5GAA Automotive Association

Safety Treatment in Connected and Automated Driving Functions phase 2

5GAA Automotive Association

Technical Report

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:	3 February 2025
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	4 November 2024

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 Technical Report (TR) documents the findings of the 5GAA work item STiCAD II.

The task of the first version of the work item – Safety Treatment in Connected and Automated Driving (STiCAD) – was to determine, propose and evaluate possibilities for telecommunication operators, vendors, and any further identified stakeholders to provide what is necessary in order to enable car OEMs to better treat safety for the new use cases enabled by V2X technologies.

STiCAD II focuses on some of the unsolved matters from the first version. This includes the following tasks:

1. Detection of further use cases that need safety treatment and impose new, additional requirements and potential new concepts beyond the two use cases analysed in STiCAD I (e.g. sensor sharing, automated valet parking). To facilitate this, a simplified approach to functional safety analysis is defined.
2. Further elaboration of the mutual trust concept proposed in STiCAD I. This includes, beyond pure technical aspects like a safety qualifier flag in the communication protocols, also more conceptual and organisational concepts. To establish a real system for handling mutual trust needs a common understanding of the overall structure (e.g. what is certified, a function or functional class, a company, etc.), governance, certification (including potential certification bodies), and underlying security concepts (e.g. similar to the Protection Profile V2X Hardware Security Module currently under discussion in the C2C-CC). Special attention should be paid to simple deployment.
3. Evaluation of potential standardisation inputs from 5GAA to safety-related work in bodies like ISO, EN, UN-ECE.
4. Follow up of activities with 3GPP on safety-related features for further 3GPP releases (Rel.18 and beyond).
5. Deeper analysis and discussion of potential reliability enhancement capabilities in the communication networks (including auto-calibration, etc.).

1 Scope

The present document describes in task 1 a methodology to quickly derive the top-level safety requirements (ASIL and Safety Goals) of 5GAA use cases, re-using the work already done in STiCAD I. It further investigates possibilities to establish mutual trust in connected and automated driving (CAD) systems. Mutual trust means that a receiver is able to judge and detect the quality of the information/content coming from another source – using metadata as well as knowledge of how the data-generating subsystem has been designed, developed and implemented, and how it is maintained and operated. For this, potential measures are considered that are needed for mutual trust (e.g. data quality, development process information, operation design domain (ODD)).

2 References

- 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 – Part 3: Concept phase', Second edition 2018-12
[2]	AIAG & VDA FMEA-Handbook, First edition 2019-06
[3]	5GAA TR T-21009 Safety Treatment in Connected and Automated Driving Functions, Version 1.0, 2021-3-9
[4]	5GAA [DRAFT] TR XW5-200029 Tele-Operated Driving (ToD) Use Cases and Technical Requirements, Version 2.0
[5]	5GAA [DRAFT] TR T-220002 Automated Valet Parking Technology Assessment and Use Case Implementation Description; System Architecture and Cellular Network Solutions
[6]	5GAA_20220803_UseCaseClassification.xlsx
[7]	5GAA_20221010_STiCAD2_Task1_MalagaF2F.pptx
[8]	5GAA TR C-V2X-use-cases-and-service-level-requirements-vol-I (6.3.2)
[9]	5GAA TR C-V2X-use-cases-and-service-level-requirements-vol-II (5.2.1, 5.4.5, 5.6.4)
[10]	5GAA Whitepaper Creating Trust in Connected and Automated Vehicles
[11]	5GAA TR Trustable Position Metrics for V2X Applications

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Automotive Safety Integrity Level (ASIL): One of four levels to specify the necessary items, elements, requirements and safety measures to apply in avoiding an unreasonable risk, with D representing the most stringent and A the least stringent level.

Controllability: Ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures. Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior.

Element: System, components (hardware or software), hardware parts, or software units.

Exposure: State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

Functional Safety: Absence of unreasonable risk due to hazards caused by malfunction or misbehaviour of electrical/electronic (E/E) systems.

Hazard: Potential source of harm caused by malfunction/misbehaviour of the item.

Hazardous event: Combination of a hazard and an operational situation.

Item: System or combination of systems, to which ISO 26262 is applied, that implements a function or part of a function at the vehicle level.

Malfunctioning behaviour: Failure or unintended behaviour of an item with respect to its design intent.

Operational situation: Scenario that can occur during a vehicle's life.

Risk: Combination of the probability of occurrence of harm and the severity of that harm.

Safety goal: Top-level safety requirement as a result of the hazard analysis and risk assessment at the vehicle level.

Severity: Estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous event.

3.2 Abbreviations

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

ACC	Automatic Cruise Control
ASIL	Automotive Safety Integrity Level
AVP	Automated Valet Parking
CAM	Cooperative Awareness Message
CPM	Collective Perception Message
DENM	Decentralised Environmental Notification Message
EBW	Emergency Braking Warning
FuSa	Functional Safety
GMS	AVP Garage Management System
HARA	Hazard Analysis and Risk Assessment
HAZOP	HAZard and OPerability analysis
ISO	International Organisation for Standardissation
N/A	Not Applicable
ODD	Operational Design Domain
QM	Quality Management
SLR	Service Level Requirements
SOTIF	Safety Of the Intended Function
ToD	Tele-operated Driving
VRU	Vulnerable Road User

4 Task 1: Simplified analysis of safety needs for V2X functions

The scope of this chapter is limited to define the methodology and will not be applied to all 5GAA use cases. Nevertheless, this document provides an example on how to use the methodology. The analysis performed in STiCAD I on Tele-operated Driver (ToD) has been extended to the analysis of another use case: the Automated Valet Parking (AVP).

