5GAA Automotive Association

# Safety Treatment in V2X Applications

5GAA Automotive Association

White Paper

**CONTACT INFORMATION:**
Executive Manager – Thomas Linget
Email: liaison@5gaa.org

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



| | |
|---|---|
| VERSION: | 1.0 |
| DATE OF PUBLICATION: | 12 July 2021 |
| DOCUMENT TYPE: | White Paper |
| EXTERNAL PUBLICATION: | Yes |
| DATE OF APPROVAL BY 5GAA BOARD: | 01 June 2021 |

# Contents

# 1. Introduction

This White Paper describes the new challenges in the treatment of functional safety arising from the introduction of connected and distributed functions, which are typical for cellular vehicle-to-everything (C-V2X) applications.

A dedicated 5GAA technical working group performed a detailed analysis to determine, propose, and evaluate possibilities for mobile network operators, vendors, and any further identified stakeholders to provide vehicle original equipment manufacturers (OEMs) what they need to treat safety in new use cases enabled by C-V2X technologies. These new use cases include scenarios beyond those considered in the ISO 26262 standard [1], which assumes that the functional safety treatment is limited to the perimeter of a single vehicle and does not consider any C-V2X communications with functional parts outside the vehicle.

For the analysis, it was decided to study representative safety requirements for two selected use cases that well cover the relevant C-V2X scenarios of network-based information delivery and direct communication:

- V2N-enabled Tele-operated Driving (ToD)
- V2V-enabled Emergency Brake Warning (EBW)

In these use cases, the concurrent presence of multiple vehicles, communication means, remote operation, and infrastructure elements generates multiple safety design options, creating different classes of challenges that can be solved in different ways by different safety engineers.

This white paper summarises the analysis available in the 5GAA Technical Report [2]. The paper also provides some possible solutions (proposals) for addressing the related challenges. Further, those proposals could become guidelines for the safety design of connected and distributed functions, and at the same time open new standardisation work streams for extending existing specifications and procedures.

# 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 'Road vehicles – Functional Safety', Second edition 2018-12 |
| [2] | 5GAA Working Group XWI-4 STiCAD 'Safety Treatment in Connected and Automated Driving Functions' |
| [3] | Dr Ekkehard Helmig, 'Legal aspects of ISO 26262' |
| [4] | 5GAA TR T-180205, Cross Working Group Work Item Tele-Operated Driving ToD Use Cases and technical requirements, July 15, 2020 |
| [5] | SAE J3016 'Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles' |
| [6] | ETSI TS 102 637-1 v1.1.1. (2010-09) 'ITS, Vehicular Comms, Basic set of applications, Part 1: Functional Requirements' |
| [7] | SAE J2945/1, 'On board system requirements for V2V safety communications', 1 March 2016 |
| [8] | 5GAA TR T-180014, 'Working group use cases and technical requirements; Day one safety use cases; Interims status – V3.0', 27 Feb 2018 |
| [9] | 'Deliverable D1.1: Use cases, requirements, Performance Evaluation Criteria', Convex project, Version 1.1, Oct 5th 2017 |
| [10] | 5GAA Tdoc T-180234, 'Emergency Brake Warning', Ford, Continental, 5GAA WG1, Conf Call #30, Nov 20, 2018 |
| [11] | ETSI EN 302 637-3 v1.3.1 (2019-04), 'ITS Vehicular communications, Basic set of applications, Part 3: Specifications of Decentralized Environmental Notification Basic Service' |
| [12] | SAE J2945/1, 'On board system requirements for V2V safety communications', 1 March 2016 |
| [13] | SAE J2980, 'R - Considerations for ISO 26262 ASIL Hazard Classification', April 2018 |
| [14] | IEC 61784-x, 'Protocol families for fieldbus use in industrial control systems', April 2019 |
| [15] | L3-Pilot, 'Deliverable 2.3 Code of Practice for development of Automated Driving', February 2021 |

# 3. Abreviations

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

| | |
|---|---|
| AD | Automated Driving |
| ASIL | Automotive Safety Integrity Level |
| CAM | Cooperative Awareness Message |
| CC | Control Centre |
| CCU | Communication Control Unit |
| CV | Controlled Vehicle |
| C-V2X | Cellular Vehicle to Everything |
| EBW | Emergency Brake Warning |
| ECU | Electronic Control Unit |
| EEBL | Emergency Electronic Brake Light |
| ETSI | European Telecommunication Standards Institute |
| FMEA | Failure Mode and Effect Analysis |
| FFS | For Further Study |
| HARA | Hazard Analysis and Risk Assessment |
| HAZOP | HAZard and OPerability study |
| HMI | Human-Machine Interface |
| ITS | Intelligent Transport Systems |
| NOC | Network Operating Centre |
| OEM | Original Equipment Manufacturer |
| ODD | Operational Design Domain |
| QM | Quality Management |
| QoS | Quality of Service |
| RHW | Road Hazard Warning |
| RSU | Road Side Unit |
| RxV | EBW V2V message Receving Vehicle |
| SAE | Society of Automotive Engineers |
| SOTIF | Safety Of The Intended Functionality |
| ToD | Tele-operated Driving |
| TxV | EBW V2V message Transmitting Vehicle |
| UE | User Endpoint |
| VCC | Vehicle Control Centre |

# 4. The Current Landscape of Safety Standards

More and more driver assistance functions, especially in the framework of automated driving, are using and relying on some form of connectivity. *Systems and functions that depend on connectivity need to be failsafe to avoid all risks to persons and property. In this section, we explore the landscape of safety standards affecting C-V2X.* Currently, 'safety treatment' in the automotive domain focuses on system components inside a vehicle and that are under full control of the vehicle manufacturer or its suppliers (which in turn are instructed by the OEM accordingly). The related standard for road vehicles used in the automotive industry is ISO 26262 [1], which describes the different phases of the development process including item definition, Hazard Analysis and Risk Assessment (HARA) leading to a certain Automotive Safety Integrity Level (ASIL), and functional and technical safety concept, as well as hardware and software requirements and consequent development and validation. A high-level summary of the standard is provided in Appendix 1 with the aim of providing some details that will be useful to follow the methodology and conclusions of this white paper, which summarises the detailed analysis [2] carried out by 5GAA.

The ISO 26262 standard is targeted at achieving safety in vehicles and defines the safety lifecycle of electrical and electronic safety-related systems in vehicles as a means to avoid hazards [3]. While ISO 26262 covers functional safety in the event of system failures, it does not treat safety hazards that can occur without system failure.

This is covered by ISO 21448, which is a new activity underway focusing on what the function does (Safety Of The Intended Functionality, SOTIF). The field of SOTIF has recently gained importance especially in emergency intervention systems and advanced driver assistance systems, which could be exposed to safety hazards even in the absence of system failures.

Activities outside the automotive domain are tackling some of the above-mentioned challenges (e.g. Fieldbus Communication [14]) which might serve as input but cannot simply be re-used. There are also some projects that deal with similar challenges (e.g. L3Pilot [15]) and whose proposals are taken into account in this paper.

In future connected and distributed functions, at least part of the overall system (telecommunication network and/or backend and/or road infrastructure and/or another vehicle) will no longer be under OEM control. In order to provide a connected function with proper safety requirements, the OEM or its suppliers need to be able to safely monitor and assess the reliability of the system parts not under the OEM's direct control.

In the past, ISO 26262-based safety has not been in the scope of mobile radio network design and approval processes. 5G networks were simulated mainly as a function of the radio link's reliability. Agreed, validated, and certified methods for end-to-end safety evaluation do not exist, but there are niche examples where certified 3GPP-related standards operate in safety or at least high-availability domains. This includes railway (GSM-Rail evolving into 5G-Rail) and public safety communication (e.g. FirstNet in US).

In these and all other cases it is neither intended, nor possible to design systems that never fail. A common solution in the automotive sector is to detect and conceal failures and bring the vehicle into a safe state (failsafe system) or into an operation mode that keeps a certain (potentially reduced) level of functionality (fail-operational system), assuring no harm to humans in and around the vehicle. By this, safety is achieved at the expense of availability. Still, a vehicle frequently stopping or slowing down due to communication failures is simply not fulfilling its purpose and will therefore not be accepted by the market, thus the need for a detailed analysis taking into proper consideration the safety but also the usability of the designed solutions.

# 5. 5GAA Approach for Use-Case Analysis

The intention of the analysis on the two selected C-V2X use cases was not to develop a product fulfilling all ISO 26262 procedures and requirements, but rather to use the standard as a guideline for analysing the potential problems arising from connected and distributed functions which require functional safety.

