. **<u>Strategies for fault avoidance:</u>** • **PFSR-FC2-1 (avoid):** The content of information that is included in transmitted EBW messages shall be accurate. • **PFSR-FC2-2 (avoid):** The format of the transmitted EBW messages shall be correct (standards compliant). **<u>Strategies for fault detection and mitigation:</u>** Requirements in PFSR-FC1-3 (above) also applies to mitigating this fault (FC2), where we would extend the requirement to state that not just the	See e.g. Hazards H#4.1, H#7.1 (Table 5-2-3) PFSR-FC2-3: pseudonymous identity change may be a problem

		validity of the EBW event is corroborated but also the content within the EBW message is corroborated. • **PFSR-FC2-3 (Requirement on: RxV, TxV):** corroborate the content of the EBW message through historical (e.g. path trajectory) information for TxV (e.g. as obtained from historic TxV CAM/BSM messages) • **PFSR-FC2-4 (Requirement on RxV):** corroborate the content of the EBW message through use of other information provided within the EBW V2X message itself (for example SAE messages include information used in threat assessment such as *DF_PathHistory, DE_BrakeSystemStatus, DE_SteeringWheelAngle*) **Strategies for fault detection and transition to 'safe state'** PFSR-FC1-4 also applies to this fault category (FC2)	
TxV, RxV or Channel	**FC3:** EBW message corrupted during radio transmission or reception	**Strategies for fault detection and mitigation:** • **PFSR-FC3-1 (Requirement on RxV and TxV):** An error detection (e.g. CRC) code is included by TxV and a check of that code shall be performed by RxV to see whether the message is corrupted and if so, the message is not passed up from PHY to higher layers of RxV	Example of hazardous event: A non-EBW message could be corrupted (e.g. a bit flip on cause code) resulting in it being received as an EBW message, which if processed could cause unintended braking
RxV	**FC4:** Content of EBW message is received correctly by RxV PHY but is not processable by the application	**Strategies for fault avoidance:** • **PFSR-FC4-1 (Requirement on RxV):** The EBW message shall be processed by the receiver hardware and software (including protocol stack) and shall be passed through to the V2X application without errors being introduced.	Example of hazardous event: A non-EBW message could be corrupted in the receiver stack (e.g. a bit flip on cause code) resulting in it being interpreted by the application layer as an EBW message, thereby causing unintended braking.
RxV	**FC5:** RxV ego sensor information available to application is erroneous	**Strategies for fault avoidance:** • **PFSR-FC5-1 (Requirement on RxV**): RxV ego-sensor information that is made available and used by the V2X application (such as time, location, direction) shall be sufficiently** accurate ** values tbd	This hazardous event and associated risk was not analysed in Table 5-2-3; if RxV ego sensor information available to the RxV application is incorrect then this could cause unintended braking (e.g. if location according to the ego-sensors is wrong and RxV determines that it is behind TxV when in fact it is in front of TxV)

RxV	**FC6:** RxV application is faulty	**Strategies for fault avoidance:** • **PFSR-FC6-1 (Requirement on RxV):** The application in RxV shall not trigger the sending of a warning to the human driver without cause (i.e. without having just received a V2V EBW message, or without some other indication from sensors that there is a genuine emergency braking event ahead)	This hazardous event and associated risk was not analysed in Table 5-2-3; a faulty application design or operation could result in unintended HMI warnings being generated
RxV	**FC7:** RxV HMI is faulty	**Strategies for fault avoidance:** • **PFSR-FC7-1 (Requirement on RxV):** The HMI in RxV shall not make a warning to the human driver without cause (i.e. without having been triggered to produce such a warning from the V2X EBW application)	This hazardous event and associated risk was not analysed in Table 5-2-3; a faulty HMI could cause unintended warning messages, leading to unintended braking
N/A	N/A	**Strategies for mitigation of hazardous event:** • **PFSR-SYS-1 (Requirement on RxV):** RxV shall send an EBW message to other vehicles when undertaking emergency braking in response to receiving an EBW message (in this way a driver warning may be provided to drivers in the following vehicles, which may help in preventing a collision)	Only useful if the following vehicle(s) are V2X equipped

Table 5-4-1: Potential Functional Safety Requirements for EBW Scenario 1, Operational Situation #1 related to Safety Goal #1

5.4.2 Potential Functional Safety Requirements for Safety Goal #2 (SG2)

SG2: Avoid or mitigate the situation where a car does not brake when it should brake.

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)	Comment
TxV	**FC8:** EBW message is not transmitted when it should have been	**Strategies for fault avoidance:** • **PFSR-FC8-1 (Requirement on TxV)**: Emergency braking events shall be detected and the corresponding required sensor information shall be provided accurately and with sufficiently** low latency to the EBW application in TxV. • **PFSR-FC8-2 (Requirement on TxV)**: On receiving sensor information indicating emergency braking the V2X application shall generate a correctly formatted EBW message and have it ready for transmission on MAC/PHY layer with sufficiently** low latency [** values of latency tbd] **Strategies for avoidance or mitigation of hazardous event:** • **PFSR-FC8-3 (Requirement on all vehicles, RxV)**: Other vehicles in the vicinity of TxV shall create EBW messages if they undertake emergency braking themselves. RxV shall use these messages (or absence of any such messages) to determine whether a warning needs to be provided to the human driver of RxV • **PFSR-FC8-4 (Requirement on all vehicles, RxV)**: RxV uses speed/acceleration/deceleration information in the CAMs/BSMs from other vehicles in the vicinity of TxV to determine whether a warning needs to be provided to the human driver of RxV • **PFSR-FC8-5 (Requirement on RxV):** Use ego-sensors of RxV (e.g. Lidar, Radar, camera) to detect emergency braking ahead, which can then be used to create the alert to the human driver of RxV	See e.g. Hazard H#1 (Table 5-2-3) PFSR-FC8-2: It may be that different manufacturers may have different triggering condition criteria, e.g. one manufacturer may not send the EBW message when the road conditions are icy, while another may always send it PFSR-FC8-5: Ego-sensors in RxV may only work where TxV is in the line of sight
TxV	**FC2 (as already listed above):** Content or format of	**Avoidance strategies:** • PFSR-FC2-2 as already listed above also applies here	Incorrect location or traffic direction could result in RxV discarding a message as being irrelevant to RxV.

	transmitted EBW message not accurate	• PFSR-FC2-1 as described above also applies here (covering location, traffic direction and cause type information), but in addition some new information elements are identified, hence we define a new PFSR • **PFSR-FC2-3 (Requirement on TxV):** The content of information that is included in transmitted EBW messages shall be accurate. The PFSR shall apply for informational content inaccuracies in any of the following: • Station type	Incorrect cause type could lead to action that is not braking or could lead to inaction. Incorrect station type could lead to RxV ignoring or discarding the message (for example an emergency braking message from an RSU could be discarded as meaningless), see Hazard H#10 (Table 5-2-3)

TxV, RxV or Channel	**FC9**: Radio system does not provide intended coverage and latency	**<u>Avoidance strategies:</u>**
		
		• **PFSR-FC9-1 (Requirement on TxV, RxV):** The communication system performance shall be such that the message is receivable without error by *X*% of vehicles within a range *Y* under traffic conditions *Z* and within time *T*
		  ○ 'Traffic conditions' refers to speed of vehicles and number of vehicles in unit area of road.
		  ○ Time *T* is measured with respect to the time that the message is available for transmission at the MAC/PHY layer in TxV.
		  ○ All parameters are tbd.
			See H#18 (Table 5-2-3)

RxV	**FC4 (as already listed above):** Content of EBW message is received correctly by RxV PHY but is not processable by the application	**<u>Avoidance strategies:</u>** • PFSR-FC4-1 as already listed above, applies here also	Example of hazardous event: an EBW message could be corrupted in the receiver stack (e.g. a bit flip on cause code) resulting in it being uninterpretable by the V2X application
RxV	**FC5 (as already listed above):** RxV ego sensor information available to application is either	**<u>Avoidance strategies:</u>** • PFSR-FC5-1, as already listed above applies here also • **PFSR-FC5-2 (Requirement on RxV**): RxV ego-sensor information that is needed by the V2X application (such as time, location, direction) shall be available	This hazardous event and associated risk was not analysed in Table 5-2-3. If RxV ego sensor information available to RxV application is incorrect then this could prevent braking from occurring. For example, if location according to the ego-

	unavailable or erroneous		sensors is wrong and RxV 'believes' it is in front of TxV when in fact it is behind TxV.
RxV	**FC6 (as already listed above):** RxV application is faulty	TBD: • Unclear how to write a fault avoidance requirement without specifying the algorithm in the V2X application that determines when warnings should be provided	This hazardous event and associated risk was not analysed in Table 5-2-3; a faulty application design or operation could result in an HMI warning not being generated, even though it should have been generated
RxV	**FC7 (as already listed above):** RxV HMI is faulty	TBD: • Unclear how to write a fault avoidance requirement without specifying more details of the HMI system design (e.g. whether it is a 'dumb' system that is expected to create warnings when told to, or whether it is 'smart' and may take into account e.g. cognitive load on the human driver in determining when or whether to raise a warning)	This hazardous event and associated risk was not analysed in Table 5-2-3; a faulty HMI could mean that a warning to the human driver is not provided, even though it should be

Table 5-4-2: Potential Functional Safety Requirements for EBW scenario 1, Operational Situation #1 related to Safety Goal #2

6 Analysis

6.1 General

The safety analysis carried out in the Chapters 4 and 5 has shown that in both selected exemplary use cases potential hazards can be identified, which need to take into account treatment of Functional Safety. A number of Safety Goals have been formulated for both cases which, in turn, generate requirements in the overall system comprising the selected functions. The analysis has further shown that for the identified safety requirements there are ideas for potential solutions. A final dedicated safety concept is not in the scope of this analysis and needs to be selected in the concrete definition of the system architectures for the final products.

Solutions cannot solely concentrate on functional safety but need to take into account a reasonable trade-off between safety, availability, security and the overall performance requirements. Figure 6-1 shows this area of trade-off that need to be mutually optimized.

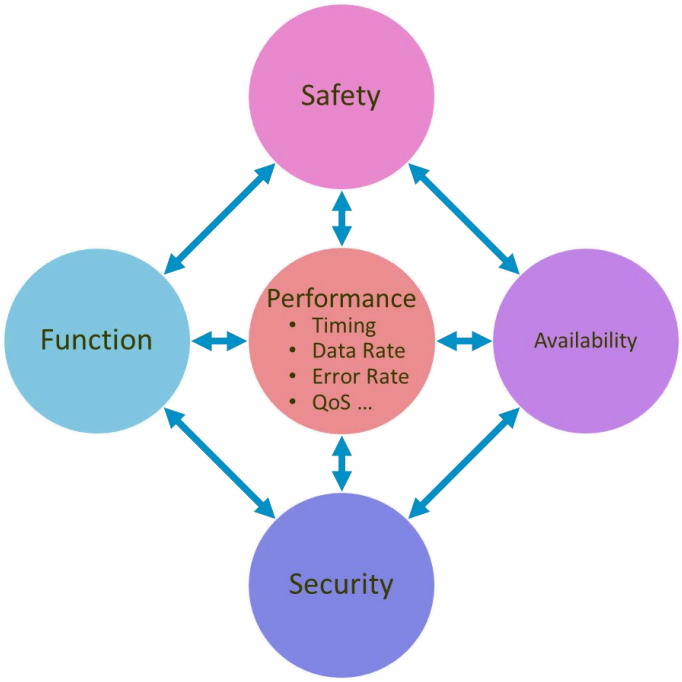

Figure 6-1: Overall trade-off between different functional requirements

Discussions in 5GAA during the work carried out in STiCAD have further shown where parts of the overall system may not be handled by the existing functional safety concepts of the automotive sector. For example, it is unlikely that an introduction of ISO26262 concepts might ever be applied in the cellular networks due to technical and economic reasons. However, this does not mean that use cases with functional safety Requirements such as those investigated cannot be implemented. The analysis carried out has shown that the black-channel concept (see Chapter 7.2) coupled with a safe monitoring of the black channels can cope with functional safety needs.

6.1.1 Potential standardisation approaches

The potential approaches to standardisation discussed in this section apply to both the ToD and the EBW use cases. Hence, for the purposes of this discussion, two new terms are defined:

- Transmitting endpoint (Tx_EP): in the EBW use case this corresponds to TxV, while in the ToD use case (which involves bidirectional communications), it corresponds either to the control centre (CC) transmit path or the controlled vehicle (CV) transmit path

- Receiving endpoint (Rx_EP): in the EBW use case this corresponds to RxV, while in the ToD use case (which involves bidirectional communications), it corresponds either to the CC receive path or to the CV receive path

At least the two following fundamentally different safety engineering approaches could be considered in addressing the standardisation challenges:

- Holistic single system safety engineering approach
- Modular engineering approach

6.1.1.1 Holistic single system safety engineering approach

In this approach, one entity specifies the key high-level aspects of the system, from both a functional and non-functional (safety) standpoint. However, with a V2X system, because different manufacturers may have built Tx_EP and Rx_EP, the single entity responsible for defining these key aspects of the overall system design and Functional Safety Concept would be an independent industry association or standards body.

6.1.1.2 Modular engineering approach

In this approach, the vendor of Tx_EP and the vendor of Rx_EP are allowed to make independent safety engineering decisions. The Tx_EP then communicates to Rx_EP any safety related information at run-time (i.e. in the V2X message). This information might be in the form of some safety information that is signed by a certification authority. The Rx_EP then makes a determination as to how and whether the message received from the Tx_EP should be acted upon based on the safety relevant information it has received from the Tx_EP.