The defined methodology is based on [1]-3 Concept phase, clauses 5 Item Definition and 6 Hazard Analysis and Risk Assessment (HARA). The derivation of the functional safety requirements (clause 7) and technical safety requirements ([1]-4) is out of the scope of this document.

HARA is a time and resource-consuming process: it requires a team of experts in the automotive field (and for 5GAA use cases, also in the telecommunication field) to analyse every possible foreseeable malfunction of a system in every relevant operating situation of the vehicle.

The standard rigorous process is too detailed to be applicable for a first analysis of the use cases, and goes beyond the scope of this work item and of 5GAA itself. Nevertheless, HARA is a crucial phase in the development of a new automotive system because it creates awareness on the safety level required for its design, and it is therefore of interest for the stakeholders involved in 5GAA use cases.

The objective of the methodology proposed in this TR is to provide a simplified HARA analysis that can be used to achieve a first and rough estimation of the ASIL level of 5GAA use cases. The idea behind this methodology is to focus on similarity across use cases and to re-use the detailed work already carried out in STiCAD I.

Another purpose of this approach is to underline the importance of having a description of the intended use of a system within a vehicle in order to properly evaluate its ASIL. Some 5GAA use cases describe the behaviour of sub functions that can be integrated in different vehicle functions. Depending on their actual application, the ASIL allocated to each sub function can generate different results.

4.1 Item definition and 5GAA use cases

Using the definition of [1], a system realising a function at vehicle level is called an ‘item’. For 5GAA use cases, the boundary of the system is wider than the vehicle itself, because it comprises system elements that are outside the vehicle (i.e. network, sensors on-road infrastructure, elements distributed among several vehicles, etc.). Regardless, the behaviour of a 5GAA function (e.g. V2V/V2X) is always perceived by drivers, passengers, and road users at the vehicle level, therefore the definition of “item” is applicable also to 5GAA use cases.

The Item Definition is a document used as the starting point to perform the Hazard Analysis and Risk Assessment (HARA), a risk analysis tool defined in [1]-3 to evaluate the top-level safety requirements, i.e. ASIL and safety goals.

In 5GAA, all the functions enabled by 5G networks are described with the formalism of 'use cases' and 'user stories', which is meant to give a clear and deep understanding of how a function is intended to work. An item definition document has the same objective of a use case, but a different formal description. For instance, it requires that a function is stated as a requirement at vehicle level. This is very useful to identify the potential malfunctions of an item, which is the first step of the HARA: addressing a malfunction by negating it according to HAZOP guide. Therefore, to trigger safety analysis following [1], the structure of a 'use case' needs to be converted into an 'item' based on the definition (they essentially describe the same thing).

4.2 The 'Quick Item Definition'

According to [1], to start the HARA process, an Item Definition should be available. The methodology described in this document does not target an exhaustive HARA. The objective is simply to perform a 'Quick HARA', therefore benefiting from a similarly 'Quick Item Definition'.

The Quick Item Definition is needed to compare use cases at a glance, describing:

- what is the function goal = the functional behaviour,
- how it is realised = the system architecture, and
- when and where it is supposed to be activated = the operating environment.

[1] requires the analyst to define many aspects in an Item Definition. In Table 1 we have prioritised the clauses of [1] in such a way that the analyst firstly defines the function, design, and operational environment. These aspects are condensed in the priorities marked from 1 to 7. Rows beyond priority 7 are useful to have a deeper understanding of the item but are not strictly necessary to compare items. The idea is to add a column for each use case to allow their comparison at a glance.

Priority	Subclause	Requirement	Description
1	5.4.1.b1)	functional behaviour at the vehicle level, including	Brief description of the functional goal to be realised by the item.
2	5.4.2.a)	elements of the item	List of the elements that are within the item's boundary. Description can be aided by block diagrams: elements + input/output.
3	5.4.2.e)	allocation and distribution of functions among the involved systems and elements	Identify sub-functions allocated to the elements of the item (within the boundary) to realise the functional goal.
4	5.4.1.b2)	operating modes or states	Description of the dynamic behaviour of the item. Also dynamic interaction between the item's elements could be considered. Description can be aided by flow diagrams, state machine diagrams and sequence diagrams.
5	5.4.1.d2)	operating environment	Description of the target operating environment. *Example: public roads, parking facility, …*
6	5.4.1.f)	capabilities of the actuators, or their assumed capabilities	*Example: Maximum speed in which the item will operate.*