The work identified potential solutions and especially looked at the communication industry's contribution in developing those functions in a safe and marketable way.
The steps followed are in accordance with ISO 26262 [1]:

- Produce an Item Definition
- Perform a Hazard Analysis and and Risk Assessment (HARA)
- Determine Functional Safety Goals

Additional steps determine:

- A set of Potential Functional Safety Requirements
- A potential set of solutions capable of meeting the most preferred Potential Functional Safety Requirements
- Possible changes needed in standards, or other industry level agreements that may be required to achieve the functional safety objectives

The safety analysis performed on Teleoperated Driving (ToD) and Electronic Brake Warning (EBW) C-V2X use cases described in the following chapters was focused on the Concept Phase, while the definition of product development requirements was considered out of scope.

# 6. V2N Use Case: Tele-Operated Driving

## 6.1. Item Definition

This use case represents a scenario where information is exchanged between two endpoints (in the specific case a Network Operating Centre, NOC, and a vehicle) through a telecommunication network.

This section identifies the items defining ToD from a safety standpoint.

### 6.1.1. Use-case requirements

An indication of non-functional requirements that may be adequate for our purposes is provided in the 5GAA ToD use case description [4], listing non-functional requirements for different variants of ToD.

### 6.1.2. 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 on Tele-operated Driving (see [4]).

Currently, there are no standardisations known for the ToD use case. However, there are discussions ongoing within different bodies (e.g. SAE) about the needs for standardisation on the technical, legal and operational side.

There are some commercial and pre-commercial products existing on the market, which mainly use proprietary implementations and interfaces.

### 6.1.3. Capabilities of actuators, or their assumed capabilities

A number of capabilities are considered in the context of this use case:

- Partially or fully automated vehicle, able to be temporarily controlled by a tele-operator
- Tele-operator has means (actuators like steering wheel, pedals) to remotely operate the aforementioned vehicle
- Remotely-operated vehicle has sensors whose data can be made accessible to the tele-operator and provide the necessary information to safely operate the vehicle
- Available means to assure time synchronisation between senders and receivers

### 6.1.4. Purpose and functionality including operating modes and states

ToD can be executed in different modes of operation. The analysis does not intend to cover all possible operation modes; instead, it intends to highlight only those requiring conceptually different aspects with respect to safety considerations.

### 6.1.4.1 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). This means the tele-operator has the means to steer, accelerate and decelerate the vehicle. The interaction of the tele-operator is mainly driven by information received from the vehicle sensors via radio communication (e.g. video, radar, lidar, ultrasonic, audio information). There might be some kind of support from the vehicle systems (responding to data from its own sensors and functions, the vehicle could override tele-operator commands by, for example, braking immediately in critical situations). Details of this interaction are part of the expanded safety concepts generated for the different operation modes.

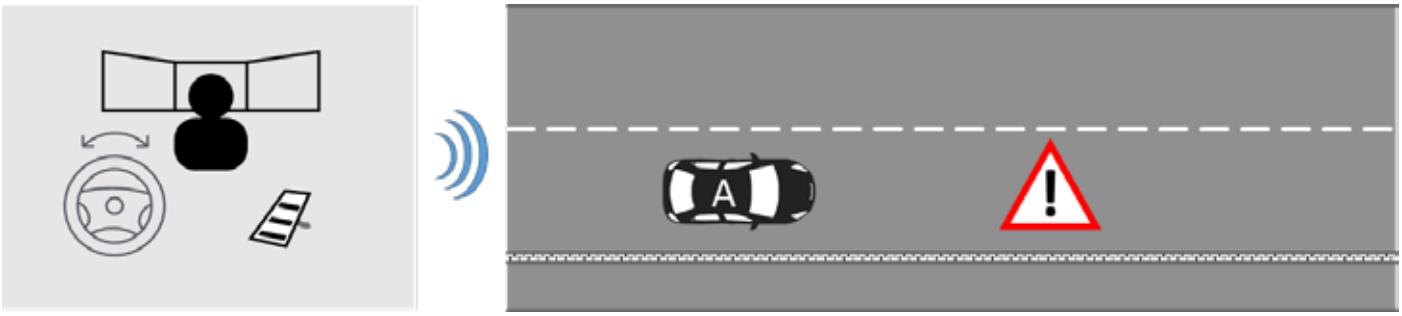



Figure 6.1 ToD direct control

### 6.1.4.2 Indirect control of the vehicle from the VCC

The indirect mode does not provide the means for the tele-operator to directly control the vehicle actuators. In this mode, the vehicle continues to drive using its automated driving features. Tele-operator support is, however, available in situations that cannot be resolved by the vehicle's automated driving system. A tele-operator could provide a way around a blocked road, for example, by allowing the automated system to do something outside its 'safe' parameters, such as driving across a footpath to keep traffic flowing.

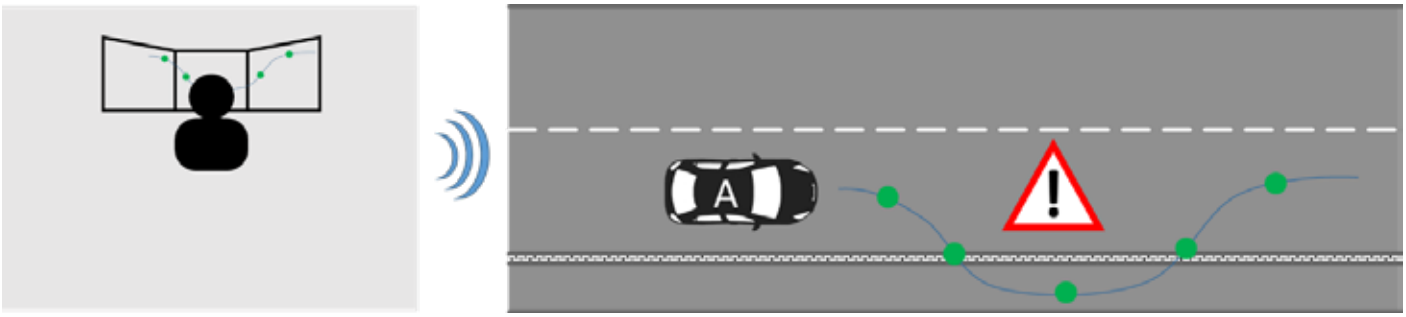



Figure 6.2 ToD indirect control

### 6.1.5. Elements of the item

The following picture shows the overall functional system architecture and identifies the relevant items involved in the direct and indirect control use cases.