6.1.1.3 Comparison of holistic and modular approaches

Standardisation issue	Holistic approach	Modular approach
Agreeing the mapping of safety requirements to Tx_EP and Rx_EP	• Pro: Vendors of both Tx_EPs and Rx_EPs know exactly what they need to do from a safety engineering perspective since the standardisation body would have specified it • Con: Undertaking a safety engineering exercise even for just the two V2X applications considered herein has been very time-consuming, as we have seen in this study, and there are of course many more V2X applications than just EBW and ToD. Hence agreeing, at an industry level, such safety engineering analyses and the preferred mitigations for them might prove very time consuming and it may turn out that it could not fully cover possible similar use cases that encompass some differences falling outside what is defined, thus delaying the whole process. In general, the approach requires heavy standardisation details	• Pro: Designers of Tx_EP and Rx_EP have autonomy in the safety engineering approaches that they choose to adopt, which reduces the need to obtain industry agreement (noting that the latter could be very time-consuming) • Con: Risk that designer of Tx_EP and designer of Rx_EP make different choices/assumptions regards split of requirements across Tx_EP and Rx_EP (e.g. vendors of Tx_EP assume vendors of Rx_EP will implement mitigations, and vice-versa). The consequence could be that the overall functional safety concept for the item does not meet the safety goals or that similar functions are treated very differently by different companies designers
Agreement on ASIL level to be used	• Pro: The standard could define the ASIL level to be applied in both Tx_EP and Rx_EP and in this way overall system safety assurance can be guaranteed • Con: Agreeing, at an industry level, the ASIL levels to be used for each V2X application might prove time-consuming and new uses cases deployment could be delayed by the lack of definition	• Pro: No industry agreement needed; this could favour a cooperative approach through 'alliances' that could share common approaches, but at the risk of different solutions based on difference alliances created in the marketplace • Con: Need to determine and standardise new messaging, to enable a Tx_EP to indicate its (potentially certified) ASIL level to the Rx_EP • Con: Risk that the designer of Tx_EP and the designer of Rx_EP make different choices/assumptions regarding ASIL level requirements, so additional new functionality

Standardisation issue	Holistic approach	Modular approach
		would need to be included in the Rx_EP design to handle the possibility that ASIL Level used in Tx_EP system is smaller than the ASIL level assumed necessary by Rx_EP designer. More work would seem to be necessary to better understand how this problem might be managed: o For example, in a one-way communication like that of EBW this might be managed by an Rx_EP choosing not to apply the brakes with the force that would be desirable due to a lack of trust or 'trust deficit' associated with the received V2X message o In two-way communication, such as a negotiated lane merge, or four-way stop management, where cars signal intention to manoeuvre, it would need to be discussed/ determined what an ASIL *N+1* Rx_EP should do with a manoeuvre intention message received from an ASIL *N* Tx_EP
Handling system integration testing, verification and validation	• Pro: A full end-to-end system assessment would be done for each possible combination of Tx_EP and Rx_EP, perhaps in some kind of safety engineering 'plugtest' • Con: This would be very time-consuming and might be logistically problematic as new vendors or new variants of modules are produced	• Pro: The testing, verification and validation is done separately for Tx_EP and Rx_EP, and can be done solely by the manufacturer that is producing the specific function • Con: All possible end-to-end systems (combinations of Tx_EP and Rx_EP from different vendors) are not tested as complete systems. Rather, an assumption is made that when the item/system 'comes into being' during run-time (Tx_EP sends message to Rx_EP), then the complete system will implicitly meet the testing, verification and validation safety engineering requirements targeted by ISO 26262 (whether this is indeed likely to be the case is for further study)

Standardisation issue	Holistic approach	Modular approach
		• Con: new vendors may be excluded in the first phases of testing, creating unbalanced market situations
Certification	• Each possible combination of Tx_EP and Rx_EP is individually tested and certified • A Tx_EP would have to provide Certificate Authority signed Tx_EP identity so that Rx_EP could determine whether the combined system Tx_EP+Rx_EP has been approved (whether there might be tracking/privacy concerns with this would have to be considered further)	• Each Tx_EP is individually certified for the adequacy of its functional safety engineering (e.g. with a signed ASIL), and this is communicated by Tx_EP to Rx_EP

Table 6-1-1-3-1: Comparison of 'holistic' and 'modular ' approaches from a standardisation viewpoint

6.2 ToD related

The safety design for V2N-based functions like ToD needs might be different for the different basic parts of the overall system. On the vehicle side, there might be standard functional safety treatment as defined in ISO26262, ISO21448 and other existing standards. On the vehicle control centre backend side, it also might be possible to apply those or other similar concepts. On the communication network side, as mentioned before, it is unlikely that ISO26262 is the right concept. It is more likely that the network is handled as a black channel and that monitoring on both sides connected to this network cares for assuring the functional safety (e.g. concepts of adding and validating checksums to ensure the correctness of received data in safe monitoring components on the sending and receiving side of data). As mentioned before, assuring functional safety is just a part of the overall story. By just adding safe monitoring capabilities on both sides of the black channel and providing system degradation concepts or concepts for entry into safe states when monitoring shows a severe problem. The system itself might be safe, but availability of the overall system might not be sufficient or the time needed for checking might not be short enough to ensure reasonable functioning of the use case or security checks might take too long and thus take the communication out of its timing requirements. A reasonable design of the system needs to take into account the different capabilities that are available on each system part and combine those concepts to an overall system that fulfils all the given requirements.

On the network side, the analysis has shown that the main emphasis should be given to providing the right means for reasonably monitoring the availability of the communication and to keep the general performance of the network at a reasonable value, as often as possible. Outages of the network might be tolerable as long as they are safely monitored on both ends of the black channel and as long as they are unlikely to keep the overall availability of the function at an acceptable level. Which level is acceptable depends on customer willingness to accept such outages and on product and economic boundaries.

It is important to underline that when the different parts of the overall system (e.g. the vehicle, network and vehicle control centre in the ToD case) are designed jointly, the aforementioned considerations might be reasonable. If, however, the design of those subsystems is done independently (e.g. by different system components suppliers), another dimension comes into play. In order to allow setups that, for instance, allow independent control centres regulate a variety of separately developed vehicles over independently operated networks, it needs agreements in, for example, the form of standards. Not only the interfaces or technical

concepts need to be standardised, but the overall safety framework needs to be agreed upon. The proposals for mutual trust concepts like those described in Chapter 7.3 sketch how such agreements could look. As depicted in Chapter 6.3 for the V2V case, similar questions arise for the V2N case. Examples could be:

- Minimum frequency of the messages exchanged
- Jointly agreed security concepts for the communication between backend and vehicle side
- QoS agreements between the cellular network operators and the customers (OEMs, backend vehicle control centre operators)
- Agreements on the qualification of the tele-operator generally and for certain types of vehicles.
- Agreements on homologation concepts on both sides
- Agreements on authentication and related certificates
- Commonly agreed general safety concepts
- Mutual certification of vehicles and control centres
- Legal agreements between the different stakeholders

6.3 EBW Related

6.3.1 Potential needs for industry collaboration and standardisation related to safety engineering

The manufacturer of a V2X module in a TxV may be different to the manufacturer of a V2X module in a RxV. This means that no single manufacturer has safety engineering oversight of the complete system.

Therefore, from a standardisation point of view there are at least the following aspects that need to be considered:

- If there are a variety of potential solutions for avoiding or mitigating faults that allocate requirements to TxV and RxV in different ways, then which one is chosen?
- How is it ensured that designers of TxV and RxV:
    - Design their systems to the same ASIL level?
    - Manage the possibility that the designer of the RxV module and the designer of the TxV module have assumed different ASIL levels?
- Provision of necessary information to the function owner: the responsibility for each function implemented in a car must lie with a single owner who is the designer of the function. Under this approach, the function owner needs to determine the reliability of the information received from other vehicles. This can, in turn, result in new standardisation requirements, such as for the inclusion of additional information in transmitted V2X messages to convey safety relevant information. Associated with these messaging enhancements, there may also be the need to specify policy and governance processes that can offer assurances (e.g. by an independent third party/certification authority) on safety relevant information provided by TxV.
- How does the industry satisfy the requirements of system integration testing, verification, validation identified in functional safety engineering standards such as ISO 26262?
- Certification: conventionally, in order to provide more confidence that safety engineering is satisfactory, a third-party auditor (independent of the vendor of a system) may provide an assessment/audit which results in a certification that the system has met the required standard. How is such a third-party system-level safety assessment to be provided where vendors of TxV and RxV are different?

These standardisation-related considerations are now discussed in the sections below, for the cases where the study has yielded findings that can be used in addressing these questions (i.e. only for first three bullets above).

6.3.1.1 Agreeing on mapping of safety requirements to TxV and RxV

To assess potential difficulties in the mapping of safety requirements to TxV and RxV, we consider this question in the context of Safety Goal #1 (‘avoid unintended braking’).

For this Safety Goal #1, eight fault categories were identified in Section 5.4.

From a standardisation point of view, the fault categories of most interest to the present discussion are those where there are multiple potential solutions for mitigating the fault and where these solutions differ in terms of whether the safety requirements fall on TxV, RxV or in some combination. It is in these circumstances where there is the potential for uncertainty on the part of the TxV and RxV designers.

Only faults FC1, FC2, FC3 had PFSRs that identified requirements on both TxV and RxV, hence in the next step only these three fault categories are considered further.

Fault Location	Fault category	Potential Functional Safety Requirements (PFSR)	Analysis of PFSR
TxV	**FC1:** EBW message transmitted when it should not have been	**PFSR-FC1-1 (Requirement on TxV)**: Information that is used by the V2X application in triggering the creation and sending of an EBW message shall be accurate	A solution that meets this requirement might potentially comprise a number of aspects, for example: • More than one sensor might be implemented to make measurements of braking/deceleration, where a 'voting' system might be used to determine whether the sensor information is accurate • Special measures might need to be taken to manage risks that messages become inaccurate due to possible faults such as those that might occur in memory, internal messaging, protocol stack handling etc.
		PFSR-FC1-2 (Requirement on TxV): Content of messages created as a result of other triggering conditions shall be accurate (such that they do not provide a mechanism for creating 'false' EBW messages – e.g. an error in *eventType* could result in a 'traffic condition warning' message being transmitted as an EBW message)	Special measures might need to be taken to manage risks that messages become inaccurate due to possible faults such as those that might occur in memory, internal messaging, protocol stack handling etc.
		PFSR-FC1-3 (Requirement on RxV): Corroborate the validity of the emergency braking event through other means in RxV and do not signal a warning to the human driver over HMI until sufficient corroboration is available • **PFSR-FC1-3-1 (Requirement on RxV):** Corroborate the validity of the emergency braking event through use of ego-sensors in the RxV, e.g. radar, lidar etc. • **PFSR-FC1-3-2: (Requirement on: All vehicles, RxV):** Corroborate the validity of the emergency braking event through	In the **PFSR-FC1-3-1** case, evidence of emergency braking using Radar or Lidar could only come from measuring the deceleration of vehicles in the line of sight of RxV. The concern here is that such a limitation would mean that a prime benefit/motivation of V2X, i.e. its non-line-of-sight messaging, would not then be exploitable In the **PFSR-FC1-3-2** case the solution only works if there are other V2X-equipped vehicles in the vicinity of TxV, which there might not be

		information received over V2X from other vehicles, either: i) EBW V2X messages received from other vehicles (e.g. if the road is congested, then other vehicles in the vicinity of the braking vehicle might also be expected to create EBW messages), or in another example, corroboration might be possible through prior reception of a message, communicated over either PC5 or Uu, indicating an end of traffic jam in the vicinity of the location indicated within the EBW message ii) Content of CAM/BSM messages transmitted by other vehicles (which might e.g. indicate rapid deceleration)	
		PFSR-FC1-4 (Requirement on: All vehicles, TxV, MA): Cars that receive an EBW message from a car that is not undergoing emergency braking may generate/raise a misbehaviour report (MBR) to a misbehaviour authority (MA). The MA may include indication of TxV's certificates on a CRL. When TxV learns that it has been placed on a CRL, TxV shall cease transmitting messages using the V2X service, and cars receiving messages from TxV can ignore them	While the technique certainly provides benefits at a system level, the control loop is very slow and cannot be relied upon to deal with all eventualities, for example, there is the problem that faulty EBW messages could be sent in the period before certificate revocation occurs
		PFSR-FC1-5 (Requirement on TxV): A simple monitor function that is separate from the main V2X application, shall perform a plausibility test before allowing an EBW message to be transmitted. Such a function may, for example, include its own in-built accelerometer. If the plausibility test is not passed,	One could envisage at least two variants: • Variant #1 is a parallel radio-level solution: here the monitoring function in the TxV would be independent of the primary sensor and V2X Tx protocol stack and would have its own V2X radio receiver and accelerometer sensor. If the monitoring function does not find it plausible that a particular EBW message should

		TxV may (tbd) prevent itself from transmitting future EBW V2X messages and thereby move itself to a 'safe state'	have been sent, then it could generate a control message to prevent future generation of EBW messages by the TxV: ○ Pro: can detect faults from anywhere within the system, including the radio ○ Con: allows at least one faulty message to get transmitted • Variant #2 is a serial network layer solution: in this solution, once the V2X message is created in one of the layers above the radio stack (e.g. at a networking layer), it is first inspected by the monitoring function, which would have its own independent accelerometer sensor, before the message is authorised to be passed to the radio layers (e.g. Link and PHY) for broadcasting: ○ Pro: No faulty messages get transmitted (subject to con) ○ Con: Does not detect errors arising in the radio stack
TxV	**FC2:** Content of transmitted EBW message not accurate	**PFSR-FC2-1 (avoid):** The content of information that is included in transmitted EBW messages shall be accurate	See analysis for PFSR-FC1-1
		PFSR-FC2-2 (avoid): The format of the transmitted EBW messages shall be correct (standards compliant)	See analysis for PFSR-FC1-1
		PFSR-FC1-3 (Requirement on RxV): Corroborate the validity of the emergency braking event through other means than RxV, and do not raise/signal a warning to the human driver over HMI until sufficient corroboration is available • **PFSR-FC1-3-1 (Requirement on RxV):** corroborate the validity of the emergency braking event through use of ego-sensors in the RxV, e.g. Radar, Lidar etc. **PFSR-FC1-3-2: (Requirement on: All vehicles, RxV):** corroborate the validity of the emergency braking event through information received over V2X from other vehicles, either:	See analysis for this PFSR provided above for FC-1

		i) EBW V2X messages received from other vehicles (e.g. if the road is congested, then other vehicles in the vicinity of the braking vehicle might also be expected to create EBW messages), or in another example, corroboration might be possible through prior reception of a message, communicated over either PC5 or Uu, indicating an end of traffic jam in the vicinity of the location indicated within the EBW message ii) Content of CAM/BSM messages transmitted by other vehicles (which might e.g. indicate rapid deceleration)	
		PFSR-FC2-3 (Requirement on: RxV, TxV): Corroborate the content of the EBW message through historical (e.g. path trajectory) information for TxV (e.g. as obtained from historic TxV CAM/BSM messages)	Would appear to be a weak solution from an independence viewpoint. Specifically, the same fault could potentially cause the problems in both event triggered EBW DENM/BSM generation and periodic CAM/BSM generation. For example, if location information or lane information is inaccurate in an EBW event-triggered message, then for the same reason that information could be inaccurate when included in a periodic CAM/BSM message.
		PFSR-FC2-4 (Requirement on RxV): Corroborate the content of the EBW message through use of other information provided within the EBW V2X message itself (for example SAE messages include information used in threat assessment such as *DF_PathHistory* *DE_BrakeSystemStatus*, *DE_SteeringWheelAngle*)	The solution may potentially enable some faults to be detected if, for example, different sensors are used in producing the different information elements in the message, and if the faulty condition is arising from the sensor. However, the solution has weaknesses from an independence viewpoint, in that many system elements will be shared/common throughout the stack. In addition, there would likely only be a limited amount that could be inferred from any expected correlations between values in different information elements of the same message

		PFSR-FC1-4 (Requirement on: All vehicles, TxV, MA): Cars that receive an EBW message from a car that is not undergoing emergency braking may raise an MBR to a MA. The latter may include indication of TxV's certificates on a CRL. When TxV learns that it has been placed on a CRL, TxV shall cease transmitting messages using the V2X service, and cars receiving messages from TxV can ignore them	See analysis for this PFSR provided above for FC-1
TxV, RxV or Channel	**FC3:** EBW message corrupted during radio transmission or reception	**PFSR-FC3-1 (Requirement on RxV and TxV):** An error detection (e.g. CRC) code is included by TxV and a check of that code shall be performed by RxV to see whether the message is corrupted and, if so, the message is not passed up from PHY to higher layers of RxV	This fault category is already solved by existing standards

Table 6-3-1-1-1: Analysis of PFSRs for fault categories 1 through 3 associated with Safety Goal #1: avoid unintended braking

Under fault category 1 (FC1), we will consider a situation on the road where there could be some downside to trusting and fully acting on an EBW message that is falsely generated (such a situation might be one where acting on an EBW message might still result in a collision, but where the RxV predicts that such a resulting collision would be less severe than if the car were not to act on the EBW message). Where there are no downsides to acting on the EBW message, arguably the car may well act on the message. This situation, where determining trustworthiness is much less important, is of less interest for the purposes of our discussion here.

For FC1), in the aforementioned type of (trust-critical) road situation, it can be seen that there are at least two fundamentally different classes of functional safety concept:

Functional safety concept class 1) RxV requires corroboration before trusting, and fully acting on, an EBW message

> This approach has the advantage that an ASIL decomposition may be possible if the system(s) providing the corroborating information to the RxV is/are sufficiently independent from the main V2X EBW processing system/function. The cost of developing each individual system may therefore be reduced. However, the approach has the disadvantage that there may now be more systems/functions involved in making the decision (which will act in the direction of increasing cost). But perhaps a more significant disadvantage is that it will sometimes mean that either the car does not brake or that the car brakes later than it could have done because either the corroboration was not available or the corroboration comes at a later point in time than the EBW message. The impact of this could be an increase in the severity of the accident.
>
> Also, from the point of view of the V2X industry ecosystem as a whole, it might also result in a reduction in the value-add provided by V2X technology. To illustrate this point, one of the key differentiators of V2X is its ability to operate non-line of sight. However, if a designer of an RxV requires that there be corroboration from, for example, a (line of sight) Radar/Lidar before acting fully on the V2X EBW message, then the value-added provided by V2X, stemming from its non-line of sight operation, is not (fully) exploited.