Priority	Subclause	Requirement	Description
7	5.4.2.f)	operational scenarios which impact the functionality of the item.	This is needed to start the HARA phase.
8	5.4.2	boundary of the item, its interfaces, and the assumptions concerning its interaction with other items and elements, shall be defined considering:	Select the perimeter (boundary) of the item under analysis.
9	5.4.1.d1)	constraints regarding the item such as functional dependencies, dependencies on other items	This includes: - dependencies on other E/E elements external to the item boundary (see 5.4.2) - dependencies on other non-E/E elements (e.g. mechanical elements) - design constraints imposed by the start of the design (e.g. the connection between the vehicle and the service front-end shall be 5G)
10	5.4.2.c)	the functionality of the item under consideration required by other items and elements	*Example. The item under analysis is the Blind Spot Warning. The ToD is an item (separate from the Blind Spot Warning) that can use the output or warnings to increase situational awareness.*
11	5.4.2.d)	functionality of other items and elements required by the item under consideration	*Example: The item under analysis is the ToD. the Blind Spot Warning is a separate item from ToD, but whose output could be used by the ToD.*
12	5.4.1.a)	legal requirements, national and international standards	*Examples: UNECE, FMVSS, ISO, ETSI, …*
13	5.4.1.c)	required quality, performance and availability of the functionality	List of performance requirements of the function at item level, e.g. accuracy, timing, etc.
14	5.4.1.e)	potential consequences of behavioural shortfalls including known failure modes and hazards, if any	This is needed to speed up the HARA phase.
15	5.4.2.b)	assumptions concerning the effects of the item's behaviour on the vehicle	*Note: TBD how to tailor this clause. The item's behaviour will have effects on the user more than just on the vehicle.*

Table 1 – Prioritisation of Item Definition clauses

The content of Table 1 is then further refined in view of the 'function-architecture-environment' in order to have the contents condensed into just three rows.

4.3 The 'Quick HARA'

4.3.1 Hazard identification

Once the use cases are described through a Quick Item Definition, it is possible to compare them and identify the similarities in terms of functional behaviour. The importance of studying similarities relies on the quick identification of the hazards. The analyst needs to 'abstract' the functionality of use cases in a single, common, functional requirement.

Suppose that two use cases are similar. For one of them the HARA was already performed and for the other not. For the latter, the analyst does not need to identify the malfunctions because they will be the same of the use case already analysed. A way to identify the malfunctions is thus to negate the functional requirements by means of

HAZOP 'guidewords' [2]: similar malfunctions will lead to similar hazards, therefore the process of identification of the hazards can be skipped. In summary:

Similar functions → Similar malfunctions → Similar hazards

For instance, ToD and AVP are similar in terms of functional behaviour: their functional goal is to automatically move a vehicle from a point A to a point B.

4.3.2 System architecture

The description of the architecture of the item (clause 5.4.2.a, 5.4.2.e and 5.4.1.b2) is important to derive the ASIL for use cases that describe sub-functions.

A sub-function does not directly identify an item. Some sub-functions can be integrated in several items, which means they can have several possible applications. A failure in one can lead to malfunctions in items integrated in or connected to the sub-function, therefore it is important to identify the application of the sub-function. If the HARA of the item was already performed, it will be possible to link the malfunctions of the sub-function(s) to the item's hazards. In summary:

Malfunction of the sub-function → Malfunction of the item → Hazard

The sub-function will inherit the ASIL of the item. It may be reduced by doing an ASIL decomposition between the sub-function of interest and other sub-functions within the same item.

4.3.3 Operating environment

According to [1], ASIL is computed on the hazardous events which are the combination of:

Hazardous event = hazard + operational situation

Operational situations (5.4.2.f) relevant for risk analysis with HARA are somehow linked to the operating environment (5.4.1.d2) and to the capability of actuators (5.4.2.f).

Items may be the same in terms of functional behaviour, but relevant operational situations may differ. If the HARA of an item has already been performed and the intersection of the sets of relevant operational situations is not empty, it is possible to extract the hazardous events from the HARA together with ASIL and safety goals, and to apply them directly to another similar item.

4.4 Application of the methodology to AVP

This section reports the application of the methodology to derive the top-level safety requirements of AVP from ToD.

4.4.1 ToD vs AVP Quick Item Definition comparison

The ToD and AVP use cases have been converted to the structure of the Quick Item Definition by using the tool for the analysis [6]. The main content of the Quick Item Definition has been further abstracted in the so-called function-architecture-environment triplet, as reported in Table 2 [7].

	Tele-operated Driving (ToD)	**Automatic Valet Parking (AVP) type-2**
Function at the vehicle level	Vehicle remotely driven by an operator.	Vehicle remotely parked.
System architecture	**Host Vehicle (HV)** Provide sensor data to ToD Operator for situation reconstruction. Follow trajectory (indirect ToD) or manoeuvre (direct ToD) provided by ToD. **ToD Operator** Can be a human or robot. Reconstruct situation based on data sent by HV. Provide trajectory/manoeuvre to HV.	**Host Vehicle (HV)** Drive along park snippets received from AVP. **AVP Garage Management System (GMS)** Sense the complete AVP operation area. **AVP Backend** Robot provides path snippets to HV.
Operating environment	Presence or absence of passengers inside the vehicle. Public road or restricted area. Absence or presence of vulnerable road users (VRU).	Absence of passengers. Parking area (indoor or outdoor). Maximum speed = 10 km/h. Absence or presence of vulnerable road users (VRU).