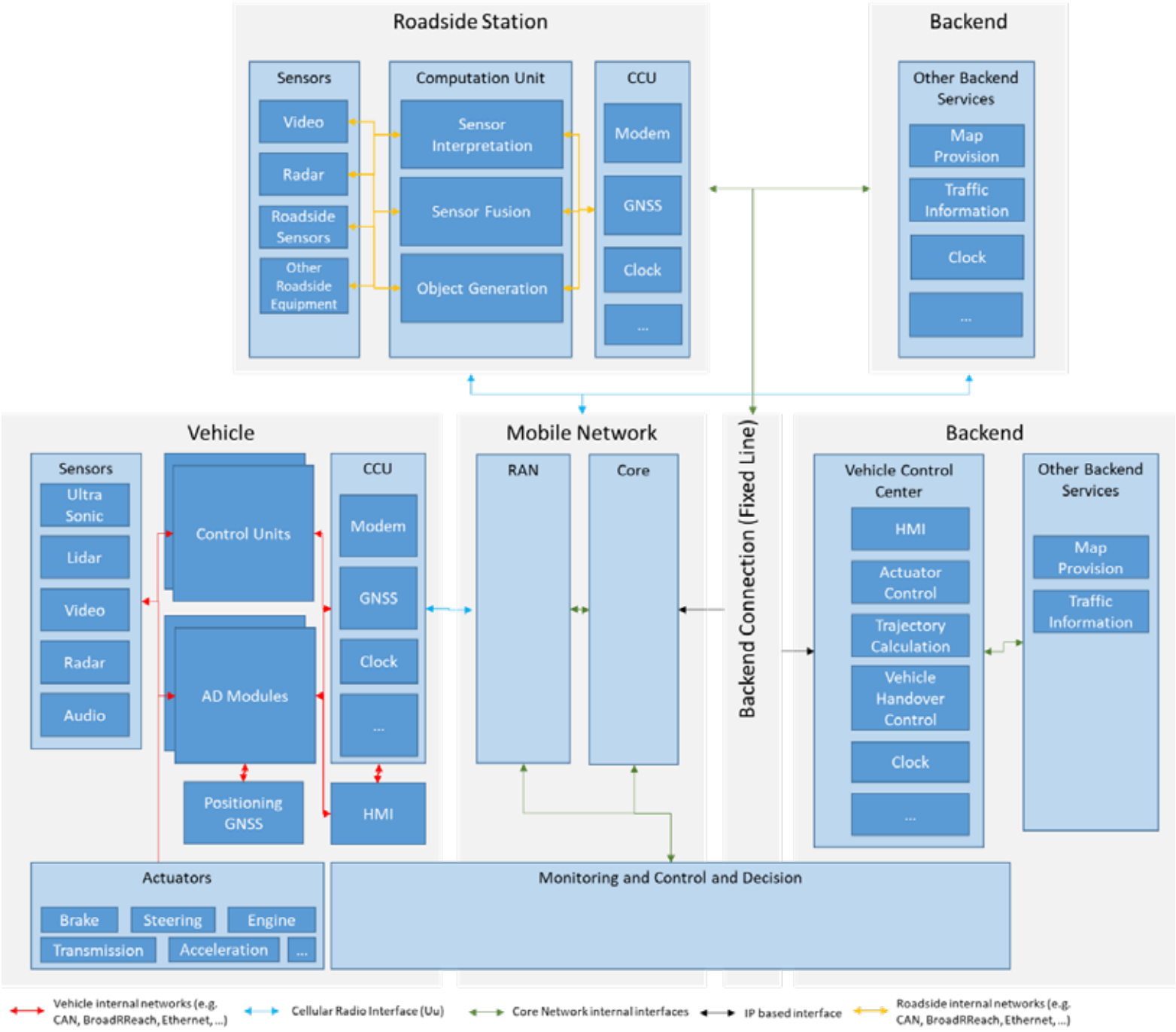



Figure 6.3 ToD overview on architecture items

#### 6.1.5.1. Direct control of the vehicle from the VCC

In the direct control mode, the vehicle's Automated Driving (AD) modules might not be involved in the operation and thus will not be part of the items in scope. For this ToD variant, no trajectories are used and thus trajectory control functions are not part of the item consideration.

#### 6.1.5.2. Indirect control of the vehicle from the VCC

In the indirect mode of operation, the in-vehicle actuators are likely to fall outside the safety consideration under the assumption that the automated driving part is not included in the safety analysis done here. Also on the VCC side, the actuator control and the Human-Machine Interface (HMI) are not considered as there is no direct actuator usage here.

## 6.2. Hazard Analysis and Risk Assessment

A full and complete HARA for the ToD use case goes beyond the scope of 5GAA and was not carried out. Instead, some representative considerations were developed in order to find representative hazards that could provide a first assessment on the possible Automotive Safety Integrity Level (ASIL) that should be met.

### 6.2.1. Operational Design Domain

The following picture provides an overview of the different classes that serve as a definition of the Operational Design Domain (ODD) for ToD. Different ODD definitions apply for the two operation modes defined before.

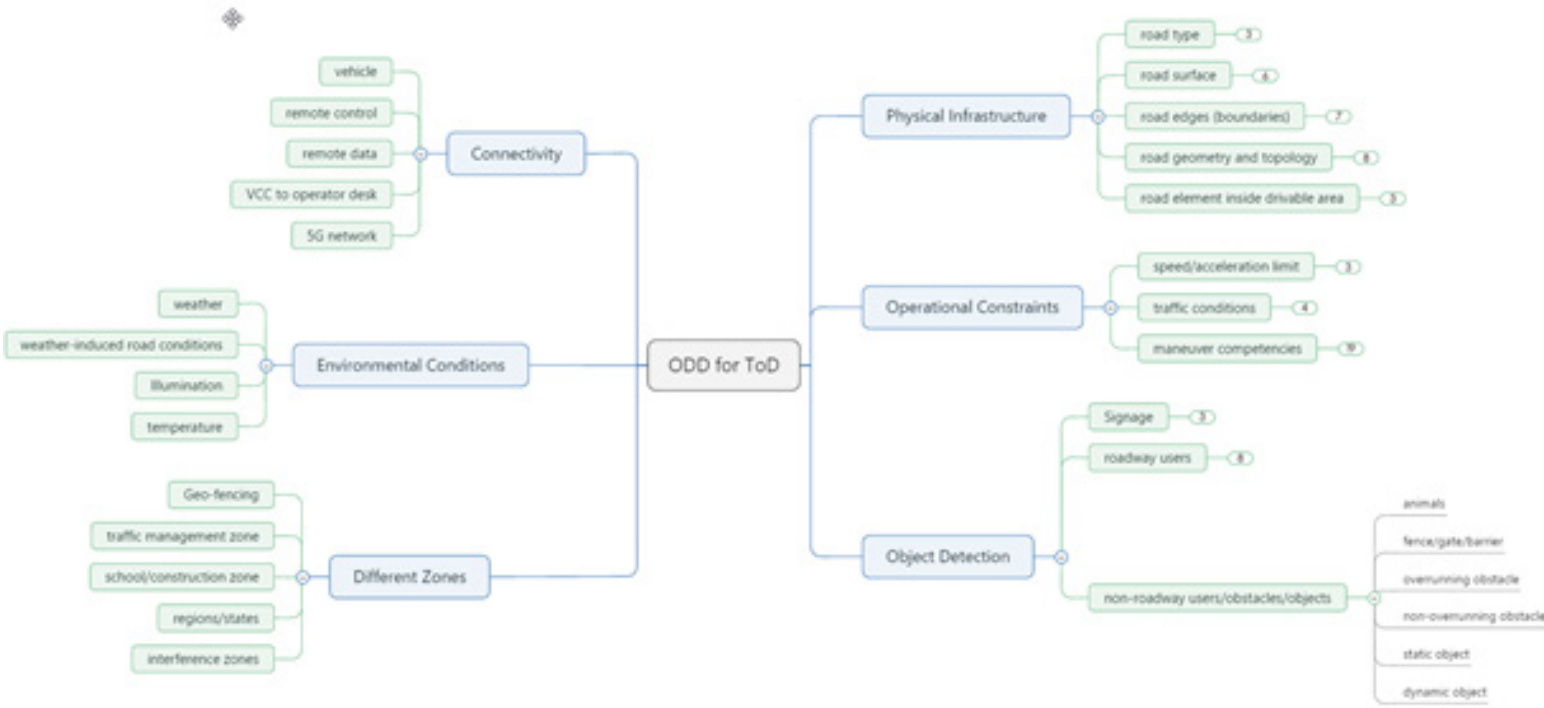



Figure 6.4 Potential ODD structure

The safety considerations carried out within 5GAA mainly concentrate on the communication part of the overall system, and therefore the ODD definition is just focusing on those parts of the system that are related to communication and does not pretend to be exhaustive. The detailed analysis of the ODD is reported in the relevant 5GAA document [2].

## 6.3. Identification of hazards

This following shows examples of hazards analysed in the 5GAA detailed document [2] with the purpose of demonstrating the approach and the type of conclusions reached through the analysis.

### Hazard example for direct control mode

| Guide Word | Application of guideword | Hazard event and its consequences |
|---|---|---|
| NO OR NOT | Control message (CM) is not sent for a certain time period by control centre (CC) to the controlled vehicle (CV) | • CV stays at a dangerous place and becomes a severe obstacle or danger for other road users<br>• Another driver is not able to react in time and thus collides with the CV |

### Hazard example for indirect control mode

| Guide Word | Application of guideword | Hazard event and its consequences |
|---|---|---|
| NO OR NOT | CM with new trajectory sent from CC does not contain necessary fields | • CV cannot perform necessary driving manoeuvre and thus becomes a severe obstacle or danger for other road users<br>• Another driver is not able to react in time and thus collides with the CV |

## 6.4. Safety goals

The following shows an example of the safety goals derived from the hazard analysis, and a possible ASIL association. It is important to highlight that in both scenarios, direct or indirect control mode, the ASIL ratings exceed the Quality Management (QM) value, showing the need for safety treatment in these V2X use cases.

| 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 | Avoid wrong control information being received by the CV | • If vehicle's autonomous sensors still function the wrong information can be checked and therefore accidents due to wrong information can be avoided – QM<br>• If vehicle's autonomous sensors no longer function or are degraded (e.g. because CC commands put vehicle outside ODD) – ASIL D |

## 6.5. Functional safety requirements and potential solution strategies

The following shows an example of the safety goals derived from the hazard analysis, and a possible ASIL association. It is important to highlight that in both scenarios, direct or indirect control mode, the ASIL ratings exceed the Quality Management (QM) value, showing the need for safety treatment in these V2X use cases.

| Fault location | Fault Category (FC) | Potential Functional Safety Requirements (PFSR) |
|---|---|---|
| CC | FC1: CC does not generate control messages when it should | **Strategies for fault avoidance:**<br>• PFSR-FC1-1 (Requirement on CC): CC implements a watchdog function ensuring regular control messages are available<br>• PFSR-FC1-2 (Requirement on CC): A real-time supervision system implemented at CC that takes care of regular message generation and sending<br>**Strategies for fault detection and mitigation:**<br>• PFSR-FC1-3 (Requirement on CC): CC informs the operator about sent messages and provides a warning if the interval between messages reaches a certain maximum value<br>**Strategies for fault detection and transition to safe state:**<br>• PFSR-FC1-4 (Requirement on CV): CV monitors the time since the last control message was received and if a certain threshold has been exceeded either move to fail-operational state (e.g. reduced speed) or, in the event another higher maximum value has been reached, enter safe-stop based on ego sensors |

# 7. V2V use case: Emergency Brake Warning

## 7.1. Item Definition

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

Two Emergency Brake Warning scenarios are considered:

- EBW scenario 1 (Human acts on message)

The EBW message results in a human receiving a warning, which may then be acted upon (SAE level 0 [5])

- 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 [5])

### 7.1.1. Use-case requirements

An indication of non-functional requirements that may be adequate for our purposes is provided in the 5GAA Emergency Brake Warning use-case description [10]. This information provides non-functional requirements for two different 'user stories'.