Functional safety concept class 2) RxV does **NOT** require corroboration before trusting, and fully acting on, an EBW message

> In this approach, corroboration in the RxV is not required and the full benefits of V2X non-line-of-sight operation are enjoyed in all circumstances. Such an approach would have to place stronger and more demanding requirements on the TxV to ensure that EBW messages are only generated when the vehicle is truly undergoing an emergency braking event and also that the contents of safety critical information elements within the transmitted message are sufficiently accurate. Potential solutions that the transmitter designer could select from include:
>
> - Mechanisms for ensuring correctness of message generation and message contents in the main V2X path (from sensor through to RF transmission)
> - Redundant elements used for certain aspects (e.g. redundant sensors)
> - Use of an independent, separate, (but more basic) monitoring solution
>
> With this class of (non-redundant) functional safety concept, the RxV's main V2X EBW message processing path would also have to be designed to ensure that the necessary safety performance can be met. This might be achieved through paying increased attention to factors such as ensuring correctness in processing of messages and their contents, and ensuring accuracy in the values provided by ego-sensors, and the processing thereof, etc.

For FC2, the findings are similar to those described above, while for FC3 a solution is already provided by existing standards.

Summary

It has been shown that there are at least two fundamentally different classes of functional safety concept, one in which the RxV requires corroboration before acting and another that does not. Different companies may well have different opinions on which approach is to be preferred.

Based on the experience of undertaking the study of the EBW V2V application described in this TR, it can be expected that performing an analysis for all V2V applications and obtaining industry agreement on a single functional safety concept to be used for each, could well prove time-consuming. It is worth noting that, any industry agreement might only need apply to the TxV design, thereby giving designers of RxVs flexibility in the approach they choose to adopt.

In addition, instead of actually seeking to obtain industry agreement on a single functional safety concept, one potentially more time-efficient alternative approach could be for industry to agree that certain functional safety concepts **cannot** be assumed (at least from the point of view of designing TxV). For example, an industry standard might state that in performing safety engineering of the TxV, the designers should **not** assume that the RxV will perform corroboration. It is worth re-iterating that such an agreement would not prevent designers of RxVs from using corroboration, but would provide the option for RxV designers to not use corroboration if they do not wish to do so.

6.3.1.2 Agreement on ASIL level to be used

Based on the experience of undertaking this exercise and from literature review, it seems quite plausible that different safety engineers in different companies could come to different conclusions regarding the ASIL level required for any particular V2V application.

7 Candidate Solutions

In this chapter some potential solutions for the requirements stated in the chapters before are pointed out. The focus here lies on the measures that can be carried out on the communication side. The solutions do not pretend to be exhaustive but rather reflect the outcomes of the investigations made in the context of generating this document. However the potential solutions stated hereafter are tackling major open issues for safety in connected and distributed automotive functions and thus can serve as a good starting point for further investigations.

7.1 Network Failure Timing Analysis

There has been an analysis carried out at the beginning of the STiCAD work that has shown, that current network control mechanisms for recovery in case of network failure, even though they might inform the UE about this failure and trigger a network reselection of the UE, are not fast enough for very latency challenging use cases.

Therefore, if network mechanisms must be able to cope with such failures, the analysis has shown that new network control mechanisms are needed. When not following the black-channel approach (see Chapter 7.2) in the overall system definition, the conclusion is that there is some need for improvement on the network side.

7.2 Black-Channel Approach

7.2.1 Introduction

According to IEC 61508, when a safety function relies on communication in its implementation, the failure measure of the communication process shall be estimated. Transmission errors, such as repetitions and deletion, and random errors (e.g. corruption) should be considered. There are two approaches to implement techniques and measures for handling these threats to data communication:

- White channel: The entire communications channel is designed, implemented and validated according to IEC 61508 and relevant safety standards.

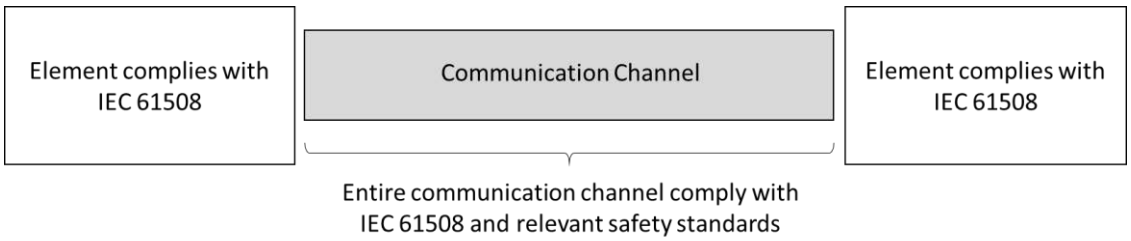

Figure 7-1: White channel

- Black channel: Part of the communication channel is not designed, implemented or validated according to IEC 61508. It bypasses the need for a safety certified communication system (white channel) but relies on end-to-end safety. The connected elements at both ends shall comply with IEC 61508.

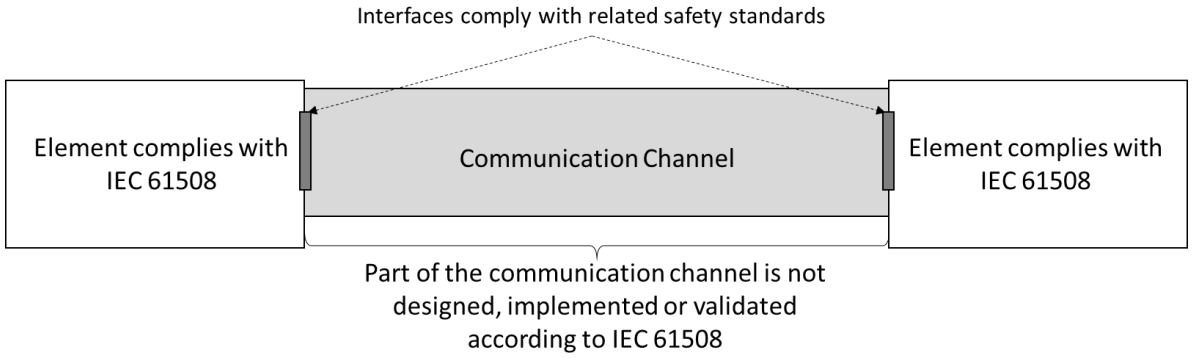

Figure 7-2: Black channel

With white-channel approach, the properties of the communication channel are properly defined and well known. Each of the components is designed with integrity levels and comply with IEC 61508 and relevant safety standards. However, designing and verifying each component of the communication channel according to safety standards can be very costly and may hinder the evolution towards new communication technologies or the possibility to utilise already deployed networks. Therefore, it is practically very difficult to develop and verify a wireless cellular communication system as a white channel.

Black channel looks like a better approach for communication of safety related data via wireless networks in terms of cost and flexibility. However, the black channel is associated with failure modes that could compromise the safety function integrity. When it is used for safety related data communication, there must be built-in mechanisms to detect any data error with enough confidence and additional diagnostics, or application functions at the connected elements, to reach the desired integrity level.

As a compromise, it can be assumed that the communication network is not a pure black channel, but provides control plane interfaces to reliably inform its state. This document lists such interfaces and provides examples; focus is on information that can be 'propagated' to an application, e.g. a monitoring function.

7.2.2 Architecture

Figure 7-3 shows the typical architecture of a vehicle communicating with Application Server(s) (ASs) located in the public internet and/or the (Multi-Access)[1] Edge Cloud (M)EC. The 3GPP network consists of a Radio Access Network (RAN) and Core Network. The Core Network and parts of the RAN are usually located in datacentres and cabinets of the Mobile Network Operator (MNO).

[1] In 5GAA context, the term Multi-Access Edge Computing (MEC) is commonly used while 3GPP specifications use the term Edge Computing and usually do not abbreviate it. This document therefore uses (M)EC to cover both contexts.

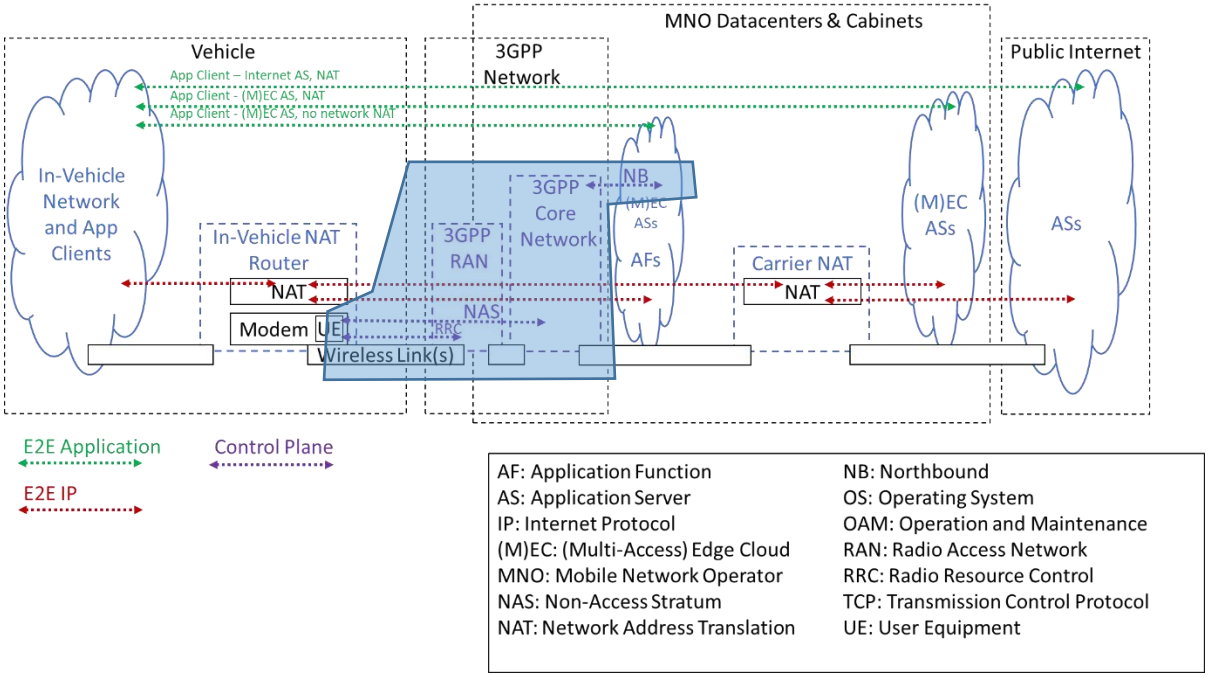

Figure 7-3: Typical architecture for a vehicle connected to a long-range cellular network; end-to-end, IP-layer and control plane connectivity is shown

(M)EC ASs and Application Functions (AFs) are usually also located in data centres and cabinets at the MNO. AFs interact with the Core Network through Northbound (NB) interfaces. On the vehicle side the User Equipment (UE) in the modem interacts with the RAN control plane through the Radio Resource Control (RRC) protocol and with the Core Network control plane through the Non-Access Stratum (NAS) protocol. Lower layers of the radio interface also implement control protocols but those are not shown since their interaction is usually hidden to higher layers.

Besides control plane interaction (marked as control plane and by the overlay polygon) also end-to-end application interaction (green) and end-to-end IP connectivity (red) is shown. IP, and strictly speaking also Transport Layer connectivity, are interrupted by Network Address Translation (NAT) routers. It is assumed that (M)EC ASs can be deployed before and after the network side NAT. For AFs it is assumed that they are deployed before the NAT.

Note: This assumption needs further evaluation.

For the vehicle it is also assumed that a NAT router is deployed providing connectivity to application clients in the vehicle.

Note: Initially, showing NAT might appear as unnecessary detail but for following extensions of this document we want to point out that any solution, e.g. to propagate information from NB to an application client in the vehicle, will also have to work in environments where these NATs are present.

Security is not covered in this chapter, but it is not precluded that the NAT router in the vehicle also includes firewall functions.

Figure 7-4 shows the protocol stacks at the client application in the vehicle, AS, AF and Core Network entities communicating with the AF[2].

[2] 3GPP 5G Core specifications TS 24.501 define a "3GPP trusted domain". AFs within this domain may communicate with any entity of the 5G Core network. This is not shown in the figure.

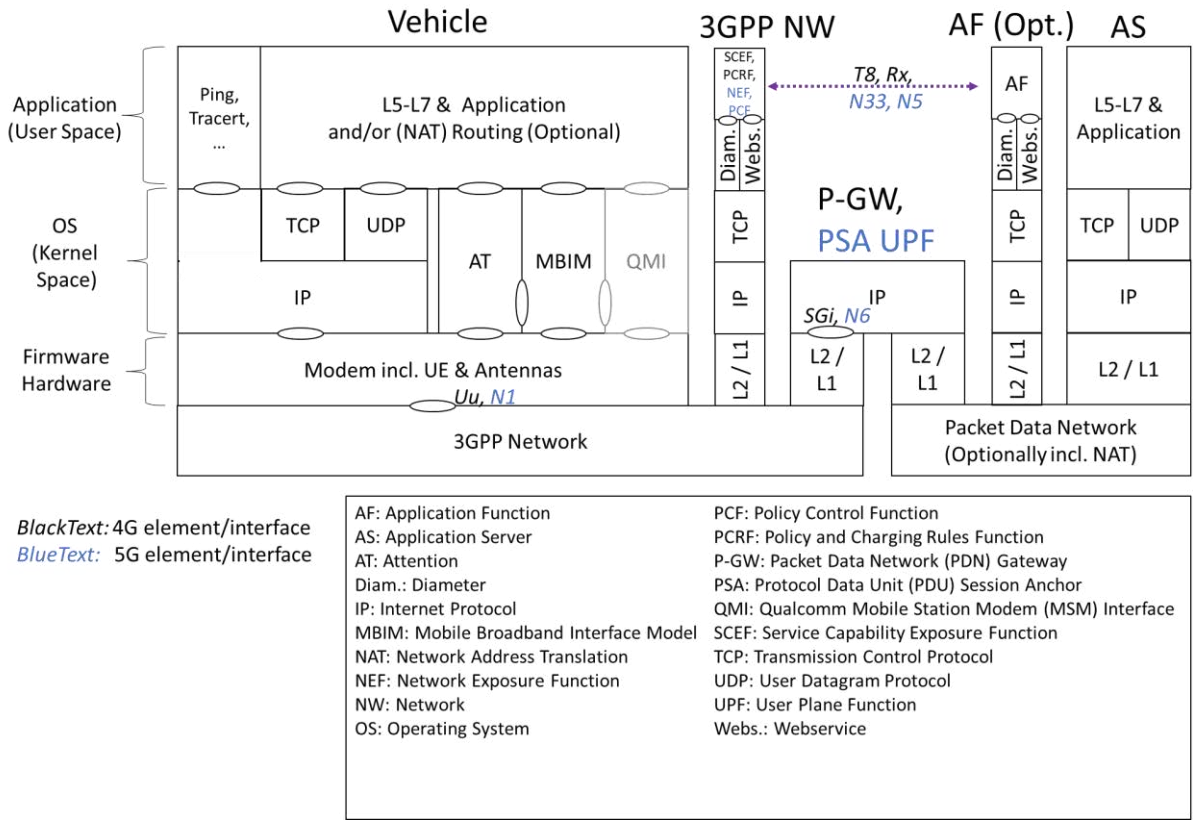

Figure 7-4: Protocol stacks at vehicle, AF, and AS

The 3GPP network is separated from the AS through[3] the SGi (4G Evolved Packet Core (EPC)) or N6 (5G Core) interface. SGi-interface terminates at the P-GW in 4G EPC and N6-interface at the Protocol Data Unit (PDU) Session Anchor (PSA) User Plane Function (UPF).