Table 2 – ToD vs AVP Quick Item Definitions abstracted

From the comparison of the functions at the vehicle level, a functional requirement at the highest level of abstraction can be formulated for both use cases as follows:

The system shall provide the vehicle with the ability to follow the path/manoeuvres imposed by a remote operator.

Note that ‘the system’ can be both ToD and AVP.

Comparison of the **system architectures** is not needed in this analysis because HARA does not depend on how the function is realised. It would be useful to perform the HARA if the AVP was a sub-function integrated within the ToD architecture, but this is not the case. The system architecture of AVP will be needed to develop the functional safety concept, but this is out of the scope of this document.

The **operating environments** are quite different; those defined for AVP can be seen as a delimitation of the one defined for the ToD. Consequently, only a subset of **operational situations** of ToD are relevant for the AVP.

4.4.2 Quick HARA for AVP

A potential high-level hazard of AVP is obtained by restricting the focus of the functional requirement stated in the previous paragraph to the vehicle level and negating it through the generic guideword 'WRONG':

"The vehicle follows the wrong trajectory."

Once we have the hazard we can go through the HARA of ToD to find similar hazards.

To find operational situations for this TR, the HARA of the ToD cases were analysed to find hazards that are applicable also to AVP. A similar hazardous event that looks applicable also to AVP is:

"The vehicle does not follow the necessary path/manoeuvres becoming an obstacle to other vehicles which might cause accidents"

The computed ASIL for this hazardous event was from B to D. We can recompute the ASIL by re-performing the HARA knowing that the resulting ASIL will be lower. The analysis could be the one reported in below Table 3.

Functional behaviour	The AVP shall provide the vehicle with the ability to follow the path/manoeuvres imposed by a remote operator.
Hazard	The vehicle follows the wrong trajectory.
Operational scenario	Vehicle driven in parking facility with VRUs walking.
Hazardous event	The vehicle does not follow the necessary path/manoeuvres becoming an obstacle to other vehicles which might cause accidents.
Exposure	E4 = high probability (scenario occurs during every drive).
Controllability	C2 = normally controllable (between 90% and 99% of the average VRUs are able to avoid harm).
Severity	S2 = severe and life-threatening injuries (survival probable) (pedestrian accident with low speed).
ASIL	B

Table 3 – Quick HARA of AVP

5 Consideration of mutual trust

5.1 General approach

In order to analyse the mutual trust matter, the chosen approach is to use the description of the selected 5GAA use cases and their information flows, highlighting the data that must be trusted by the entities involved in the use case. Through this high-level analysis and the selection of different use cases, there will be enough material to elaborate considerations on how to treat the mutual trust matter.

5.1.1 Selected use cases

The selected use cases are the following:

- Automatic Valet Parking
- Group Start
- Coordinated Cooperative Driving Manoeuvre
- See-through for Passing

They were selected among 5GAA's many use cases because they are sufficiently different from one to another to illustrate a range of important elements for the trust analysis.

5.1.2 Use case analysis and generic assumptions

For each of the use cases it was analysed which architecture items are involved (e.g. cloud, vehicle) and which data are exchanged between those items. Additionally, an analysis of potential errors was performed, identifying the main ones. Through this approach, it is then possible to identify which kind of data need to be considered in the trust analysis and between which entities or items the trust needs to be established.

Following WG1 considerations, some general assumptions are made for the implementation of the use cases; in bold are those assumptions involving/implying trust on other entities:

- Vehicles **are assumed to have knowledge** of the road topology and its surroundings via different possible input sources such as sensors, map providers, GNSS information, or functions such as local dynamic maps generated within the vehicle.
- The **positioning accuracy** of vehicles **require high-level accuracy** within the required range, as described in the use case descriptions
- **BSM and/or CAM-type cyclic** beacon messages (as examples) **are assumed to exist** and their information can be accessed and used by the participants for the execution of the complex interactions.
- Participants (RSU, Vehicles, VRUs, Applications Servers, etc.) are available at the locations where the use case takes place.
- **Communication partners are equipped with software and hardware** (e.g. compatible wireless communication technologies) enabling the use cases.

Note: How to trust full compatibility throughout the whole manoeuvre? A vehicle may declare certain capabilities that could turn out to be insufficient for safe use case performance.