### 7.1.2. Legal requirements, national and international standards

The following standards apply:

- ETSI 102 637 [6] defines an Emergency Electronic Brake Light use case
- SAE J2945/1 [7], Section 4.2.3 describes an Emergency ElectronicBrake Light use case

Though not standards, the following documents provide use-case descriptions:

- 5GAA have defined an 'Emergency Brake Warning' use case [8]
- An EEBL use case was described by the Convex project [9]

### 7.1.3. Capabilities of actuators, or their assumed capabilities

The following capabilities are considered or assumed:

- Brakes are activated promptly in response to signals (foot pedal is depressed by human driver) or electronic signal (robot) and there is adequate granularity to allow a variety of braking forces to be applied

- ABS (Anti-lock Braking System)

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

- Emergency Brake Assist

Vehicle detects that the braking action applied by the human driver corresponds to an emergency braking manoeuvre, and in this case the vehicle may apply additional braking force, as needed

### 7.1.4. Purpose and functionality including operating modes and states

Two EBW modes of operation were analysed, with the purpose of identifying a greater range of possible safety-related requirements.

#### 7.1.4.1. Human acts on message

In this scenario, a Transmitting Vehicle (TxV) detects an emergency braking event (e.g. measured rate of deceleration exceeds a threshold) and transmits an EBW V2V message, received by a Receiving Vehicle (RxV). The 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 (through audio, vibration or visual methods) and take action (intended action is speed reduction).

#### 7.1.4.2. Hybrid: Human and/or robot act on message

In this scenario, the first steps are similar to the previous one, but if the human driver does not take action within a specific time, then the vehicle applies its AEB and performs a braking manoeuvre. Another scenario is when the human takes action within a specific time, but the applied braking force is not optimal, resulting in the vehicle taking corrective action.

### 7.1.5. Elements of the item

A high-level description of the item is shown in Figure 7.1.

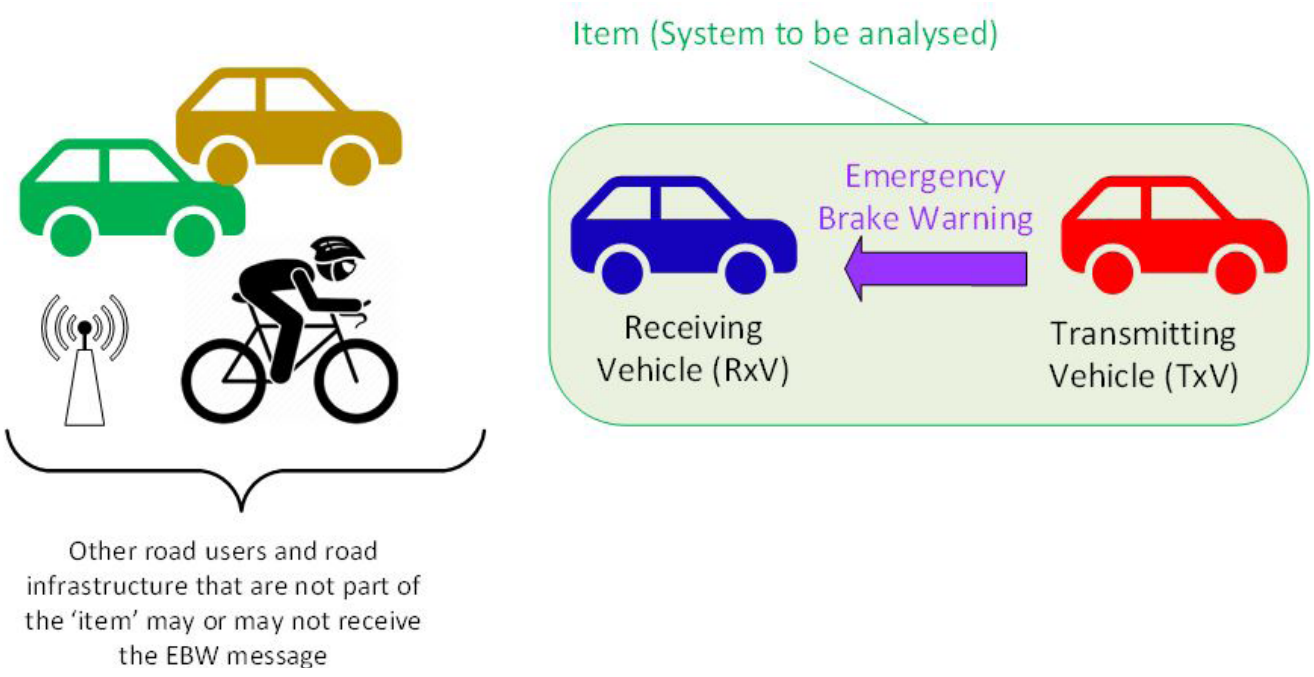



Figure 7.1 Item definition for Emergency Brake Warning

Note that it is assumed that the communication between TxV and RxV is direct and uses the PC5 interface (direct channel). 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.

Figure 7.2 shows the functional architecture of the item that is applicable for both scenarios; this architecture was partly inspired by information provided in ETSI and SAE specifications [6, 11, 12].

The green line is needed in the scenario where the robot acts on the message automatically actuates the brakes.