The NB interfaces consist of T8, Rx, N33, and N5. Rx (4G EPC) and N5 (5G Core) are used for QoS related interaction, e.g. requesting dedicated QoS bearers. The Rx-interface uses the Diameter (Diam.) protocol while all other NB interfaces use RESTful webservice Application Programming Interfaces (APIs). T8 (4G EPC) and N33 (5G Core) expose many different services. Most of these services are defined identically for 4G and 5G networks.

On the RAN side the Uu-interface[4] terminates at the UE in the vehicle. The UE is part of the modem consisting of hardware and firmware. The modem interacts with the operating system (OS). For the user plane, usually sending and receiving of messages is enabled through APIs provided by the OS for message transmission and reception over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). TCP APIs also allow to establish and release connections to a peer TCP layer in an AS.

Note: It is for further study if, how and when the TCP APIs informs the client application about transmission failures. It should be assumed that it takes several seconds for TCP to detect a connection failure, if detected at all. On the AS side, TCP and UDP OS APIs are the only ones present.

Direct communication over IP omitting TCP and UDP is also possible but usually only used for tools like ping and traceroute both triggering Internet Control Message Protocol (ICMP) communication.

7.2.2.1 Modem control and management interfaces

Two commonly present and one optional interface exist for control and management of 3GPP modems. They usually permit the triggering of NAS and RRC communication from the UE and pass received NAS events to the OS.

Note: It is for further study if RAN-initiated RRC messages are also propagated to the OS.

---

[3] The AF interfaces T8, Rx, N33, and N5 can be routed through the same router but this does not always have to be the case.

[4] In case of 5G Core, the N1-interface is explicitly defined for NAS communication while 4G EPC NAS does not have an extra name for the interface it uses and considers NAS to be also done over Uu-interface.

Attention (AT) commands are standardised in TS 27.007 [1]. A common way of invoking these commands is in a request-reply pattern, e.g. to request a packet data network connection and getting a confirmation when this succeeds. Besides that, unsolicited commands also exist where the modem indicates to the OS that certain events have occurred. The code +CGEV indicates a change in data connectivity. This includes changes initiated from the UE and the network. Besides TS 27.007, reference [2] provides an overview of +CGEV codes.

As well as AT commands, the Mobile Broadband Interface Model (MBIM) [3] was defined by the USB Implementers Forum to control and manage modems over USB. Microsoft Windows' system usually uses MBIM. Implementations for Linux also exist. MBIM_PACKET_SERVICE_INFO indications are used to inform the OS about changes in the network connection, analogous to +CGEV with AT commands.

Qualcomm chip-based modems usually also provide the Qualcomm Mobile Station Modem (MSM) Interface (QMI) to communicate with modems. Description of the interface is not public, so it was not further evaluated.

7.2.3 Conclusion

From the information provided in this chapter, it is quite likely that in future V2X systems there are parts, especially the communication between vehicles and backend via cellular radio, that cannot (fully) be controlled and influenced by the manufacturer of the function in the system (e.g. for the ToD function the vehicle OEM and/or the backend service developer/provider). However, when there are Functional Safety Requirements given for the function realised by the overall system, those black channels need to be taken into account. Principle concepts exist where those black channels are treated in the aforementioned class of systems by safely monitoring the end points on each side, but they need to be further enhanced and detailed. In addition to the pure safety assurance, there is a need to improve the availability of the service provided by the black channel to fulfil the requirements given for a certain product, including the above-mentioned function. This availability issue is seen as one of the major challenges to the telecom systems in the safe ITS context.

7.3 ASIL Qualifier Concept

V2X safety related use cases usually rely on two families of standards. In the US, the WAVE protocol family of IEEE 1609 is used by the SAE standards J2735 and J3161/1 (WIP). WAVE systems transmit and receive the SAE J2735-defined message set, including BSM, SPaT, MAP, etc. In Europe, a similar set of ETSI standards (e.g., ETSI EN 303 613, ETSI EN 302 637-2, ETSI EN 302 637-3) was developed and is used for C-ITS. Related activities are also observed in Asia, e.g. C-SAE in China. As basic concepts of those standards are very similar, while ETSI work is derived from IEEE, we chose to concentrate on the ETSI standard without limiting generality. In ETSI C-ITS, two messages intended to help prevent accidents between vehicles have been standardised.

The first to mention is the Cooperative Awareness Message (CAM) that is transmitted by all vehicles between one- and ten-times per second. The CAM contains data about position, speed, heading, etc., which enables receiving vehicles to predict if a collision with the transmitting vehicle is impending.

In addition, the Decentralised Environmental Notification Message (DENM) is transmitted in special situations, e.g. in the event of a strong braking manoeuvre. In this message, position, speed, heading, etc. are also sent together with the event information. Again, this message can be used by receiving vehicles to gain better understanding of the surrounding traffic situation and take countermeasures against potential threats, if necessary. There are further message types, such as Collective Perception Message (CPM) or Manoeuvre Control Messages (MCM), which carry similar basic information to CAM and DENM but they are extending or modifying the data transmitted to suit other types of functions.

The data is accompanied by confidence interval information. The standards define that the true values must be within the transmitted interval around the reported data in at least 95% of the cases. Unfortunately, it is not defined how exactly the statistical data is compiled (i.e. over which time interval). Therefore, it is unclear how large the error probability of the transmitted data is with respect to the Functional Safety Requirements, and what makes these data unusable in safety related driving functions. Here, more detailed discussions and potentially standardisation work are needed.

To guarantee the authenticity of the transmitted messages, each message is digitally signed with pseudonym certificates. On the one hand, frequent changes of pseudonym certificates assure the anonymity of the vehicle and driver. Thus, it is almost impossible to track vehicles. On the other hand, these certificates assure that only trustworthy systems can sign a message, as only these systems obtain certificates.

The following discusses the need for extension or modification of the existing standards and concepts in order to support functions that have requirements on the functional safety side.

7.3.1 Communication related safety requirements and measures

To limit the probability of false activation of a safety related, V2X-based driving function, such as an ASIL-rated Emergency Brake Warning (e.g. EBW or ToD), the V2X ECU needs to implement the safety measures derived according to ISO 26262's methodology and that apply to this class of ECUs (e.g. self-test at startup and partly during runtime, and usage of qualified hardware components). Additionally, during the development phase, an enhanced level of quality needs to be achieved by using tools, such as Failure Modes and Effects Analysis (FMEA), software assessments, etc. These measures are the basis for the function-specific measures. For driving functions relying on V2X communications, there are, among others, two main fault types that result in corresponding Functional Safety Requirements:

REQ#1: Data communication shall be protected against intentional or accidental corruption (e.g. 'FC3: (EBW) message corrupted during radio transmission or reception' (See Section 5.4), 'FC4: messages correctly generated by CC are corrupted during transmission to the CV' (See Section 4.6).

REQ#2: Transmitted data shall be correct and accurate (e.g. 'FC2: content of transmitted (EBW) message not accurate' (See Section 5.4), 'FC2 (ToD): CC generates faulty or inaccurate control messages' (See Section 4.6).

7.3.1.1 Protecting data communication against intentional or accidental corruption

The first safety requirement (REQ#1) is a typical objective for communication systems, such as internal vehicle communication busses. To detect and correct (if applicable) classical communication errors the usual features, such as timestamps, checksums (CRC), and message counters must be implemented. According to ISO 26262-6 (D.2.4 Exchange of information) [28] at least these communication errors need to be considered:

- Repetition of information
- Loss of information
- Delay of information
- Insertion of information
- Masquerade or incorrect addressing of information
- Incorrect sequence of information
- Corruption of information
- Asymmetric information sent from a sender to multiple receivers
- Information from a sender received by only a subset of the receivers
- Blocking access to a communication channel

Possible countermeasures are also assessed in the ISO 26262-5 [29]. The following table shows a first qualitative evaluation for the example 'communication bus'.

Safety mechanism/measure	**Typical diagnostic coverage**	**Notes**
One-bit hardware redundancy	Low	-
Multi-bit hardware redundancy	Medium	-
Read back of sent message	Medium	-
Complete hardware redundancy	High	Common mode failures can reduce diagnostic coverage
Inspection using test patterns	High	-
Transmission redundancy	Medium	Depends on type of redundancy Effective only against transient faults
Information redundancy	Medium	Depends on type of redundancy
Frame counter	Medium	
Timeout monitoring	Medium	
Combination of information redundancy, frame counter and timeout monitoring	High	For systems without hardware redundancy or test patterns, high coverage can be claimed for the combination of these safety mechanisms

Table 7-3-1-1: Qualitative evaluation of diagnostic coverage for 'communication bus' [29]

As shown in the table above, a high diagnostic coverage without hardware redundancy or a huge number of test patterns is only possible using the combination of 'information redundancy', 'frame counter' and 'timeout monitoring'. Information redundancy is usually achieved by adding a checksum (CRC). Other redundancies are possible as long as the error detection probability is on a comparable level. For automotive ethernet, an analysis shows that good 32-bit CRCs for data blocks of 4kB size and a 'hamming distance' of six fulfil the ISO26262 requirements up to ASIL D with respect to error detection capabilities. In the V2X communication case, there is a 256-bit-long signature inside the security header, which is 'collision free' – as far as we know today. In this context, 'collision free' means that there are no two different data packets that deliver the same signature. Given this, no additional CRC on the application level is necessary. Frame counters can be identified as the sequence number of the GeoNetworking header and timestamps inside CAM and DENM can be used for timeout monitoring. For the timeout monitoring, we should note that this is mainly necessary for checking the availability of the communication channel.

In conclusion, the four countermeasures (Counter, Timestamp, Station ID, Signature) are available on the application level to detect all previously mentioned errors as shown in the table below:

Fault	Countermeasures
Repetition of information	Counter
Loss of information	Counter
Delay of information	Timestamp
Insertion of information	Station ID, Signature
Masquerading or incorrect addressing	Station ID, Signature
Incorrect sequence of information	Counter
Corruption of information	Signature, application-level CRC
Asymmetric information sent from a sender to multiple receivers	Signature (to detect corruption at any of receivers)
Information from a sender received by only a subset of the receivers	Counter (loss on specific receivers)
Blocking access to a communication channel	Counter (loss or timeout)

Table 7-3-1-2: List of possible faults and corresponding countermeasures

The Station ID refers to a vehicle-internal ID and is either derived from the certificate or a random Station ID is generated at every certificate change. Thus, the Station ID changes when the certificate changes.

As the automotive industry focuses more and more on security issues, measures against security attacks also need to be implemented. In the V2X communications case, the prevention of information manipulation (ensuring authenticity) and the authentication of the sender are the most important tasks. Information confidentiality is not an issue because it is a basic feature of the system that the vehicle informs everybody in the vicinity of its route and status. According to the security threat analysis of the SeVeCom PPP project [30], the relevant attacks and countermeasures are summarised in the following table:

Security attack	Countermeasures
Message manipulation	Cryptographic, asymmetric signature based on ECC
Message forging	Certification of public keys and certain sender/application attributes by a trusted PKI
Message replay	Timestamps and/or sequence numbers plus Geostamps
Message falsification	Data plausibility checking in order to detect manipulated messages
Privacy infringement	Changing, pseudonymous identifiers
Denial-of-service	Load control, protocol monitoring

Table 7-3-1-3: List of possible security attacks and corresponding countermeasures

These detection and security features are already part of the ETSI C-ITS standards, so that V2X can be seen as secure and safe in this regard.

7.3.1.2 Ensuring data correctness and accuracy

The second safety requirement (REQ#2) is usually addressed in a vehicle by assigning the transmitting ECU a related safety goal and checking that this ECU fulfils its requirements. In managing the safety of the vehicle that receives the V2X communications, the transmitting ECU is external and thus outside the vehicle system borders (and its development process). Further, there are no requirements in the V2X standards or the laws stipulating that V2X signals must fulfil safety requirements. Thus, the V2X receiver has to assume that the probability of receiving incorrect data via a V2X message is higher than what would be determined as necessary according to an ISO 26262-based analysis. As a result, today's V2X systems cannot implement a safety critical function (e.g. triggering potentially dangerous actions).

In essence, the fundamental objective is to enable a V2X receiver to assess, if the transmitted data can be used for safety-related vehicle functions.

To address this issue, several potential solutions can be envisioned:

a) **'Special' security certificates** are only granted, if an ECU not only fulfils the usual security requirements but in addition guarantees that the correctness and accuracy of transmitted data meets ASIL B requirements. In this case, the format of the transmitted messages is not changed, only the meaning of the confidence interval signals is adapted to ASIL B requirements. Additionally, the definitions of the transmission schedule may be adapted, considering applicable congestion control mechanisms.

Pros	Cons
No changes in the existing standards necessary, only enhancement of the evaluation for the certificate awarding is necessary	QM applications also need to wait until all data is available, e.g. in ASIL B quality, because messages signed with the "safety & security" certificate can only be transmitted, if all data are available in the requested quality
	Only one level of functional safety is supported (ASIL A/B/C/D)
	Using sets of different certificates for usage in different situations (e.g. QM, ASIL A, etc.) enlarges the complexity of the certificate handling and does not fit to the ideas of the V2X communication standards (e.g. frequent certificate changes may be necessary, also while an event cause is lasting)

Table 7-3-1-2-1: Pros and cons of 'special' security certificates

b) V2X message definitions are extended, so that every data field relevant to ASIL-rated functions is provided with a corresponding '**ASIL qualifier**', which indicates whether the provided data is 'qualified' to be used by safety critical functions of a certain ASIL. Hence, there could be multiple ASIL qualifiers per V2X message.

Pros	Cons
Flexible and extensible solution for all possible functions (from QM up to ASIL D)	V2X message definitions need to be adapted
Easy support for dynamically changing data quality (e.g. positioning accuracy depends on GNSS reception quality)	
Possibility to add a 'safety CRC' to the message so that the security signature needs no longer to be used for safety checks, which helps in separating the design of security and safety related functions, respectively	

Table 7-3-1-2-2: Pros and cons of 'ASIL qualifiers'

These additional qualifiers can be collected in respective additional ASN.1 containers, so that the extended messages remain compatible with existing message definitions. In essence, the proposed 'ASIL qualifier' concept supports the fulfilment of safety requirements of connected and automated driving functions, particularly regarding V2X data quality and usability. In some cases, the same safety level that matches a conventional, non-connected design, e.g. solely based on in-vehicle sensors, may be achieved.

7.3.2 Considerations for future automated driving functions

For future automated driving functions (e.g. Tele-operated Driving) that may rely on V2X communications, not triggering an appropriate action is also a safety risk, e.g. if a vehicle does not correctly recognise a situation and does not brake or change lane.

Moreover, even if the necessary data is available in the transmitting vehicle and systematic and security issues are handled by the system design, the problem that the transmission may be blocked by other vehicles (e.g. trucks) or buildings or even an interfering transmitter still exists. A blocked or interfered transmission then may result in not appropriately recognising a dangerous situation.

This danger can be addressed by several means, including by introducing redundancy into the situation detection. A possibility for this is the usage of a second communication channel that is not sensitive to the same interference sources (or blockage), but delivers 'redundant information' (e.g. a communication channel operating at different frequencies). Thus, the receiving vehicle is able to perform the same 'situation detection' or at least it is enabled to detect that the C-ITS system does not 'see' all transmissions. A system that knows that it is missing important input can handle this situation, e.g. by handing over the control to a 'sensor-only' mode or even handing over the vehicle control to the driver.

Another redundancy method may be to build up a function that not only relies on a single sensor, e.g. V2X, but uses several different sensors so the failure of a single sensor only degrades the function, delivering less performance or convenience, but does not result in a complete function deactivation. In such sensor fusion-based designs, the guidelines of the ISO 26262 need to be considered to assign the right requirements to the respective system components.