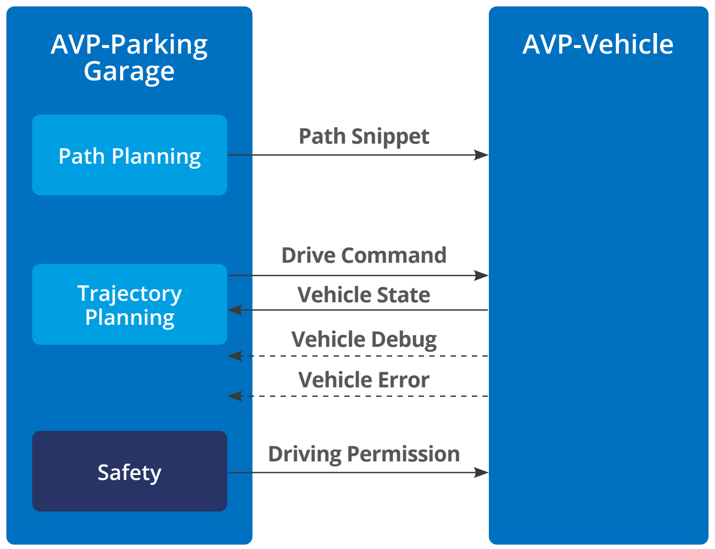
- **Acknowledgements on physical and on application layer** are possible (e.g. HARQ PH5 Rel.16)
- Lower-layer mechanisms allowing individual participants, groups or all traffic participants to be addressed are enabled and only the affected participants can actively be involved in the use case. The enabling mechanisms will be presented in a later section of this report.

5.1.2.1 Automated Valet Parking

5.1.2.1.1 How does it work?

For a detailed use case description, please refer to [5] and [9].

The attached block diagram shows the information flow between the involved entities, with a short description.



PathSnippet: Target values for path following controller

DriveCommand: Current values for path following controller measured and calculated by the infrastructure
10 ms cycle time

VehicleState: Feedback signals from vehicle to infrastructure *about 10 ms cycle time*

VehicleDebug: Debug and additional feedback signals
about 10 ms cycle time

VehicleError: Error codes from vehicle assign al to abort driving job
on demand

DrivingPermission: Safe driving boundaries calculated by the infrastructure
100 ms cycle time

Figure 1 – AVP data exchange

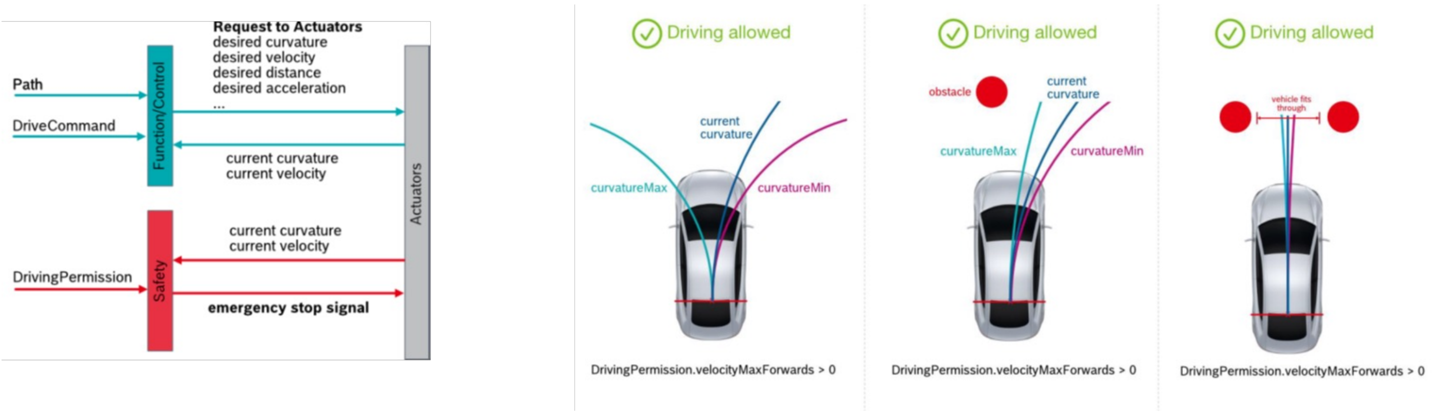


Figure 2 – AVP safety concept

5.1.2.1.2 Main failures impacting functional safety

- **Timing is not correct:** If there is an inconsistency in the timing information for different items, the real-time checking and proper reactions cannot be established.
- **Position is not correct:** If there is an inconsistency in the position information of the vehicle or of the garage area, the path snippets and trajectory could be wrong.
- **Vehicle provides wrong information in the current curvature and velocity information:** When the information provided by the vehicle is incorrect, the vehicle representation on the side of the controlling part outside of the vehicle might be wrong and thus path snippets might be miscalculated.
- **The control side provides wrong driving permission signal:** When the driving permission is wrong, the actuators might perform incorrect safety critical actions.
- **Wrong emergency stop signal:** Whenever there is a need for an emergency stop, this has a safety impact, so a missing emergency stop signal due to errors in the system is safety critical.

5.1.2.1.3 What needs to be trusted?

	Back-end	Vehicle (HV)
Modules involved in timing calculation	x	x
Modules involved in position calculation and assessment	x	x
Modules involved in current curvature calculation		x
Modules involved in driving permission calculation	x	
Modules involved in emergency stop calculation		x