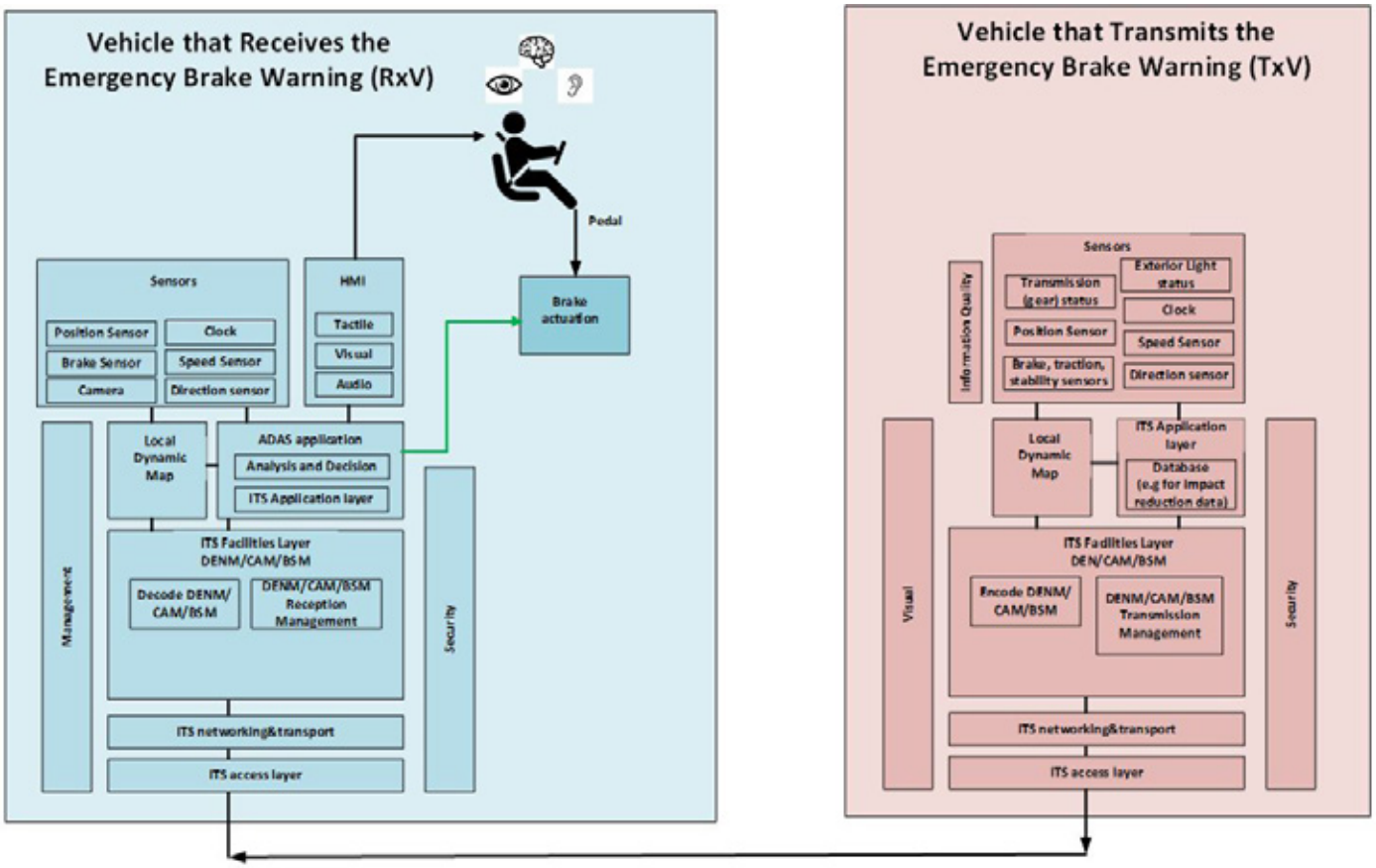



Figure 7.1 Item definition for Emergency Brake Warning

## 7.2. Hazard Analysis and Risk Assessment

### 7.2.1. Operational domain

There are many operational situations that could be considered, and many potentially relevant operational dimensions are provided in [2]. An example of a common operational situation that was used for the purposes of the detailed Hazard Analysis and Risk Assessment in 5GAA's study of the EBW use case is described below.

**Operational situation**

- Highway: Fast road on which vehicles are allowed to travel at 100km/h 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 outside their line of sight
- RxV is driven along the highway at a constant speed, no manoeuvres are being undertaken
- Road conditions and weather are good
- Highway is busy, with a mixture of motorised four- (or more) wheeled vehicles, some of which are V2X equipped and some are not

## 7.3. Identification of hazards

The following is an example among the hazards analysed in the 5GAA detailed document [2] with the purpose of showing the approach and type of conclusions reached through the analysis. The HAZard and OPerability study (HAZOP) guidewords are applied to the V2V DENM EBW message.

| Guide Word | Application of guideword | Hazard event and its consequences |
|---|---|---|
| NO OR NOT | Field within DENM message is **not** present or is **not** accurate | Consider the case where a DENM message is received by RxV, and where due to a fault in TxV, the cause code indicates an EBW event, even though the trigger/cause for the DENM message was another less critical event and TxV is not in fact undergoing emergency braking.<br><br>Impact:<br>• RxV receives the message and determines that there is an EBW event<br>• The warning is provided to the human driver via the HMI<br>• The human driver of RxV applies the brakes hard<br>• A following vehicle which is not V2X equipped, crashes into the rear end of RxV |

For the identified hazard, the guidelines provided in [13] have been applied to classify exposure, severity and controllability; the right-hand column provides an estimate of the ASIL rating. In determining this ASIL the operational domain described in the table above (Section 3.2.1) was assumed along with an assumption that there was a mixture of V2X equipped and non-V2X equipped vehicles (details of the in-depth analysis performed are provided in an appendix of [2]). The table below considers the EBW scenario where only a human driver acts on the V2X message.

| Exposure | Severity | Controlability | ASIL rating (possible range) |
|---|---|---|---|
| Exposure to the operational domain is high (>10% of time): E4 | Impact will occur at a speed sufficient to cause severe and life threatening injuries, though survival is probable: S2 | There is the possibility that drivers following a vehicle, which has erroneously sent an EBW message, can determine that there is not in fact an emergency ahead and therefore modify their braking/driving accordingly. Under normally controllable conditions, more than 90% of drivers are able to avoid the specified harm: C2 | ASIL B (E4,S2,C2) |

In the equivalent EBW case where a robot may act on the message, the analysis provided a rating of ASIL C (Exposure=E4, Severity=S2, Controllability=C3).

## 7.4. Identification of hazards

The table below shows the safety goals identified for the EBW use case.

| Hazardous event and associated risk | Safety goal | Possible ASIL ratings for selected hazardous events |
|---|---|---|
| Unintended braking of the vehicle RxV that receives a V2X message causes a vehicle that is following RxV to crash into RxV | Avoid or mitigate unintended braking if there are following vehicles | At least ASIL B, for the case where a human acts on the EBW message<br><br>At least ASIL C, in the case where a robot acts on the EBW message |
| Vehicle does not brake early enough due to EBW message not being received, thus causing a following vehicle to crash into one in front | Avoid or mitigate the situation where a vehicle does not brake when it should | Somewhere in range QM ⟶ B |

## 7.5. Functional safety requirements and potential solution strategies

The table below shows Potential Functional Safety Requirements inspired by the HARA. The functional safety requirements are marked as being 'potential', because there may be multiple ways of meeting a safety goal, with corresponding different functional safety requirements.

Following ISO 26262 Part 3, Section 7.4.2.3 [1], a number of strategies 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 events, etc. PFSRs are organised in the example 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) |
|---|---|---|
| TxV | FC1: EBW message transmitted when it should not have been | **Strategies for fault avoidance:**<br>• PFSR-FC1-1 (Requirement on TxV): Information used by the V2X application in triggering the creation and sending of an EBW message is accurate<br>• PFSR-FC1-2 (Requirement on TxV): Content of messages created as a result of other triggering conditions is 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)<br>**Strategies for fault detection and mitigation:**<br>• PFSR-FC1-3 (Requirement on RxV): Corroborate the validity of the emergency braking event through other means in RxV and do not warn the human driver over HMI until sufficient corroboration is available<br>  • 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.<br>  • 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:<br>  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)<br>  ii) Content of CAM/BSM messages transmitted by other vehicles (which might e.g. indicate rapid deceleration) |

| Fault location | Fault Category (FC) | Potential Functional Safety Requirements (PFSR) |
|---|---|---|
| TxV | FC1: EBW message transmitted when it should not have been | **Strategies for fault detection and transition to safe-state:**<br>• PFSR-FC1-4 (Requirement on: All vehicles, TxV, MA): Vehicles 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 indications of TxV's certificates on a Certificate Revocation List (CRL). When TxV learns that it has been placed on a CRL, TxV ceases to transmit messages using the V2X service. In addition, cars receiving messages from TxV can ignore them.<br>• PFSR-FC1-5 (Requirement on TxV): A simple monitoring function that is separate from the main V2X application performs 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, TxV may (tbd) prevent itself from transmitting future EBW V2X messages and thereby move itself to a safe state. |

# 8. Analysis of potential solutions

## 8.1. General considerations

The safety analysis carried out in Chapters 6 and 7 has shown that in both selected use cases potential hazards can be identified and, indeed, functional safety treatment is needed.

Safety goals were 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. Selection of a preferred safety concept is not in the scope of this analysis, but a selection will need to be made by implementers.

It is important to highlight that 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 8.1 shows this area of trade-offs.