7.4 Solutions based on 5GAA activities

Some of the approaches mentioned as potential solutions to the safety requirements listed in the Chapters 4.6 and 5.4 are already considered in activities in 5GAAworkgroups or working items or other activities outside of 5GAA. The following provides a list of the identified requirements and the related 5GAA results available or in progress. The details of the results are not listed here, instead some hints about how the referred work can help to solve the identified requirement is given in the comment column of the following table.

Safety Requirement	**Working activity**	**Comment**
PFSR-FC2-1 **PFSR-FC2-2** **PFSR-FC2-3**	5GAA WG7 Misbehaviour Detection ETSI ITS WG5	In the mentioned activities, there are aspects considered and analysed that might help to detect misbehaviour and thus might help to identify useless or dangerous data packets and separate it from the useful ones. The concepts mentioned will be one possible component but others like plausibility checks by comparing with other sensor information or based on unrealistic information need to be added. The concepts are not limited to functions that use the network and also apply to V2V functions but need some network components to keep track. Those components are part of the PKI and therefore can be assumed as being existent in V2X systems The tools proposed in the cited work can help to identify reasonable technical concepts with respect to PFSR-FC2-3
PFSR-FC3-1 **PFSR-FC3-2**	5GAA WG2 XWIs NESQO, eNESQO and PRESA	The work carried out in the cited 5GAA activities is proposing the means to improve monitoring and prediction of QoS in the communication networks used. This is not directly helping functional safety, as the proposed functions are likely not being developed according to ASIL rules, however it can help to improve the overall quality of the

		function by boosting the availability of the function. For example, information from the QoS prediction can help the function to adapt its ODD or better prepare for a potential communication loss. In ToD for example, the allowed speed could be adapted to the predicted QoS or an outage prediction could be used to prepare for a 'safe stop' in advance and thus the stop could be carried out in a more reasonable way
PFSR-FC3-3 **PFSR-FC3-4** **PFSR-FC3-5** **PFSR-FC3-6**	5GAA WG2 3GPP QoS Framework	Detection of QoS degradation is part of the existing QoS framework in the cellular communication frameworks defined by 3GPP Future work in 5GAA WG2 could identify potential gaps in the existing QoS frameworks especially with respect to the functional safety requirements and suggest dedicated extensions
PFSR-FC8-1 **PFSR-FC8-2** **PFSR-FC8-3** **PFSR-FC8-4** **PFSR-FC8-5** **PFSR-FC8-6** **PFSR-FC13-1** **PFSR-FC13-2** **PFSR-FC13-3** **PFSR-FC13-4** **PFSR-FC13-5** **PFSR-FC13-6**	5GAA WG2 XWIs NESQO, eNESQO and PRESA	The means for keeping a certain needed QoS are part of the works carried out in the mentioned activities Future work in 5GAA WG2 could identify potential gaps in the existing QoS frameworks especially with respect to the functional safety requirements, and suggest dedicated extensions

8 Standards Impacts

The standards impacts discussed in this section apply to both the ToD and EBW use cases. Hence for the purpose of this discussion we use again the terms Tx_EP and Rx_EP, which were first defined in Section 6.1.1.

In any one real-world instantiation of an item/system comprising a V2X connected Tx_EP and Rx_EP, the manufacturer of the Tx_EP may be different to the manufacturer of the Rx_EP. This means that no single manufacturer has safety engineering oversight of the complete system. This is one of the key reasons why standardisation has the potential to play an important role in safety treatment of V2X.

Where there are a variety of different possible functional safety concepts for avoiding or mitigating hazards, and where those different concepts allocate the functional safety requirements to Tx_EP and Rx_EP in different ways, then the question arises as to how the selection amongst the different possible functional safety concepts should be made. This is because if the manufacturer of Tx_EP and the manufacturer of Rx_EP design their systems assuming different functional safety concepts then clearly there can be implications.

Another related question which arises, is how, for a given use case, it can be ensured that the designers of Tx_EP and Rx_EP either:

- Design their systems to the same ASIL level

or

- Manage the possibility that Rx_EP and Tx_EP are designed to different ASIL levels

Conclusion: Based on the experience of undertaking the analysis included in this TR, it does <u>not</u> seem reasonable to expect that safety engineers from different manufacturers, if working independently, will necessarily come to the same conclusions about exactly what ASIL level is required for a particular use case.

There are the following possible options for handling the above-mentioned concerns:

Possible standardisation option #1: An industry level agreement or standard is provided such that, for each use case, it is specified what functional safety requirements and/or what (e.g. ASIL) need to be supported in Tx_EP. Noting that with this option, the Rx_EP would also need to acquire assurance that Tx_EP is standards-compliant during V2X operation.

- A major element of the standardisation work would be to obtain industry agreement on the ASIL level to be used for each use case
- A secondary standardisation task would be to consider how Rx_EP obtains assurance that Tx_EP has been designed in a standards-compliant way; this may for example be achieved by a signing operation that is backed by a certification authority
- For this option, it remains to be determined:
    - What would be the most appropriate industry association or standardisation committee to undertake this work
    - Whether it may be simplest to agree a) what should be assumed, or b) what should not be assumed when determining functional safety requirements for the Tx_EP
    - Whether it might be sufficient just to agree the ASIL level that is to be used in the Tx_EP for a particular use case
- Pros:
    - Avoids design and implementation difficulties for the Rx_EP associated with having to handle different ASIL levels in Tx_EP and Rx_EP
    - Each instantiation of a Tx_EP and an Rx_EP will obtain the full possible benefits of the use case; this is in contrast to the situation where the ASIL level in Tx_EP is less than that assumed to be required by Rx_EP, which may result in some fall back in the behaviour of Rx_EP operation with associated reduction in the efficacy of the use case
- Cons:
    - Determining ASIL for V2V EBW (see Appendix F) was non-trivial, hence obtaining industry agreement on an ASIL level for every use case seems likely to prove difficult and time-consuming; indeed, it may even be challenging to identify an exhaustive set of possible use cases
    - Another issue is that the required ASIL level in the Tx_EP will depend on what capability is placed in Rx_EP; e.g. in the study of the EBW use case it was found that if the EBW message was used to generate a warning to a human driver then ASIL B was required, while if the EBW message could be acted on by a robot (autonomous braking function) then ASIL C is required; different manufacturers may have different preferences in terms of what capability they would place in the Rx_EP, and therefore different preferences on what ASIL level is required in Tx_EP, and hence this would be another aspect on which agreement would have to be reached

Possible standardisation option #1.1: Information disclosure based approach (variant of #1 above):

- Manufacturers could disclose, e.g. by populating a shared database, the ASIL levels that they have assumed in their Tx_EP design for each use case, or for some subset of representative use cases
- This might be a relatively 'light touch' approach, which could have the effect of causing some consensus building to take place over time as OEMs debate with one another the reasons for any differences that may exist; such debates might occur individually between OEMs, or if 'the industry' deems it preferable, such debates could move to a standardisation body or industry association

Possible standardisation option #2: The Tx_EP provides the Rx_EP with sufficient information to enable Rx_EP to determine either the ASIL level that is provided by the Tx_EP and/or the functional safety engineering requirements implemented in Tx_EP.

- One possible standardisation task would then be to specify a method by which the Tx_EP includes an indication of ASIL in the transmitted message, in such a way that the Rx_EP can rely on it (e.g. the ASIL level could be signed, with certification authority backing)

- It remains to be determined whether it would be preferable to leverage the existing Security Credential Management System (SCMS) certificate such that it would additionally provide this safety engineering assurance, or whether a new 'safety certificate' would be preferable
- Pros:
    - Designers of Tx_EP and Rx_EP have autonomy in the safety engineering approaches that they choose to adopt; there is no need to obtain industry agreement on safety engineering approach and/or ASIL for each use case (which could prove difficult and/or time consuming to achieve)
- Cons:
    - Risk that the manufacturer of Tx_EP and the manufacturer of Rx_EP make different choices/assumptions regards required ASIL level and/or the split of requirements across Tx_EP and Rx_EP (e.g. vendors of Tx_EP assume vendors of Rx_EP will implement mitigations, and vice-versa); consequence could be that the Rx_EP is forced to some fallback mode of operation in which the full benefits of the use case would not be realised

Possible standardisation option #3: a hybrid of Options #1, #1.1 and/or #2. In this approach Tx_EPs are required to adopt standardisation option #2, e.g. by including some explicit indication of Tx_EP ASIL level in the transmitted message. But in addition, the industry also attempts to reach some consensus on ASIL level requirements for a (possibly small and representative) set of use cases as suggested in Option #1 or #1.1. so as to encourage convergence in the assumptions made by the safety engineers in different manufacturers.

It can also be observed that any requirement for industry agreement on ASIL level or on the distribution of functional safety requirements need only be concerned with agreeing what is to be done in Tx_EP (not Rx_EP). This would provide Rx_EP designers with the information and certainty that they require regards what they can expect from the Tx_EP, while also giving those same Rx_EP designers flexibility with their choice of Rx_EP design, e.g. regarding topics such as how and whether to use corroboration.

Conclusion: The need for any standardisation and agreement regards distribution of functional safety requirements and/or in ASIL level-setting should be focused on what shall be done in the Tx_EP.

It was also observed that in some V2X messages the data is accompanied by confidence-interval information. The standards define that the true values must be within the provided range (as included in the transmitted message) around the reported data in at least 95% of the cases. Unfortunately, it is not defined how exactly the statistical data is compiled (i.e. over which time interval). Therefore, it is unclear how large the error probability of the transmitted data is with respect to the requirements of functional safety, which makes this data unusable in safety related (non-QM) driving functions. More detailed discussions and potentially standardisation work are needed.

Conclusion: Further clarification is needed in standards regards the statistical definition of confidence interval.

9 Conclusions

The objective of the STiCAD work has primarily been to identify what standardisation needs may exist related to provision of safety treatment in V2X systems. Two representative use cases were selected to gain insight into this question:

- V2N Tele-Operated Driving
- V2V Emergency Brake Warning (EBW)

The pre-eminent existing automotive safety engineering standard, ISO 26262, is written from the perspective that the largest item (system to be safety engineered) is a single vehicle. Therefore, it can be seen that the safety engineering of V2X systems moves the automotive industry into a new safety engineering paradigm.

Conclusion: ISO 26262 needs to be updated if it is to be used to tackle the safety engineering of cars that are connected using V2X communications.

Despite the above observation, throughout this study we have used the basic framework provided by ISO 26262, and it was found to be fit for our purposes. The reader should be cautioned that throughout this document we have used ISO 26262 terms like 'ASIL' when describing and discussing systems comprising components in multiple vehicles, despite the fact that such trans-vehicle systems are currently outside the scope of ISO 26262.

The study has shown that it is critical that safety be managed rigorously in at least some V2X use cases.

9.1 V2X ToD Perspectives

Conclusion: The detailed analysis of the ToD use case has shown that for the 'direct control' use case, the system needs to be designed generally according to ASIL D level. The 'indirect control' use case might need lower ASIL levels, however this depends on the capability of the vehicle to perform 'plausibility checks' of the given indirect control commands with independent ego-sensors in the vehicle.

It follows that:

Conclusion: The messages exchanged between the vehicle control centre and the vehicle need special consideration with respect to functional safety.

Conclusion: The communication networks between vehicle and vehicle control centre are currently not developed according to ASIL or other similar safety consideration schemes due to technical and commercial reasons.

It follows that:

Conclusion: In order to, under the above circumstances, still be able to provide functions like ToD, the black-channel approach together with safe monitoring on both sides of the communication is a possible reasonable approach to fulfil given requirements.

Conclusion: In order to fulfil the high availability requirements of a function such as ToD, the network side of the system, even though not being ASIL capable, needs to factor in small outage ratios and high compliance to the given QoS requirements.

Conclusion: If V2N functions such as ToD need to be flexible with respect to the mutual independence of suppliers and providers on the vehicle, network and backend side, there is a great need for standardisation on different levels particularly for:

- **Technical interfaces (message frequency, security, format, protocols, …)**
- **Commonly agreed safety considerations and concepts (monitoring, general SIL levels)**
- **Mutual trust**
- **Commonly agreed homologation concepts**
- **Commonly agreed mutual certification**
- **Legal concepts**

9.2 V2V EBW Perspectives

Conclusion: for the V2V EBW use case, detailed analysis showed that where a human acts on an EBW warning message the system must be designed to at least ASIL B, while for the hybrid case, where a robot acts on the message if a human fails to do so in a timely manner, the system must be designed to at least ASIL C.

It follows that:

Conclusion: V2X messages that provide warnings to human drivers can, for at least some use cases, require safety engineering treatment (i.e. ASIL level is greater than QM).

Conclusion: Different use cases have different ASIL level requirements.

From the above conclusion, it follows that:

Conclusion: Components of a system in either TxV or RxV that are common across multiple V2X use cases will have to be designed to the ASIL level of the implemented use case that requires the highest ASIL level.

It can be envisaged that different OEMs may implement different subsets of the superset of all possible V2X use cases.

During the study, the question arose as to which entities bear the responsibility for determining whether a V2X message is sufficiently reliable, such that action can be taken based on the contents of the V2X message. This is dealt with in the following statement.

Conclusion: In the case of a unidirectional V2X communication from a TxV to an RxV (such as with EBW), the RxV needs to make the assessment of whether the received message can be relied upon and then act accordingly. Hence the RxV must be provided with the capability, as well as any necessary information, in order to assess the reliability of the received message and its contents.

For the V2V EBW use case multiple possible functional safety concepts were identified and explored.

Conclusion: For a given V2V use case, multiple possible functional safety concepts may exist, and may differ according to the split of Functional Safety Requirements across TxV and RxV.

The different potential functional safety concepts identified for EBW can each have a different implication for the potential value-add provided by V2X. For example, one possible concept might rely on the existence of two or more independent and redundant systems. In this situation, a braking actuation might only occur if a V2X EBW message is corroborated with evidence from another independent system e.g. Radar/Lidar. Such an approach could enable an ASIL decomposition to be used, which would reduce the ASIL requirements for each individual system, and this might thereby reduce cost. However, at the same time, in this example, one of the key benefits and value propositions of V2X is lost if such an approach is taken. Specifically, one of the key advantages of V2X compared with Radar/Lidar is V2X's ability to provide advanced warning of events that are out of the line of sight. However, if V2X messages are not acted upon until there is line-of-sight corroboration from, for example, Radar or Lidar then this benefit of V2X is either not enjoyed or is not enjoyed as fully as it might have been. In contrast, an alternative functional safety concept which enables RxV to act solely on the basis of a V2X message, and without requiring corroboration from another independent system, may require that both TxV and RxV be designed to a higher ASIL level, possibly at increased cost, but with the benefit that the non-line-of-sight operation can be fully exploited.

Conclusion: Choice of functional safety concept can impact the ability (or not) to <u>fully</u> exploit some of the V2X ecosystem's unique differentiators, such as V2X's advantage of non-line-of-sight operation. Full exploitation of a unique differentiator, such as non-line-of-sight operation can in turn enable some accidents to be avoided which would otherwise not have been avoided.

For the EBW use case, two safety goals were identified:

- SG1: Avoid or mitigate unintended braking if there are following vehicles
- SG2: Avoid or mitigate the situation where a car does not brake when it should brake

Considering these safety goals from the perspective of the Functional Safety Requirements implied for the TxV, it can be seen, firstly, that TxV should only generate EBW messages when there is a true emergency braking event and, secondly, that safety critical information contained within the message should always be sufficiently accurate.

Conclusion: For the EBW use case, safety engineering of the TxV is principally concerned with correct and timely generation of V2X messages, as well as ensuring sufficiently accurate value-setting of any safety critical information elements that are contained within those V2X messages.