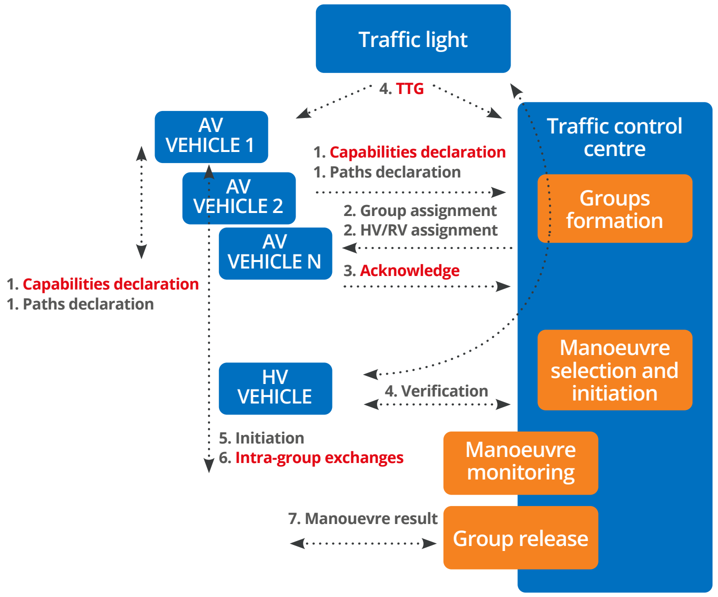
Table 4 – Trusted data in AVP

5.1.2.2 Group Start

5.1.2.2.1 How does it work?

For a detailed use case description, please refer to [9].

The attached block diagram shows the information flow between the involved entities, with a short description.



Capabilities declaration: Braking, speed, accelerations, sensors, timings...

Path declaration: Direction, path and timing information

TTG: Time to green/to red information

Group assignment: Assignment of AV into homogeneous groups and definition of vehicle role (HV, RV)

Acknowledge: Feedback from AV vehicles and trajectories/group confirmation

Verification: HV vehicle checks with traffic light and TCC information is correct and group is ready

Initiation: HV vehicle starts the manouevre and communicates to all RVs of its group to start

Intra-group updates: HV and RV exchange information during manoeuvres to signal possible deviations from the agreed plan (pedestrian crossing, delays, etc.) or manoeuvre changes; information is also sent to TCC

Manouevre result: HV communicates the positive/negative result to TCC and then releases the group

Figure 3 – Group Start data exchange

For the analysis of this use case, the following assumptions are made on the capabilities of vehicles, TL and TCC:

- The analysis considers AV vehicles.
- The analysis considers only the decentralised UC (through TCC).
- Depending on the actual design, vehicles may use their own capabilities to double check information and decisions, and this makes a big difference on the safety design and trust requirements.
- For simplification, it is assumed that once groups are formed, manoeuvre signals and requirements are not significantly different from the AVP case, even though details might differ depending on implementation details.