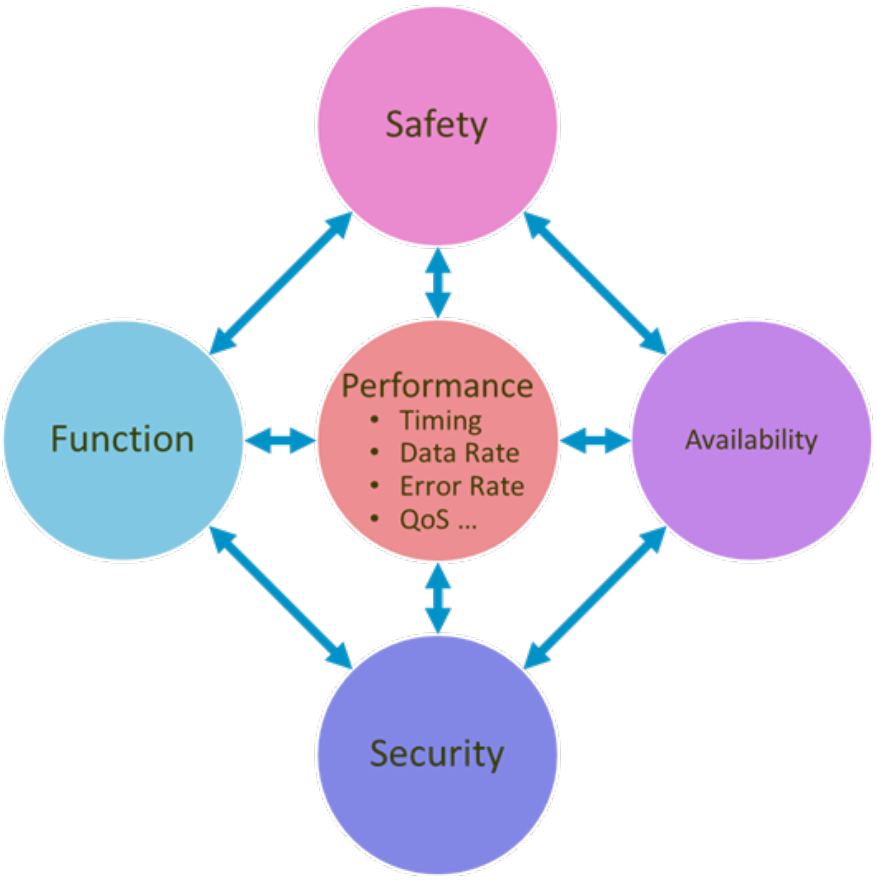



Figure 8.1 Overall trade-off between different functional requirements

During the discussions in 5GAA it was determined that there might be parts of the system that cannot be designed and implemented according to safety engineering processes, or meet ISO 26262 requirements for technical and economic reasons. However, this does not mean that use cases with functional safety requirements, such as those investigated, cannot be implemented. Indeed, some examples of how this may evolve are provided in the following paragraphs to illustrate this.

## 8.2. Candidate solutions

This section describes some candidate solutions to address some of the challenges in supporting safety-critical communication over V2X. The set of described solutions is not intended to be exhaustive, but rather reflects the outcomes of the investigations made in the context of the analysis. However, the potential solutions described hereafter are tackling the major open issues on safety in connected and distributed automotive functions, and thus serve as a good starting point for further investigations.

### 8.2.1. Open channel approach

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

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

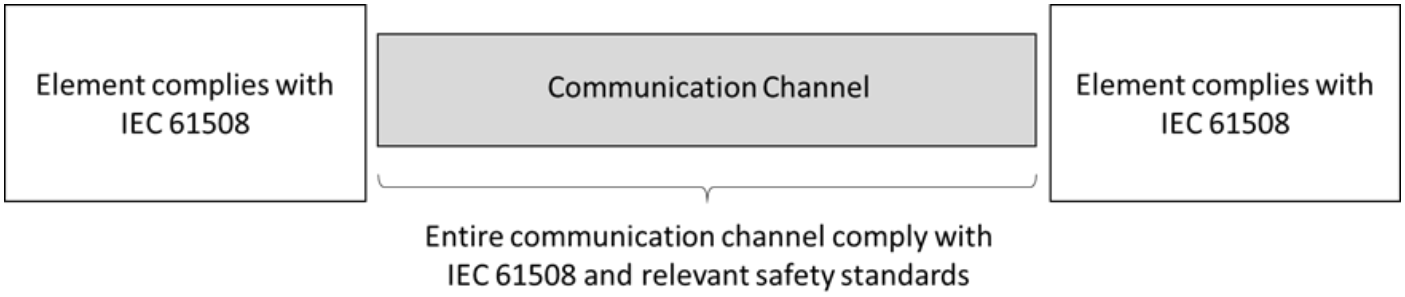



Figure 8.2: Closed channel

- Open 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 (closed channel) but relies on safety on an end-to-end basis. The connected elements at both ends comply with IEC 61508.

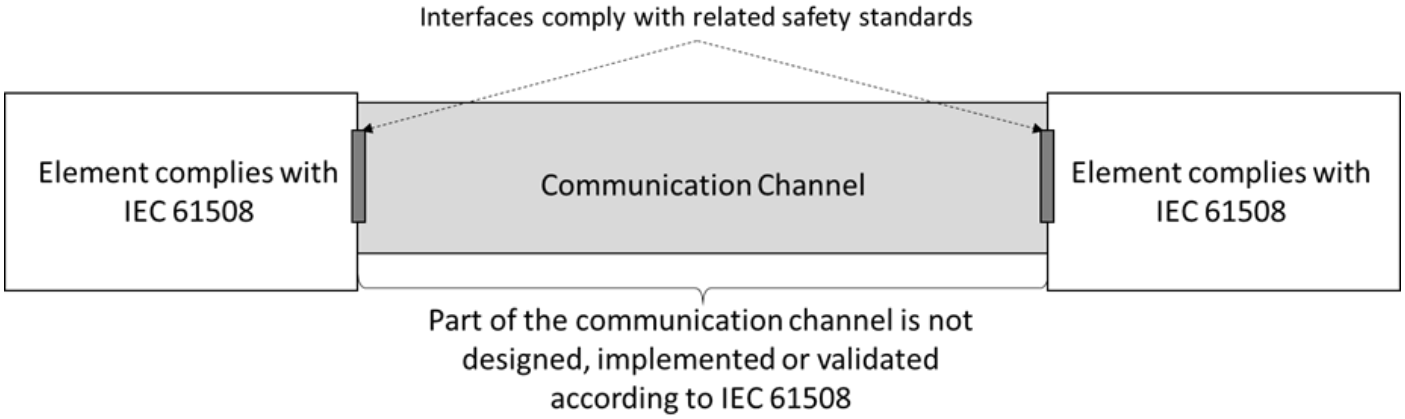



Figure 8.3: Open channel

In the closed channel approach, the properties of the communication channel are properly defined and well known. Each component is designed with integrity levels and complies 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 networks already deployed. Therefore, in practice it is very difficult to develop and verify a wireless cellular communication system as an closed channel.

Open channels look like a better approach for communication of safety-related data via wireless networks in terms of cost and flexibility. However, the open channel is associated with failure modes that could compromise safety functions and integrity. When 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 open channel, but provides control plane interfaces to reliably describe its state.

Besides the pure safety assurance, there is a need to improve the availability of the service provided by the open channel as much as needed to fulfil the given requirements for a certain product that includes the relevant function. This availability issue is one of the major challenges to telecom systems in the context of safety-critical Intelligent Transport Systems (ITS).

### 8.2.2. Mutual trust 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). 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. Additionally, there are also activities in Asia, e.g. C-SAE in China. Since the basic concepts of those standards are very similar, this chapter provides an exemplary approach based on the ETSI standards without limiting their general applicability.

In ETSI C-ITS, two standardised messages are available to help prevent accidents between vehicles: Cooperative Awareness Message (CAM) and Decentralised Environmental Notification Message (DENM).

CAM is transmitted on a periodic basis by all vehicles and contains data about position, speed, heading, etc., enabling receiving vehicles to achieve situational awareness, update their HD maps and possibly take other actions depending on the information received.

DENM is an event-triggered message that is transmitted in special situations, such as a strong braking manoeuvre. This message adds the event information to the previous data and can be used by receiving vehicles to understand the surrounding traffic situation and take counter measures against potential threats.

Data are accompanied by confidence-interval information, but unfortunately the error probability of the transmitted data cannot be accurately determined, thus making these data unusable in safety-related driving functions [2]. Therefore, more detailed discussions and potentially standardisation work are needed.

In the following pages, possible extensions or modifications of existing standards and concepts are analysed in order to support functional safety treatment.

#### 8.2.2.1. Communication-related safety requirements and measures

To limit the probability of false activation of a safety-related, V2X-based driving functions (e.g. an ASIL-rated EBW or ToD), the V2X ECU needs to implement related safety measures based on ISO 26262.

For driving functions relying on V2X communications, there are, among others, two main fault types that result in two corresponding functional safety requirements analysed below.

*Data communication protection against intentional or accidental corruption*

This first safety requirement is a typical objective for communication systems, such as internal vehicle communication buses. In our V2X examples the fault types considered are:

- EBW: Messages corrupted during radio transmission or reception
- ToD: Messages correctly generated by CC are corrupted during transmission to CV

To detect and correct (if applicable) classical communication errors, the usual features such as timestamps, checksums (CRC) and message counters must be implemented.

The analysis in [2] shows that four countermeasures (counter, timestamp, station ID, signature) available in V2X messages at application level are suitable to detect all the communication faults that ISO 26262-6 (D.2.4 Exchange of information) [1] covers, including loss, delay and corruption of information.

Moreover, as security issues are receiving more attention in the automotive industry, measures against security attacks need to be implemented as well. In the V2X communication case, the prevention of information manipulation (ensuring authenticity) and the authentication of the sender are the most important tasks. The analysis in [2] confirms that countermeasures to security attacks (such as message manipulation, falsification, etc.) are available in V2X messages.