10 Possible Future Work

There are a number of pieces of work that could be undertaken if the project is to be continued in a follow-on phase:

- A further level of detail could be provided for each of the conclusions identified above, particularly where some aspects have been marked as 'to be determined' (tbd)
- Besides non-line-of-sight operation, another key differentiator of V2X is its ability to signal intention to manoeuvre. With a use case like four-way stop (and in contrast to EBW), each vehicle may be both TxV and RxV during any messaging dialogue that may occur during the operation of the use case. It would therefore be interesting to assess whether there might be any new safety treatment standardisation requirements that arise for such use cases
- The work could also be enhanced to consider how and whether any new standardisation requirements emerge as higher levels of autonomy are considered. as evidenced in the EBW sub-cases requiring ASIL levels which may increase (SAE) autonomy levels
- Further aspects that should be considered from a standardisation perspective are:
    - System testing, validation and verification:

ISO 26262 defines processes for system-integration testing, verification and validation as it relates to safety. In a system comprising modules from different vendors, there may be multiple different combinations of TxVs and RxVs leading to multiple different individually unique systems. Questions arise as to how and whether testing of each possible combination should be performed.

- Certification:

  In order to provide increased confidence that safety engineering is adequate, an auditor that is independent of the vendor of a system may provide an assessment/audit which results in a certification that the system has met the required safety integrity level.

  Hence there is the question whether it is necessary to provide such third-party assessment of a system comprising a V2X connected TxV and RxV, where TxV and RxV may be from different vendors. And if necessary, then how best to achieve it, and how and by whom/what would such a certification be consumed?

  Another question is whether it is only necessary for the safety of the V2X functionality in a given TxV design to be certified (and with such proof of certification communicated to the RxV).

- Liability:

  According to today's view, the liability is with the OEM that implements the part of the function where the actuation is triggered and thus the hazard is finally caused when system failure is happening. However, in future functions like EBW or ToD, there might be new views on the liability issue. For example, when a tele-operator is controlling a vehicle that has limited sensor availability (e.g. due to sensor damage), the liability might be with the tele-operator for the actions and commands generated while it stays with the OEM for monitoring the communication and verification of the commands. Those aspects should be further investigated in order to prepare those type of functions for the future.

11 Appendix A – ETSI's Emergency Electronic Brake Light Use case

[FR_UC005_001]	Unique use case identifier shall be defined for this use case.
[FR_UC005_002]	Unique event identifier shall be assigned to the "emergency electronic brake lights" event.
[FR_UC005_003_VS]	The vehicle ITS station shall have access to the in vehicle system to detect the 'emergency electronic brake lights' event. This shall be at least the emergency brake light and the vehicle brake status.
[FR_UC005_004_VS]	The vehicle ITS stations shall be able to verify whether the 'emergency electronic brake lights' event may be a risk to other vehicles.
[FR_UC005_005_VS]	If an ITS station detects an 'emergency electronic brake lights' event, the corresponding RHW application shall be triggered.
[FR_UC005_006_VS]	The corresponding RHW application shall request to construct and transmit an 'emergency electronic brake lights' DENM.

[FR_UC005_007_VS]	The originating ITS station shall transmit the ‘emergency electronic brake lights’ DENM at a defined transmission rate during a valid time.
[FR_UC005_008_VS]	If the originating ITS station detects the event termination of the ‘emergency electronic brake lights’ event, it shall send out a cancellation DENM. This new DENM shall reference to the previous DENM.
[FR_UC005_009_VS]	The originating vehicle ITS station shall add an estimated valid time to the ‘emergency electronic brake lights’ DENM.
[FR_UC005_010_VS]	The RHW application of the originating ITS station shall determine the transmission latency of the ‘emergency electronic brake lights’ DENM.
[FR_UC005_011]	The RHW application at the originating vehicle station shall determine the transmission area of the ‘emergency electronic brake lights’ DENM.
[FR_UC005_012]	The ‘emergency electronic brake lights’ DENM shall provide the emergency brake vehicle current position as the event position with a location referencing sufficient for matching to a certain road section. The location reference shall include at least coordinates in the WGS84 coordinate system and heading information of the vehicle.
[FR_UC005_013_VS]	Information included in the DENM shall allow a receiving vehicle ITS station to check the relevance of the ‘emergency electronic brake lights’ event and estimate the collision risk level.
[FR_UC005_014_VS]	The RHW application shall decide whether an ‘emergency electronic brake lights’ warning information should be provided to user via HMI.
[FR_UC005_015_VS]	The ‘emergency electronic brake lights’ warning information should be provided with an appropriate timing.
[FR_UC005_016]	Additional to the information distributed via DENM, the RWH application may use information of the CAM containing information about the vehicle brake status, vehicle speed, and the vehicle position.

Figure A.1: Application functional requirements emergency electronic brake lights [2]

12 Appendix B – Selected non-functional requirements provided in [4]

User Story	**Detailed description and specifics**
User Story #1	HV is moving at very high speed different from RV in a highly congested traffic scenario illustrated above. HV is driven by human driver. RV applies breaks in order to make an emergency stop. HV is at distance D behind the RV and the HV driver does not see RV applying breaks or is distracted. Wet road conditions assumed.
User Story #2	HV is at least Level 2. HV is moving at very high speed different from RV in a highly congested traffic scenario illustrated above. HV is driven by human driver or robot. RV applies breaks in order to make an emergency stop. Wet road conditions assumed.
.....	

User Story #1			
SLR Title	**SLR Unit**	**SLR Value**	**Explanations/Reasoning/Background**
Range	**[m]**	360	Under the assumptions of Vrv=25m/s, Vhv=50 m/s and a=0.4g this is the minimum distance (400ms margin or 200m) at which HV needs to be warned to avoid collision.
Information requested/ generated	**Quality of information/ Information needs**	BSM or CAM (between 200-400 bytes)	The message should be delivered to HV. It contains the information about the hard breaking event at RV. It contains other information regarding RV such as location, velocity, acceleration, etc.
Service Level Latency	**[ms]**	120ms	Ideally, the information about the Hard Breaking event should be conveyed as soon as possible. Examining current radar and camera vision sensors the detection times are 100-300ms which makes V2X latency within the same budget. Additionally, for the reliability that we are requesting this latency seems reasonable. For example, the latency of 100ms causes the HV to travel additional 5m before final stop at 50m/s initial velocity, however, this additional distance is budgeted in the range estimate.

			This includes handling, access, and OTA latency.
Service Level Reliability		99.99%	The Hard Breaking event message needs to be delivered to the HV with high reliability.
Velocity	**[m/s]**	50	
Vehicle Density	**[vehicle/km^2]**	10,000	Assume maximum density.
Positioning Accuracy	**[m]**	1.5 (3σ)	HV needs to know whether the hard breaking vehicle in the front is in the same lane.
Interoperability/ Regulatory/ Standardisation Required	**[yes/no]**	Yes	Interoperability needs to be in place for HV to receive a message from RV.

User Story #2			
SLR Title	**SLR Unit**	**SLR Value**	**Explanations/Reasoning/Background**
Range	**[m]**	290	Under the assumptions of Vrv=25 m/s, Vhv=50m/s, 0.5 second reaction time and a=0.4g (and 300ms margin or 15m) this is the minimum distance at which the Level 3 system needs to be warned to avoid collision.
Information requested/ generated	**Quality of information/ Information needs**	BSM or CAM (between 200-400 bytes)	The message should be delivered to HV. It contains the information about the hard breaking event at RV. It contains other information regarding RV such as location, velocity, acceleration, etc.
Service Level Latency	**[ms]**	120ms	Reasonable latency in the context of the other existing sensor systems as well as taking into account the high reliability needed.
Service Level Reliability		99.99%	The Hard Breaking event message needs to be delivered to the HV with high reliability.
Velocity	**[m/s]**	50	

Vehicle Density	**[vehicle/km^2]**	10000	Assume maximum density.
Positioning Accuracy	**[m]**	1.5 (3□)	HV needs to know whether the hard breaking vehicle in the front is in the same lane.
Interoperability / Regulatory / Standardization Required	**[yes/no]**	Yes	Interoperability needs to be in place for HV to receive a message from RV.

13 Appendix C – ETSI system architecture

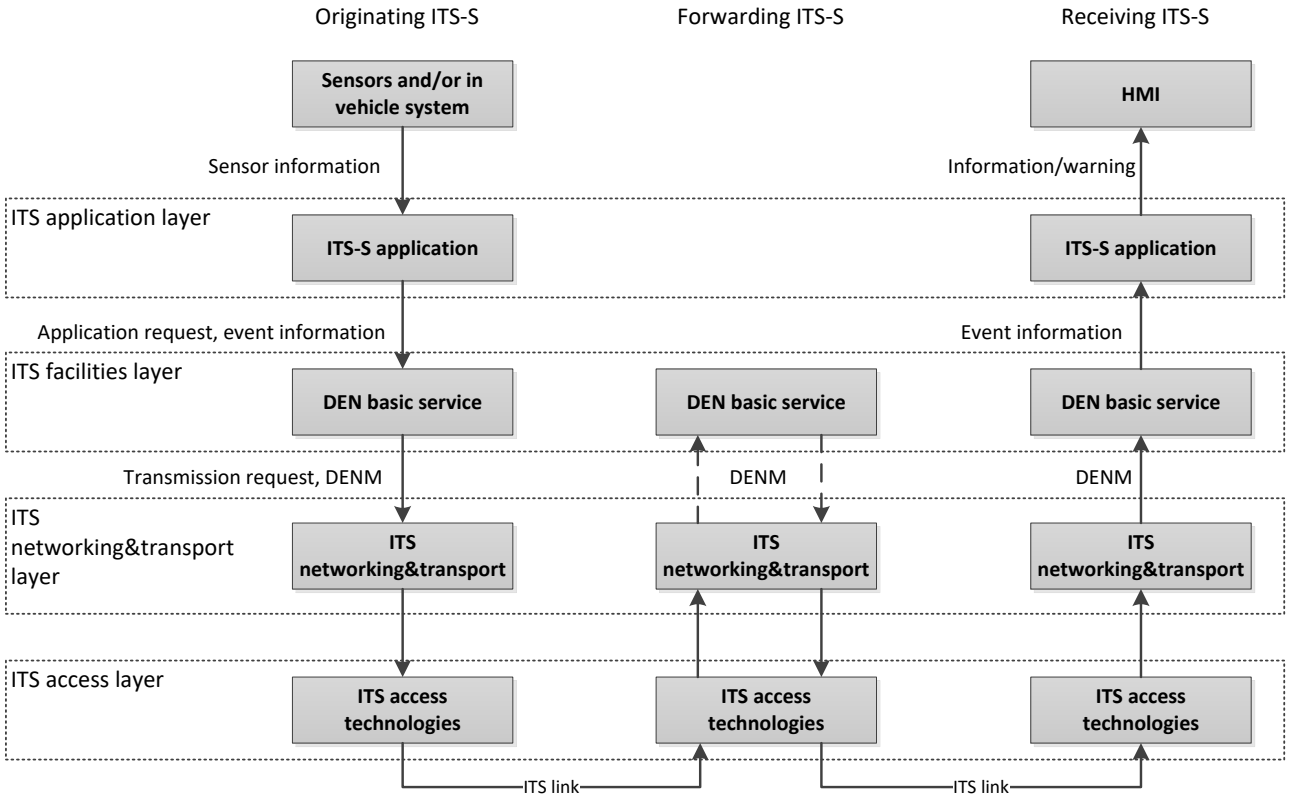

Figure C.1: General data flow for ITS-S application supported by the DEN basic service [5]

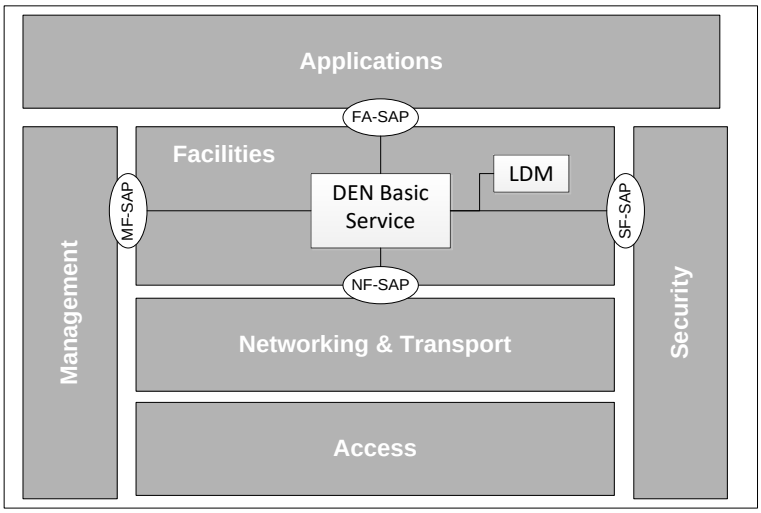

Figure C.2: DEN basic service and logical interfaces [5]

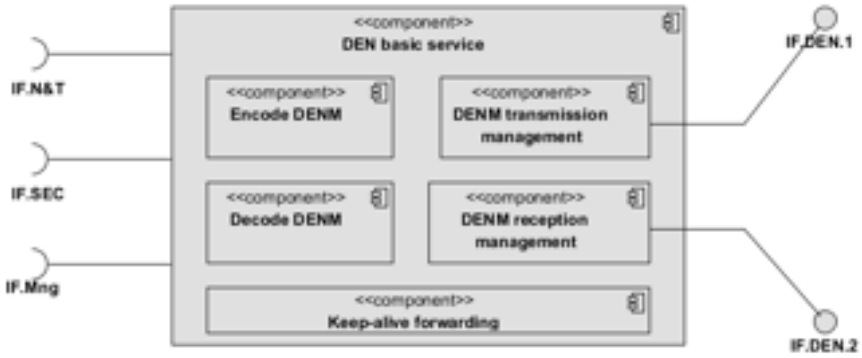

Figure C.3: DEN basic service component diagram [5]