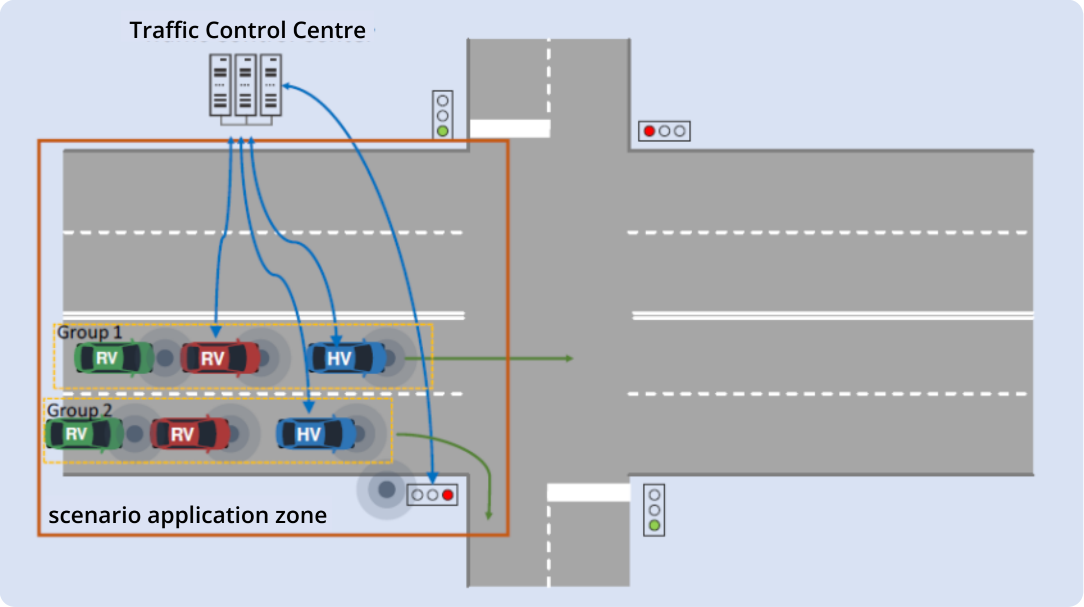


Figure 4 – Group Start schematic

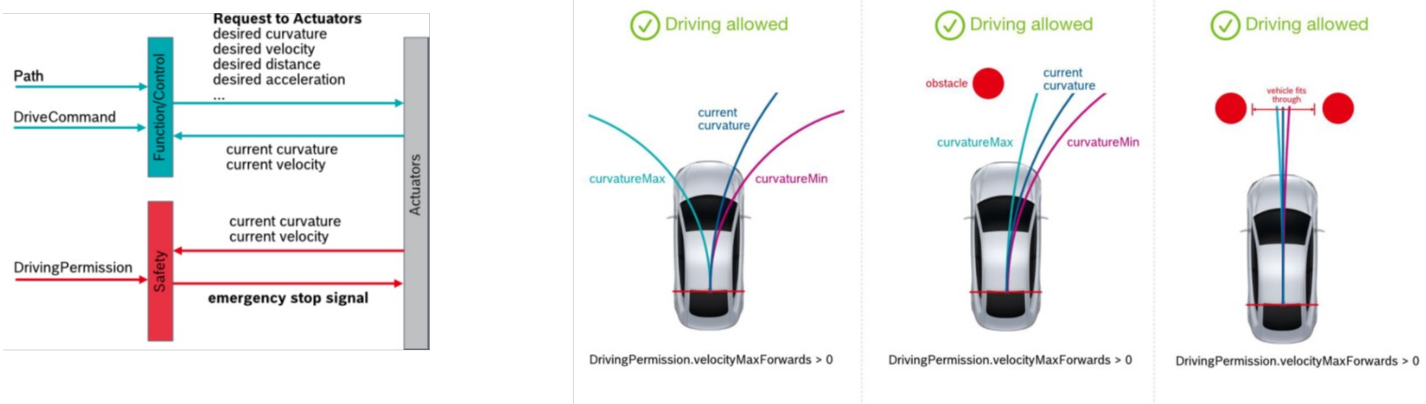


Figure 5 – Group Start safety concept (assumed to be same in general as AVP)

5.1.2.2.2 What might go wrong?

Group Start specific:

- **Self-declared vehicle capabilities are wrong or inconsistent:** When a vehicle provides wrong or incorrect information about its capabilities, the group formation could be inconsistent and during manoeuvres vehicles might not be able to respect what is needed to safely implement the agreed manoeuvre; this may mean manoeuvre abortion (less critical) or make it impossible to properly react to sudden deviations/actions, such as an emergency braking (safety critical).
- **Traffic light information is not correct:** If the traffic light provides wrong information on its status, the HV decisions will be incorrect, leading to evident safety problems.
- **RV and HV incapable of synchronising changes before and during manoeuvres:** If HV and RV vehicles are not capable of synchronising and actuating possible trajectory or movement changes, due for example to sudden changed conditions, the whole manoeuvre will be impacted.

Similar to AVP:

- **Timing is not correct:** If there is an inconsistency in the timing information for different items, the real-time checking and proper reactions cannot be established.
- **Position is not correct:** If there is an inconsistency in the position information of the vehicle or of the garage area, the path snippets and trajectory could be wrong.
- **Vehicle provides wrong information in the current curvature and velocity information:** When the information provided by the vehicle is incorrect, the vehicle representation on the side of the controlling part outside of the vehicle might be wrong and thus path snippets might be calculated incorrectly.
- **The control side provides wrong driving permission signal:** When the driving permission is wrong, the actuators might perform wrong safety-critical actions.
- **Wrong emergency stop signal:** Whenever there is a need for an emergency stop, this has safety impact, so a missing emergency stop signal due to errors in the system is safety critical.

5.1.2.2.3 What needs to be trusted?

	TCS	TL	HV	RV
Vehicle capabilities			x	x
Entities involved in timing calculation	x	x	x	x
Entities involved in position calculation	x		x	x
Entities involved in group formation logic	x			
Entities involved in HV/RV coordination	x		x	x
Entities involved in TCS/TL/HV/RV coordination	x	x	x	x [*]

Table 5 – Trusted data in Group Start

(*) As an example of the impact of design details on functional safety, RV

- may only depend on HV coordination (full platooning, high safety impact on incorrect messaging and coordination), or
- can use their in-vehicle sensors to confirm decisions (for instance RV may give priority to their cameras information instead of HV information).

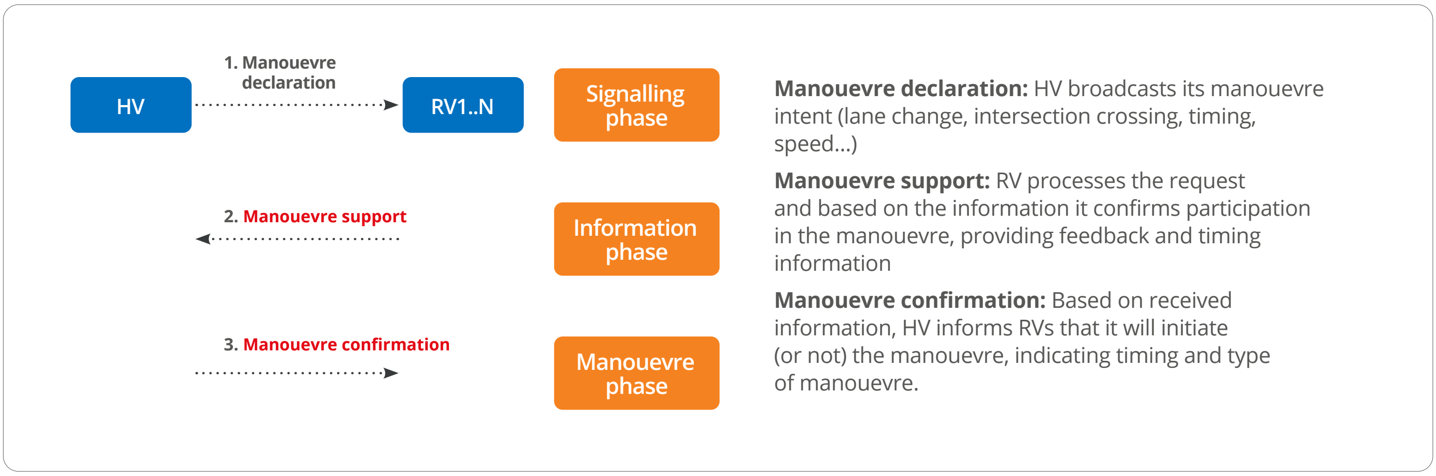
For trust analysis purposes, we can assume the worst-case scenario (from safety point of view), where RVs heavily rely on HV.