It is therefore possible to conclude that the required detection and security features are already part of the ETSI C-ITS standards, so V2X can be deemed secure and safe in this regard.

*Data correctness and accuracy assurance*

This second safety requirement is usually addressed in a vehicle by assigning the transmitting Electronic Control Unit a related safety goal and checking that this ECU fulfils its requirements. In our V2X examples the fault types considered are:

- EBW: Content of transmitted messages not accurate
- ToD: CC generates faulty or inaccurate control messages

For the safety analysis of the receiving vehicle, the transmitting ECU is outside the vehicle boundary (and its development process).s V2X signals are not currently designed to fulfil safety requirements, current V2X systems cannot implement safety-critical functions. The fundamental objective is therefore making sure that a V2X receiver is able to assess whether the transmitted data can be used for safety-related vehicle functions. In this regard, two potential solutions can be envisioned:

a) '**Special**' security certificates are only granted if an ECU not only fulfils the usual security requirements, but also guarantees that the correctness and accuracy of transmitted data fulfils the requirements of the implemented distributed function (for example ASIL B). In this case, the format of the transmitted messages is not changed, since 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.

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

### 8.2.3. Redundancies in future automated driving functions

Even if suitable mechanisms are available in a transmitting vehicle and systematic security issues are handled by the system design, the transmission may still be blocked by other vehicles (e.g. trucks) or buildings or even by an interfering transmitter. In this situation, the full extent of a dangerous situation may not be fully recognised.

This danger can be addressed in several ways, such as by introducing 'redundancy' into the way situations are detected. One possible solution relies on a second communication channel that is not sensitive to the same radio channel conditions and delivers 'redundant information' (e.g. over a communication channel operating at different frequencies). A system capable of recognising missing commands can handle anomalous situations, e.g. by handing over control to an ego-sensor-only mode or even handing over the vehicle control to the driver.

Another redundancy method avoids relying on a single input (e.g. V2X) Using different sensors means the failure of one sensor only degrades a single function without leading to a complete function deactivation. In such sensor fusion-based designs, the guidelines of ISO 26262 need to be considered to assign the right requirements to the respective system components.

### 8.2.4. Network failure timing analysis

In the event of a failure, current network recovery control mechanisms are not fast enough for use cases with stringent latency requirements, even though they might inform the UE about the failure and trigger a network reselection.

To cope with such failures, new network control mechanisms are needed. In the absence of a open channel approach (see next section) the conclusion is that improvements are necessary on the network side.

### 8.2.5. Solutions based on 5GAA activities

Some of the approaches mentioned as potential solutions addressing the safety requirements and listed in this paper are already considered in 5GAA workgroups or other activities outside 5GAA.

Item [2] provides details on how the specific identified safety requirements for ToD and EBW use cases find possible answers in 5GAA working activities, such as Misbehaviour Detection, Quality of Service monitoring as well as prediction mechanisms.

# 9. Impacts on standards

The potential approaches to standardisation discussed in this section can apply to the ToD and 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 (involving bidirectional communication), 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 (involving bidirectional communications), it corresponds either to the Control Centre (CC) receive path or to the Controlled Vehicle (CV) receive path

In real-world V2X deployments the manufacturers of Tx_EP and Rx_EP can be different. This means that no single manufacturer has safety engineering oversight of the complete system, confirming that standardisation plays an important role in how V2X treats safety. From the analysis carried out in 5GAA [2], it looks unlikely that safety engineers from different manufacturers, if working independently, would come to the same conclusions on which ASIL is required for a particular use case.

It is therefore necessary to reach a common agreement on functional safety rules and guidelines for V2X systems. At least two fundamentally different safety engineering approaches could be considered in addressing the standardisation challenges:

*Holistic single-system safety engineering approach*

Under this approach a single entity specifies the key high-level aspects of the system, from both a functional and non-functional (safety) standpoint. However, with a V2X system, where different manufacturers may build Tx_EP and Rx_EP, the single entity responsible for defining these key aspects of the overall system design and functional safety concept should be an independent industry association or standards body.

*Modular-engineering approach*

Under this approach the vendors of Tx_EP and 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). The information might be in the form of some safety information that is signed by a certification authority. The Rx_EP then determines how and whether the message received from the Tx_EP should be acted upon based on safety-relevant information received from the Tx_EP.

Both approaches have pros and cons, which are analysed in detail in [2].

The holistic single-system approach targets generic standardisation, facilitating designers with common and agreed guidelines, both in the way safety is treated and tested (e.g. through plug-tests) and also how ASILs are assigned. It is evident that, given the complexity of V2X solutions, the time and effort needed to reach the necessary industry consensus would be long and may not bring answers in time to deploy new use cases due to the lack of definition.

The modular-engineering approach gives safety designers more freedom and autonomy in the definition and assignment of safety mechanisms in the selected items, and therefore looks like being a faster approach. However, different decisions made by different parties could well lead to solutions that do not interoperate as effectively as desired (e.g. solutions defined in different industry-borne ecosystems or alliances).

# 10. Conclusions

The objective of 5GAA activities has primarily been to identify what standardisation needs may exist related to safety treatment in V2X systems. Two representative use cases were selected to gain insight into the matter:

- V2N-enabled Tele-operated Driving (ToD)
- V2V-enabled Emergency Brake Warning (EBW)

The pre-eminent existing automotive safety engineering standard, ISO 26262, assumes that the largest item (system to be safety engineered) is a single vehicle and a single entity (i.e. an OEM), is responsible for the safety design process. Therefore, the design of safety-related (safety-critical) vehicle functions relying on V2X systems require the automotive industry to move to a new safety engineering paradigm.

Therefore, a major conclusion derived from 5GAA analysis is that **ISO 26262 needs to be updated if it is to be used for tackling the safety engineering of connected vehicles relying on 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 purpose. 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 and infrastructure, despite the fact that such cross-vehicle systems are currently outside the scope of ISO 26262.

The study concluded that safety has to be rigorously managed in at least some V2X use cases.

## 10.1. V2N-based ToD perspective

5GAA's detailed analysis [2] has shown that for the direct control use case the system needs to be designed according to ASIL D level, while for the indirect control use case lower ASILs should be acceptable. However, this depends on the capability of the vehicle to perform plausibility checks of the received indirect control commands through independent ego sensors in the vehicle.

These conclusions imply that:

- Messages exchanged between VCC and vehicle need special consideration with respect to functional safety.
- Communication networks between vehicle and VCC are currently not developed according to ASIL or other similar safety consideration schemes due to technical and commercial reasons.

Therefore:

- Under the above circumstances, in order to provide functions like ToD, an open-channel approach together with safe monitoring on both communication sides is a possible reasonable approach to fulfil the given requirements.

- To fulfil the high availability requirements of functions like ToD, the network side of the system, despite not being ASIL capable, needs to take care of and assure small outage ratios and high compliance to the given QoS requirements.

In 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 high need for standardisation on different levels, and in particular for:

- Technical interfaces (message frequency, security, format, protocols, ...)

- Commonly agreed safety considerations and concepts (monitoring, general ASILs)

- Mutual trust

- Commonly agreed homologation concepts

- Commonly agreed mutual certification

- Legal concepts

## 10.2. V2N-based EBW perspective

5GAA's detailed analysis [2] showed that when humans act on an EBW warning message the system must be designed to at least ASIL B. 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.

These conclusions imply that:

- V2X messages providing warnings to human drivers can, for at least some use cases, require safety engineering treatment.

- Different use cases have different ASIL requirements.

Therefore:

- 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 of the implemented use case that requires the highest ASIL.

Other important conclusions of the analysis are:

- With unidirectional V2X communication from TxV to RxV (e.g. an EBW case), RxV needs to assess whether the received message can be relied upon, and act accordingly; hence, the RxV must have the capability, as well as any necessary information, to assess the reliability of the received message and its content.

- 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 settings of any safety-critical information elements contained within those V2X messages.
  For the same function different potential functional safety concepts can have different potential value-added provided by V2X (e.g. if the safety concept design requires corroboration of the V2X message by RxV ego sensors, such as Lidar, which only operate in the line of sight, then the benefit of non-line-of-sight operation provided by V2X will not have been fully exploited.

# 11. Future work

Since the study was not meant to address safety treatment for V2X in an exhaustive manner, there are some additional activities that could be undertaken .

For example:

- The work could be enhanced to consider how new standardisation requirements emerge as higher levels of autonomy are considered. It is worth noting that our analysis showed the possibility that the required ASIL may increase as autonomy (SAE autonomy level) increases.