14 Appendix D – EBW warning message contents

The following figure shows the ASN.1 description of the ETSI DENM message, taken from [2], where Data Elements that may (FFS) have major impact in determining the relevant systems involved in support of ETSI's Emergency Electronic Brake Light event, are highlighted in red (where such data elements are known to be included in the EBW message according to [11]) and are marked in brown, where they appear to be of potential relevance to the EBW use case but it has not yet been confirmed whether or not they may be included in an EBW message.

```
DENM-PDU-Descriptions {itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wg1 (1) en
(302637) denm (1) version (2)
}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS
ItsPduHeader, CauseCode, Speed, InformationQuality, ReferencePosition, ClosedLanes,
DangerousGoodsExtended, Heading, LanePosition, LightBarSirenInUse, RoadType, HeightLonCarr,
PosLonCarr, PosCentMass, PositioningSolutionType, RequestResponseIndication, StationType,
SpeedLimit, StationarySince, TimestampIts, WheelBaseVehicle, TurningRadius, PosFrontAx,
PositionOfOccupants, Temperature, VehicleMass, VehicleIdentification, EnergyStorageType, ActionID,
ItineraryPath, NumberOfOccupants, PositionOfPillars, RelevanceTrafficDirection, RestrictedTypes,
Traces, TransmissionInterval, ValidityDuration, RelevanceDistance, EventHistory, TrafficRule,
DeltaReferencePosition FROM ITS-Container {
itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wg1 (1) ts (102894) cdd (2) version (2)
};
```

```
DENM ::= SEQUENCE {
    header ItsPduHeader,
    denm DecentralizedEnvironmentalNotificationMessage
}

DecentralizedEnvironmentalNotificationMessage ::= SEQUENCE {
    management ManagementContainer,
    situation SituationContainer OPTIONAL,
    location LocationContainer OPTIONAL,
    alacarte AlacarteContainer OPTIONAL
}

ManagementContainer ::= SEQUENCE {
    actionID ActionID,
    detectionTime TimestampIts,
    referenceTime TimestampIts,
    termination Termination OPTIONAL,
    eventPosition ReferencePosition,
    relevanceDistance RelevanceDistance OPTIONAL,
    relevanceTrafficDirection RelevanceTrafficDirection OPTIONAL,
    validityDuration ValidityDuration DEFAULT defaultValidity,
    transmissionInterval TransmissionInterval OPTIONAL,
    stationType StationType,
    ...
}

SituationContainer ::= SEQUENCE {
    informationQuality InformationQuality,
    eventType CauseCode,
    linkedCause CauseCode OPTIONAL,
    eventHistory EventHistory OPTIONAL,
    ...
}

LocationContainer ::= SEQUENCE {
    eventSpeed Speed OPTIONAL,
    eventPositionHeading Heading OPTIONAL,
    traces Traces,
    roadType RoadType OPTIONAL,
    ...
}

ImpactReductionContainer ::= SEQUENCE {
    heightLonCarrLeft HeightLonCarr,
    heightLonCarrRight HeightLonCarr,
    posLonCarrLeft PosLonCarr,
    posLonCarrRight PosLonCarr,
    positionOfPillars PositionOfPillars,
    posCentMass PosCentMass,
    wheelBaseVehicle WheelBaseVehicle,
    turningRadius TurningRadius,
    posFrontAx PosFrontAx,
    positionOfOccupants PositionOfOccupants,
    vehicleMass VehicleMass,
    requestResponseIndication RequestResponseIndication
}

RoadWorksContainerExtended ::= SEQUENCE {
    lightBarSirenInUse LightBarSirenInUse OPTIONAL,
    closedLanes ClosedLanes OPTIONAL,
    restriction RestrictedTypes OPTIONAL,
    speedLimit SpeedLimit OPTIONAL,
    incidentIndication CauseCode OPTIONAL,
    recommendedPath ItineraryPath OPTIONAL,
    startingPointSpeedLimit DeltaReferencePosition OPTIONAL,
    trafficFlowRule TrafficRule OPTIONAL,
    referenceDenms ReferenceDenms OPTIONAL
 }

StationaryVehicleContainer ::= SEQUENCE {
    stationarySince StationarySince OPTIONAL,
    stationaryCause CauseCode OPTIONAL,
    carryingDangerousGoods DangerousGoodsExtended OPTIONAL,
    numberOfOccupants NumberOfOccupants OPTIONAL,
    vehicleIdentification VehicleIdentification OPTIONAL,
    energyStorageType EnergyStorageType OPTIONAL
}
```

```
AlacarteContainer ::= SEQUENCE {
    lanePosition LanePosition OPTIONAL,
    impactReduction ImpactReductionContainer OPTIONAL,
    externalTemperature Temperature OPTIONAL,
    roadWorks RoadWorksContainerExtended OPTIONAL,
    positioningSolution PositioningSolutionType OPTIONAL,
    stationaryVehicle StationaryVehicleContainer OPTIONAL,
    ...
}

defaultValidity INTEGER ::= 600

Termination ::= ENUMERATED {isCancellation(0), isNegation (1)}

ReferenceDenms ::= SEQUENCE (SIZE(1..8, ...)) OF ActionID

END
```

Figure D.1: ASN.1 specification of DENM [5]

15 Appendix E – SAE EEBL

An Emergency Electronic Brake Light (EEBL) use case is described in SAE J2945/1 [3].

Besides describing the use case, Table 4 of SAE J2945/1 [3] also describes the data elements which need to be included in a BSM message when sending an EEBL warning. Many of the data elements are similar to those which would be included in an ETSI DENM EBW message. However, the SAE EEBL BSM message additionally includes (where detailed definitions are provided in SAE J2735 [10]):

- DF_PositionAccuracy:
  - Quality of the location information
- DF_PathPrediction:
  - Prediction of trajectory along with a confidence level associated with the prediction.
- DF_PathHistory:
  - Historic geometric time tagged path over some period or distance
- DE_TransmissionState:
  - What gear is the car in
- DF_BrakeSystemStatus:
  - State of features such as traction control status, anti-lock brake system status(ABS), stability control system status (SCS), brake boost applied, auxiliary brake status
- DE_ExteriorLights:
  - Includes main lights, fog lights, hazard warning lights, indicator lights
- DE_VehicleEventFlags:
  - Includes hard braking event notification
- DE_SteeringWheelAngle:

Note that many of these data elements are included either to help with threat assessment, threat assessment confidence or system robustness.

SAE define a hard braking event as a vehicle decelerating at greater than 0.4g.

A hierarchical decomposition of the requirements in the EEBL use case and their mapping onto the various components of the system is provided in Appendix A.10 of SAE J2945/1 [3].

16 Appendix F – Detailed ASIL determination for a particular EBW hazard

In this appendix, a more detailed assessment of ASIL rating is provided for Hazard H#7.1 (Table 5-2-3) , and the work is extended to consider both the case where a human driver is the recipient of the warning over HMI and the alternative case where an Automatic Electronic Brake (AEB) system exists.

Six different scenarios are considered to further improve understanding of the EBW use case, its benefits and the impacts of a fault. We first recap how the EBW feature is supposed to be used and how it provides a safety benefit we then go on to assess what the consequences of a failure could be. Scenarios considered are:

- V2X not used:
  - Scenario 1: An idealistic scenario in which V2X is not used and all cars follow one another at a 'safe stopping distance' that would be adequate even if the leading car undertakes emergency braking
  - Scenario 2: A realistic scenario in which V2X is not used and cars do not follow one another at a safe stopping distance
- V2X is employed, a human driver receives the warning over HMI:
  - Scenario 3: As in Scenario 2 but in which V2X is now employed; the benefits of the EBW feature are demonstrated
  - Scenario 4: As in Scenario 3 in which V2X is employed by all vehicles, but in which a fault causes a leading vehicle to erroneously generate an EBW message
  - Scenario 5: A scenario in which V2X is employed by a proportion of vehicles (~ 50%); the scenario considers the consequences of a failure occurring that causes a leading vehicle to erroneously generate an EBW message
- V2X is employed, an AEB system exists in the car that receives the EBW message:
  - Scenario 6: As Scenario 5 except that an Automatic Electronic Brake (AEB) system exists in the car that receives the EBW message

Throughout the paper we consider the case of a busy, high-speed highway.

Scenario 1: Idealistic emergency braking, without V2V

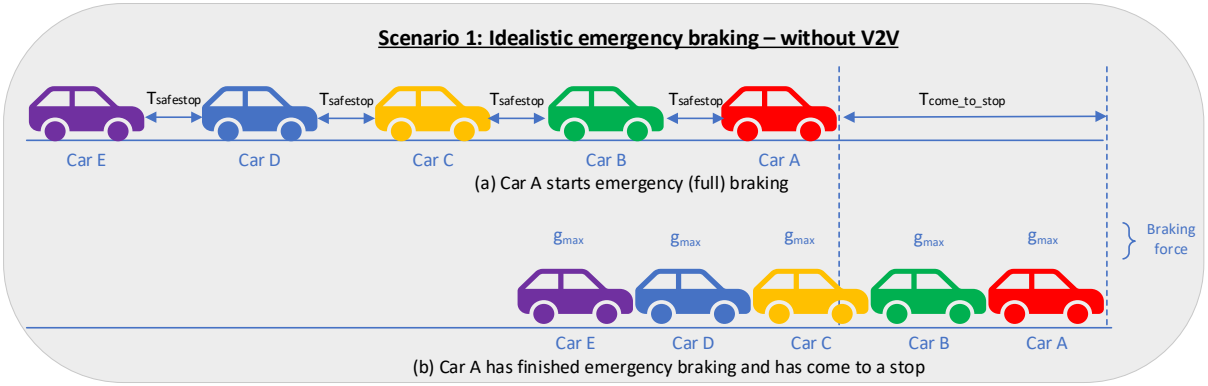

Figure F.1: Idealistic emergency braking, without V2V

Discussion of Scenario 1:

With respect to Figure F.1, we consider a simple idealistic scenario which is also one in which V2X is not used. Let's assume that Cars A, B, C, D and E are all travelling at the same constant speed and all can come to a stop in the same distance when brakes are applied fully. We assume that the time gap between the cars, $T_{safestop}$, is equal to t_{r2}, the reaction time of a driver (where for simplicity we also assume that this reaction time is the same for all drivers).

We define the deceleration of one of these cars under full braking as g_{max} (measured in m/s^2) and that when this full braking is applied, the lead vehicle, Car A, comes to a stop in time $T_{come\_to\_stop}$.

In this idealistic scenario, we can see that all cars could come to a stop and not collide, and that in order to do so all cars would have to apply the max braking deceleration g_{max} (assume here for simplicity that the drivers cannot see beyond the vehicle that is immediately in front of them and therefore get no prior warning of the need to brake, which could otherwise allow them to brake more gradually).

Scenario 2: Realistic emergency braking, without V2V

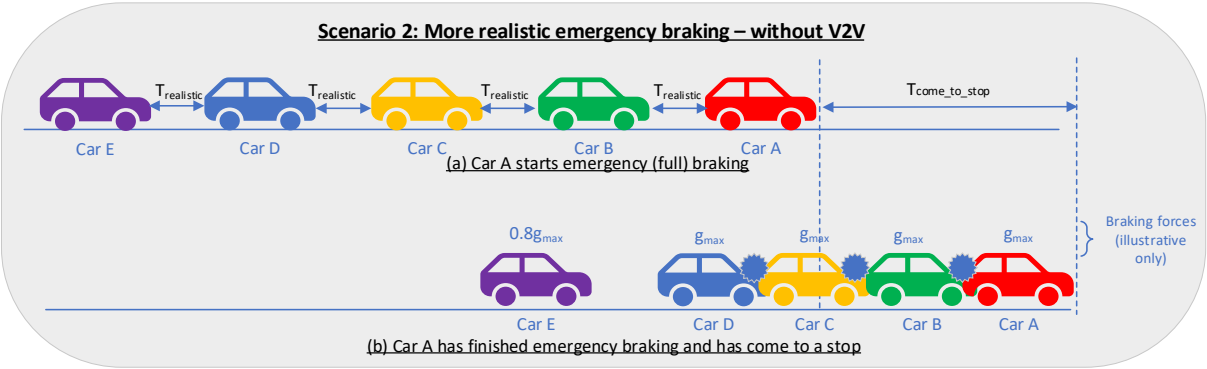

Figure F.2: Realistic emergency braking, in the absence of V2X

Discussion of Scenario 2:

In Figure F.2 we again consider the scenario where V2X is not used, but here we make some more realistic assumptions about the ability of cars to always stop in time, when a lead car undertakes emergency braking. We can make the following observations:

- Vehicles may have quite different performance in terms of their stopping distances (consider a sports car vs a truck)
- Driver reaction times can be very different
- Human drivers do not compute the theoretical required braking distance, and they do not know the current actual distance to the car in front. They may at best use rules of thumb like the 'two second rule'
- It has been shown that drivers do not, in practice, keep a safe distance on motorways. In [26] measurements made on German motorways showed that for 41% of the time, where one car follows another on a highway, there was a time gap of less than the minimum as defined by German law (0.9 secs). The time gaps became shorter the busier the motorway became. In contrast, reference [26] states that modern Adaptive Cruise Control systems keep the time gap at between 1 and 2 seconds:
    - In [19], which is a survey of surveys paper, it was concluded that the time a driver takes to respond to unexpected but common signals such as a lead car's brake lights is about 1.25 sec, whereas response times for surprise events is roughly 1.5 seconds (this response time includes mental processing time and time taken to move foot from accelerator to brake)
    - Since reaction time (1.25-1.5 secs) is greater than the time between vehicles (0.9 sec) for a large number (41%) of busy highway situations, then it can be seen that in practice the idealistic conditions of Scenario 1 are often not met, and therefore under such conditions, that collisions are highly likely to occur if a leading vehicle undertakes emergency braking
- Drivers of cars further back along the line could experience two effects which act in opposite directions:
    - A benefit for drivers of cars that are more distant from Car A is that the driver may be able to see beyond the vehicle immediately in front of them and hence may get some advance warning and be able to start applying brakes earlier and potentially with less than maximum force
    - However, a disadvantage for drivers of cars that are more distant from Car A is that the braking of Car A can lead to a shockwave effect that can result in progressively harder braking being required of vehicles further down the line, and which can ultimately result in a collision [24, 25]

Taking these more realistic assumptions into account, then with respect to the example situation shown in Figure 2b, we can observe that there is a significant chance that at least the handful of cars following Car A will crash into one another.

Scenario 3: Emergency braking with EBW V2V

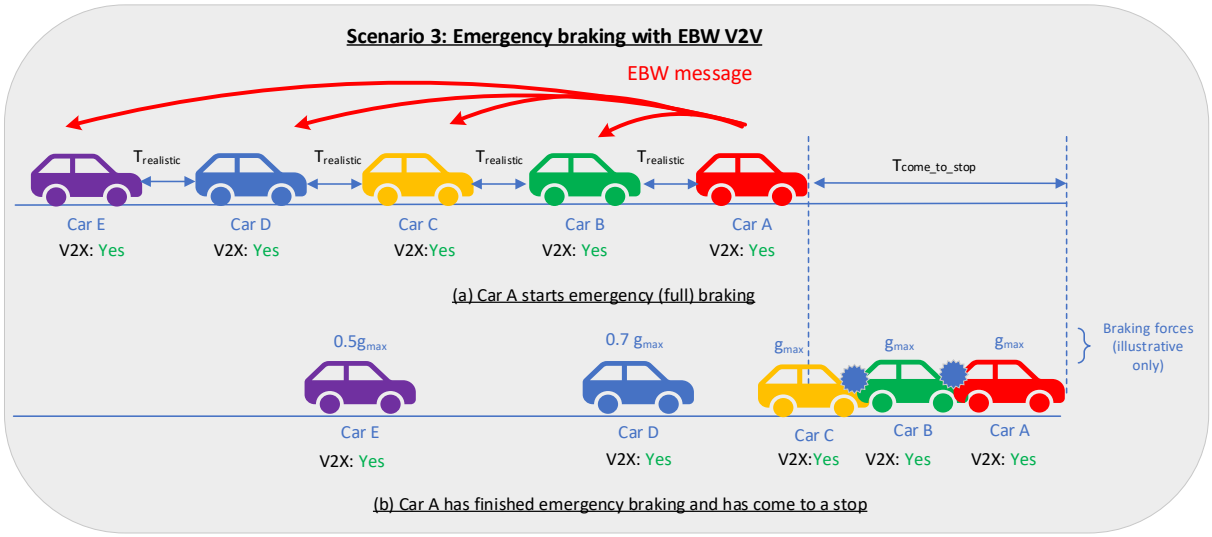

Figure F.3: Emergency braking with EBW via V2V

Discussion of Scenario 3:

In the scenario shown in Figure F.3 we consider the introduction of the V2V EBW feature on all cars. With respect to Figure 3a, Car A sends a V2V EBW message to all cars. It is assumed that each car will create an alert over HMI to the human driver indicating the degree of braking to be applied in proportion to the distance from the emergency braking event (i.e. request for heavy braking for vehicles that are close to the event, and lighter braking for vehicles that are distant from the emergency braking event).

If we contrast Figure F.3b with Figure F.2b, we see that in this example Car B still collides with Car A because the EBW message does not provide any advance notice of the emergency braking event over and above what drivers can see with their own eyes, where we also assume that the time gap between Car B and Car A was less than $T_{safestop}$. In this illustrative example we assume that the driver of Car C also does not get sufficient advance warning to prevent it colliding with Car B. Cars D and E receive the EBW V2V messages and hence can start braking earlier, and therefore with less braking force than is the case for the equivalent cars in either Fig 1b or Fig 2b. We see that in this example, and in contrast to the non-V2X Scenario 2, Car D no longer collides with Car C. This illustrates the safety benefit of the EBW V2V feature.