- Further aspects related to standardisation are:

    - Extension of ISO 26262 provisions on system testing, validation and verification of safety requirements in distributed systems that comprise modules from different vendors, and for which no one OEM has complete safety engineering oversight of the whole end-to-end system

    - Certification schemes targeting increased trust in safety engineering through independent auditors or bodies

- Business aspects and analysis of economic justification for implementing safety in certain functions and architectures.

- Liability extensions related to complex and multi-vendor scenarios: liability is currently with the OEM implementing the part of the function where the actuation is triggered and thus the hazard is finally caused when system failure occurs. However, future functions such as EBW or ToD might require new views and discussions on liability. For example, when a tele-operator is controlling a vehicle with limited sensor availability (i.e. due to damage), the liability might then fall on the tele-operator for the actions and commands generated. Otherwise, it stays with the OEM or other involved stakeholder including those involved in monitoring and

# Annexe 1 - A snapshot on ISO 26262 standard

## Methodology

ISO 26262 defines a well-specified process providing guidelines for designers of vehicle functions, following two major phases (Concept and Product Development), divided into steps leading to detailed technical requirements for development activities, as shown in Figure A1.

The standard introduction states "with the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures". The standard's goal is to control this complexity and reduce potential hazards and harm.

The hierarchical flow followed in the process can be summarised as follows:

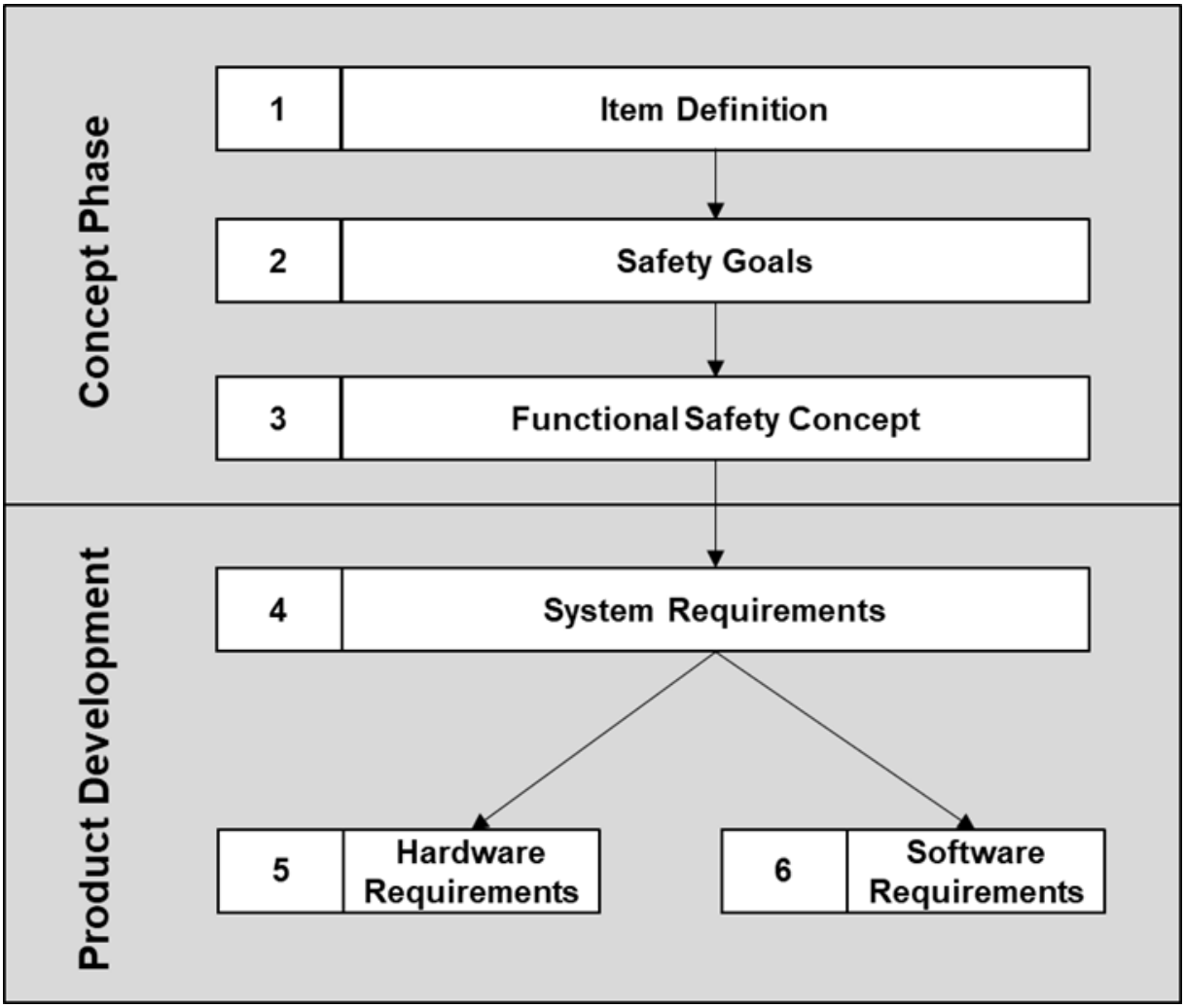
1. An item is a sub-system or component implementing a vehicle function that is analysed for hazards (Item Definition)

2. Safety Goals are top-level safety requirements for each item; these goals are used to formulate functional safety requirements, needed to avoid any unreasonable risk for each hazardous event. Safety Goals are derived by understanding all the potential hazards that may contribute to the failure of a component. Each Safety Goal is assigned an ASIL (Automotive Safety Integrity Level) attribute as well as the requirement specified to bring the vehicle to safe-state. The standard defines five ASILs, with QM being the lowest level, followed by ASIL A, B, C and finally D as the highest safety level. The process leading to Safety Goals and their related ASILs is based on the Hazard Analysis and Risk Assessment (HARA), used to identify the malfunctions that could possibly lead to E/E system hazards and to assess their associated risk. The findings are then used to formulate the safety goals required to be met for achieving safe-state.

3. The Functional Safety Concept is the specification of Functional Safety Requirements (FSR), their allocation to elements of the preliminary architecture, and their interaction necessary to achieve the Safety Goals. If a FSR derives from Safety Goals with different ASILs, then the FSR inherits the highest ASIL among the Safety Goals. A FSR describes what a system element does to ensure the Safety Goal is not violated.

4. The Technical Safety Concept is the specification of Technical Safety Requirements (TSR) which help to refine FSRs. TSRs describe how a FSR is implemented by system elements ensuring the related Safety Goal is not violated.

5. Technical Safety Requirements are allocated to Hardware and Software whose requirements specify the characteristics and behaviour of sub-elements.




It is important to underline that the HARA is performed typically by system engineers who make an evaluation of whether a hazardous event might occur during or due to vehicle operation, as well as the evaluation of its severity, the probability of exposure and the hazardous' event controllability of the driver. Such an evaluation is based on selective assumptions and assessments, typically based on experience, available statistics, historical data and specific design know-how.

From the above description, it becomes evident that the ASIL assignment for specific functions may depend on how conservative the function designers are, thus potentially resulting in different designers coming to different conclusions regards the appropriate ASIL.

For complex items, the possibility of having different assessments and conclusions increases and the introduction of additional complexity due to V2X scenarios inevitably leads to broader variance of conclusions and adopted methods.

## Operational and environmental constraints

For safety considerations during certain functions, it is important to define the Operational Design Domain (ODD). The ODD defines conditions and constraints under which the considered function is intended to work in a safe manner, and a malfunction results in a hazardous event.

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.

## Hazard Analysis and Risk Assessment (HARA)

The HARA is composed of two major steps:
**Hazard analysis**: Identifies the unintended situations that could occur during the time of failure:

- Identify malfunctions by neglecting nominal behaviour with HAZOP (HAZard and OPerability analysis) guidewords (e.g. missing, erroneous); HAZOP is an exploratory analysis that assumes risk events are caused by deviations from design or operating intentions

- Identify operational situations in which a malfunction could result in a hazardous event

**Risk assessment**: Deals with the possibility, severity and controllability of a malfunction:

- Estimate Exposure (E) of operational situation or the probability of it being within the operational situation

- Estimate Controllability (C) of hazardous event or the potential ability of a driver or other people to avoid a specified harm

- Estimate Severity (S) when a hazardous event is not controlled or the potential extent of harm to one or more individuals

The values of E, C and S are used to determine ASIL, according to ISO 26262. During the process of HARA, several hazards for an item are derived. Each hazard may have different ASIL values depending on its severity, exposure and controllability.

The ASIL defines the safety measures that need to be adopted in the development of the system (i.e. how safe the system must be to avoid any unacceptable risk). ASIL D represents the most stringent level and ASIL A the least stringent level, while QM allows designers to follow a standard system for managing quality.

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see https://5gaa.org


5GAA
Automotive Association