Scenario 4) EBW V2Vmessage is sent when it should not have been sent (all vehicles have V2X)

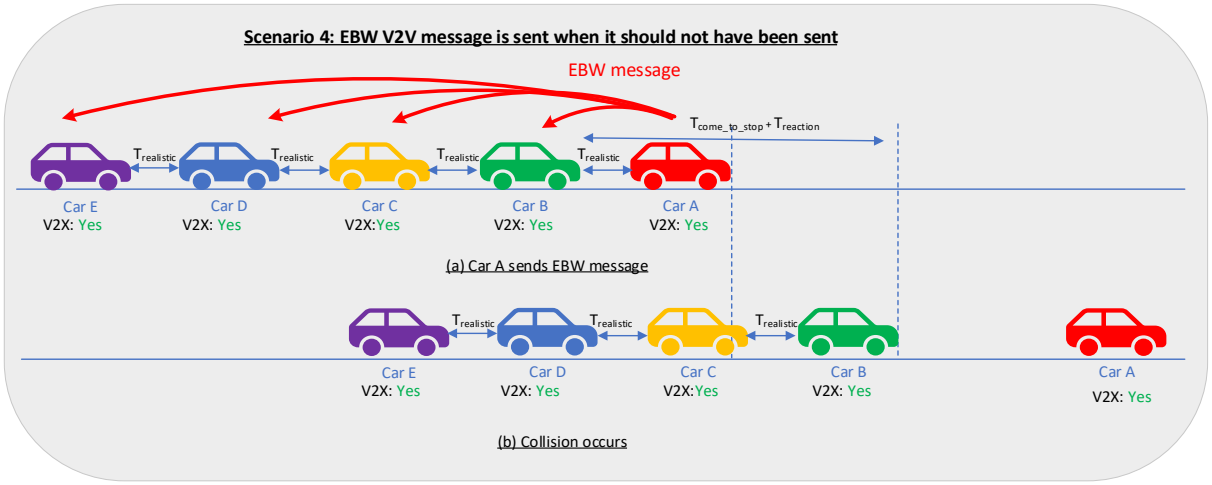

Figure F.4: EBW V2Vmessage is sent when it should not have been sent (all vehicles have V2X)

Discussion of Scenario 4:

Scenario 4 is the same as Scenario 3 but with the difference that the lead car sends an EBW message due to a fault and does not actually undertake any braking.

It is then necessary to determine whether a safety issue (e.g. accident) can occur. If we assume that the drivers of Cars B, C, D and E all receive the EBW message at the same time, and that the human drivers react at the same speed and they all apply maximum braking force (their cars having the same stopping distances), then it can be seen that no collision would result. These assumptions are somewhat idealistic, nevertheless it does indicate that in the scenario where all cars are V2X equipped, the impact of the fault should likely not result in a collision.

Scenario 5) EBW V2Vmessage is sent when it should not have been sent (NOT all vehicles have V2X)

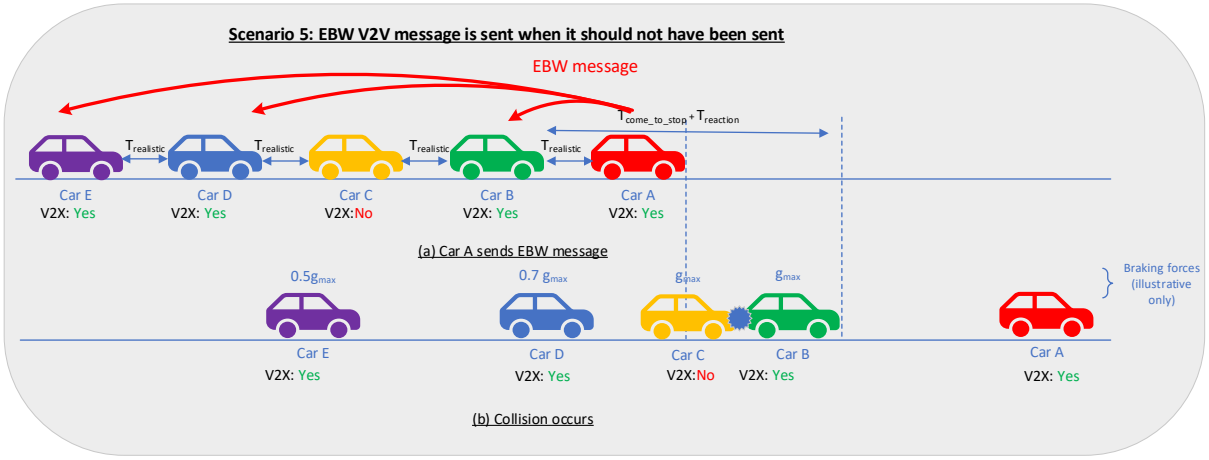

Figure F.5: EBW V2V message is sent when it should not have been sent (NOT all vehicles have V2X)

Discussion of Scenario 5:

In the scenario of Figure F.5 we consider the case where Car A, due to a fault, sends a V2V message indicating that it is undergoing emergency braking when in fact it is not, and instead continues to progress as normal. In this scenario, we assume the human driver of Car B receives a message over HMI informing the driver to brake hard, e.g. this could be an audio announcement saying something like 'brake hard'. In this scenario, we assume that the human driver of Car B has trust in the system and, therefore, applies the brakes hard until he/she comes to a standstill (note, we assess the likelihood of this happening in practice, within the 'controllability' section below). Since Car C is not V2X equipped, and has not received the message from Car A, the driver of Car C collides with Car B because we assume that the time gap between Car B and C is less than $T_{safestop}$.

ASIL rating for Scenario 5:

This section uses the methods described in [1] and [12] for selecting the values associated with the factors (exposure, severity and controllability) that are used in determining ASIL levels.

Exposure

- According to [16] in Great Britain, for cars and taxis, of the total miles travelled, 20% are on motorways, 15% are on urban A roads, and 30% are on rural A roads:
    - It can be concluded that cars spend approx. 65% of miles covered on these fast roads, as assumed in Scenario 4
- We assume V2X has been rolled out for a number of years and there is a mixture of V2X equipped cars and non-V2X equipped cars (~50% : 50%)
- Probability of cars travelling at more than 60mph on a motorway in the UK is 82% [22]. We assume that a similar high percentage of traffic on other highways ('A' roads) also travels at more than 60mph
- The probability of Scenario 5 is:
    - Probability of car being on motorway or 'A' road (dual carriageway) (0.65) AND
    - Probability of car travelling at speeds of 60mph on motorway or 'A' road (0.82) AND
    - Probability that cars are travelling at time gap of less than 0.9ss when <u>following another car at speeds in excess of 60mph</u> (0.41) AND
    - Probability of the underlined condition above (unknown, we define it as P_u) AND
    - Probability that at least one car in a line of cars that are within range of the V2X message, is non-V2X equipped, while other cars are V2X equipped is relatively high (we will approximate as ~1)
        - Assuming that ~50% of cars have V2X, and ~50% do not
        - Note that the probability of the exact scenario depicted in Figure 5 of Car B being V2X equipped and Car C not being V2X equipped is 0.5 x 0.5 = 0.25, but other combinations could lead to similar issues, for example if Car C is V2X equipped and Car D is non-V2X equipped

- Overall probability of Scenario 4 is 0.65 x 0.82 x 0.41 x Pu = 21.8 x P_u %

- Exposure classification:
  - We don't know P_u, and we have made a few approximations above, but it seems reasonable to conclude that, exposure to the scenario is high **E4** (> 10% of average operating time)

Severity

Event	Time (s)	Position of Car A (ft)	Position of Car B (ft)	Position of Car C (ft)	Position of Car D (ft)
Car A sends an EBW message (due to fault)	*T*	*S*	*S*-79.2 (a)	*S*-158.4 (b)	*S*-237.6 (c)
Cars B and D start braking	*T*+1.5 (d)	*S*+132 (e)	*S*+52.8 (e)	*S*-26.4 (e)	*S*-105.6 (e)
Car C starts braking	*T*+2.875 (f)			*S*+94.6 (f)	
Position Car C would stop in if no other cars in the way				*S*+352.6 (g)	
Car B comes to stop	*T*+7.36 (i)		*S*+310.8 (h)		
Car C comes to stop				*S*+310.8 (h,g)	
Car D comes to stop	*T*+7.36 (i)				*S*+152.4 (j)

Table F.1: Calculation of times and positions of events for Scenario 5 (for Cars A, B, C, D)

(a) At 60mph (88 ft/s) a gap of 0.9s corresponds to 88x0.9 = 79.2ft
(b) At 60mph a gap of 1.8s corresponds to 88x1.8 = 158.4ft
(c) At 60mph a gap of 2.7s corresponds to 88x2.7 = 237.6ft
(d) Assume driver reaction time to HMI is average of 1.25s and 1.5s = 1.375s
- In [19], which is a survey of surveys paper, it was concluded that driver response time to unexpected but common signals such as a lead car's brake lights is about 1.25s, whereas response times for surprise events is roughly 1.5s

In [23] it is stated that V2X latency as measured at the application layer for EEBL should be between 100ms and 150ms (average 125ms). Hence, we assume that the drivers of Cars B, D and E start braking 1.5s after Car A transmits EBW message

(e) All cars are travelling at 88ft/s (60mph). So, in 1.5s they have travelled 88x1.5=132ft
(f) The driver of Car C starts braking after he/she witnesses and reacts to the braking of Car B. Car B starts braking at T+1.5s, so car C starts braking at 2.875s. At the point Car C starts braking it will have travelled another 88ft/s x 1.375 = 121ft. Hence it will be in the position S-26.4 + 121 = S+94.6ft
(g) Position Car C would stop in if no other cars were to block its way = S+94.6+258 (see (h) below) = S+352.6
(h) Driver of Car B brakes at average expected deceleration of 15ft/s/s [11]
Using the equation ($v^2 = u^2 + 2as$, where v is final velocity, u is initial velocity, a is deceleration and s is distance travelled), then given v=0, u=88ft/s and a = -15ft/s/s, then stopping distance s=258ft
- According to NACTO [20] an average driver could decelerate at 15ft/s/s, and a reasonably skilled driver could decelerate at 20ft/s/s

(i) Time to brake = 88/15 = 5.86s
(j) S-105.6+258=S+152.4

The calculations above show that, if Car C is unimpeded, it will come to rest 42ft beyond Car B. Assuming the driver of Car C does not attempt to swerve out of its lane (which could also be dangerous) it will collide with Car B.

The severity rating allocated to a rear/front collision can be classified dependent on speed of impact.

Computation of speed of impact of Car C into Car B

Using the equation $v^2 = u^2 + 2as$, where u=88ft/s, a=-15ft/s/s, s=(310.8-94.6)=216.2. Then v (velocity on impact) = 35.4 ft/s = 38.4km/h.

Severity classification

- Table B1 [12] indicates that severity rating is likely to be **S2** (severe and life-threatening injuries, survival probable)

Controllability

- Controllability from perspective of Car B:
    - Drivers will come to trust the warning messages provided by the car. If the driver of Car B receives an EBW message, and they know that they need to react to it by braking hard, (e.g. because the HMI is a replay of an audio recording saying 'brake hard') then most drivers will do so
        - The experiments of [17] and [18] in which a leading car switched on brake lights, even though it did not in fact decelerate, indicated that the driver of a following vehicle will apply brakes (up to 54.8% of the time in the results of [17] and up to 84% of the time in the results of [18])
        - However, one question that arises here is, if the driver of Car B sees that the vehicle(s) ahead (especially Car A) are not in fact slowing down, how might that affect the degree of braking by the driver of Car B? For example, might the driver of vehicle B ease off the brakes?
            - According to NACTO [20] an average driver could decelerate at 15ft/s/s, and a reasonably skilled driver could decelerate at 20ft/s/s. Braking time to come to a complete stand still from 60mph would be (88/15) = 5.8s, so there would be time for the driver of Car B to react to the non-braking of Car A and to ease off the brakes before the car has come to a complete stop
- Controllability from perspective of Car C:
    - Car C, which is assumed to be not V2X equipped, may get no other indication that the car immediately in front is about to brake hard due to the nature of the failure (generation of EBW without proper cause), which means that controllability for the driver of the following vehicle is very poor if the driver of Car B does decide to apply the brakes hard
- Controllability classification:
    - **C2** (normally controllable – more than 90% of drivers are able to avoid the specified harm)
        - Where in this case we assume that avoiding the harm could be achieved if the driver of Car B sees that Car A is not decelerating and therefore having started to brake, subsequently either takes their foot off the brake before coming to a stop and/or starts braking more gently
            - Note that while in a short platoon of vehicles (as considered here), this action may be sufficient to avoid a rear-end collision, in longer lines of vehicles, even a temporary but sharp deceleration could result in a shockwave which could propagate back causing a rear-end collision to occur many vehicles behind Car A [24, 25]. Though in the case of Scenario 5 the likelihood of this shockwave-caused rear-end collision occurring should be reduced in many cases due to the presence of a proportion of (V2X equipped) vehicles in the line, which would be expected to start braking more gradually and at an earlier point in time than they would do if they weren't V2X equipped

Overall ASIL rating

E4-S2-C2=**B**

Scenario 6) EBW V2Vmessage is sent when it should not have been sent (NOT all vehicles have V2X), AEB applied

Discussion of Scenario 6:

Scenario 6 is the same as Scenario 5 except that AEB is applied by Car B. After Car B has received the V2V EBW message the system in Car B waits a period for the human driver to apply the brakes, and if the human driver does not apply the brakes within this period then the AEB system will apply the brakes.

Note that while it might be anticipated that other information would be taken into account in order to corroborate the contents of the V2V EBW message before acting on it (for example, Radar readings or periodic CAM/BSM messaging might be taken into account), such features should form part of the functional safety concept. Section 3 of ISO 26262 states:

> **7.4.1.2** The item without internal safety mechanisms shall be evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered in the hazard analysis and risk assessment.

If the system in Car B takes no other information into account in corroborating the EBW V2V message then it will bring the car to a standstill if the fault is such that the validity period of the EBW message is longer than the 5.87 secs

required to bring the car to a standstill, and assuming that the fault is such that Car B receives no ‘EBW cancellation’ message from Car A.

Overall ASIL rating

Based on the analysis of Scenario 5, we can conclude that this would be a situation that would be either very difficult to control, or uncontrollable for the driver of Car C, and therefore this scenario should be given a controllability rating of **C3** (less than 90% of all drivers are usually able to avoid the specified harm). Hence:

E4-S2-C3= **C**

17 Change History

Date	Meeting	TDoc	Subject/Comment
14 May 2020	Virtual Malaga meeting	0.2	TR Tdoc number: XW4-200014
3rd July 2020		0.3	Updates to EBW sections included as per agreements at the virtual Malaga meeting: • Add back in 'camera' to the EBW system architecture diagrams • Include content of XW4-200011 into the appendix and update the rest of the document accordingly.
16th July 2020		0.4	Includes changes agreed at the 16th July 2020 STiCAD conference call (acceptance of the comments made by Pirelli)
22nd July 2020		0.5	Adding ToD part in chapter 4 and change of headlines of chapter 7 to prepare inclusion of contributions from different partners.
3rd Nov 2020		0.6	Added EBW related Analysis and Conclusions sections, as discussed and agreed at the Oct 2020 virtual F2F meeting.
17th Nov 2020		0.61	Continental's 'ASIL Qualifier' contribution added
19th Nov 2020		0.62	Changes accepted following presentation at the 19th Nov 2020 conference call. Also an update made to include a new chapter in the candidate solutions section to capture other relevent work for 5GAA.
26th Nov 2020		0.7	Additions from Kurt • Consideration of the inputs from Leo about possible correlation with past/ongoing activities in 5GAA (chapter 7.4) and some additional hazards. • Some parts for ToD (Chapters 6, 7 and 9).
22 Dec 2020		0.71	• Comments from Steve and Corrado added. • Steve edited the Standards impact section to make it apply generically for ToD and EBW. • Steve edited the 'Potential standardisation approaches' section to make it generic to both EBW and ToD and moved it under the 'General' heading of the Analysis section
22 Jan		0.81	• Final additions as discussed in the Meeting at 19th January.
27 Jan		0.9	• Final version including all modifications and final review in vF2F meeting at 26th January • Resolving all change marks and final version for review outside STiCAD team.


5GAA
Automotive Association