5.1.2.3 Coordinated Cooperative Driving Manoeuvre

5.1.2.3.1 How does it work?

For a detailed use case description, please refer to [9]. In the following analysis, the user story of Cooperative Lane Change is considered, and generally applies to a manoeuvre based on interactions among vehicles.

The attached block diagram shows the information flow between the involved entities, with a short description.



Manouevre declaration: HV broadcasts its manouevre intent (lane change, intersection crossing, timing, speed…)

Manouevre support: RV processes the request and based on the information it confirms participation in the manouevre, providing feedback and timing information

Manouevre confirmation: Based on received information, HV informs RVs that it will initiate (or not) the manouevre, indicating timing and type of manouevre.

Figure 6 – Coordinated Cooperative Manoeuvre data exchange

For the analysis of this use case, the following assumptions are applied to the capabilities of vehicles, HV and RVs:

- The analysis considers AV vehicles.
- Depending on the actual design, vehicles may use their own capabilities to double check information and decisions; this can make a big difference on the safety design and trust requirements.

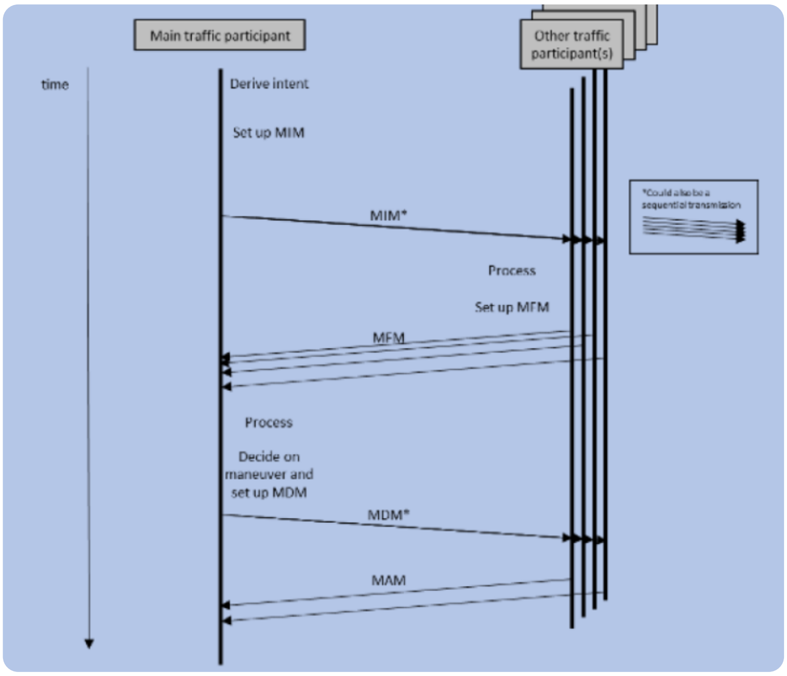

Main traffic participant
Other traffic participant(s)
time
Derive intent
Set up MIM
*Could also be a sequential transmission
MIM*
Process
Set up MFM
MFM
Process
Decide on maneuver and set up MDM
MDM*
MAM

Figure 7 – Coordinated Cooperative Driving Manoeuvre sequence diagram

5.1.2.3.2 Main failures impacting functional safety

- **HV manoeuvre definition could be incorrect:** If the HV manoeuvre definition is not consistent, the other vehicles may be misled to follow the HV and generate issues.
- **RV processing of HV data could be wrong:** If the RV processes data that are corrupted or incomplete, it may reach wrong conclusions and affect the manoeuvre success.
- **RV capabilities to effectively participate in the manoeuvre could be wrong:** If the RV capabilities are different from what is declared, HV may be misled and implement a manoeuvre logic (or timing, or speed) that RV is unable to follow or fulfil.
- **HV processing of received information to take decision on implementing manoeuvre could be wrong:** If the HV processing generates errors or wrong decisions, the RVs may follow wrong instructions and implement dangerous manoeuvres.
- **All timing/capabilities information are incorrect:** If timing and synchronisation is incorrect, the manoeuvre can be severely impacted due to misalignment between commands and actuation of logic.
- **All position information are incorrect:** If there is an inconsistency in the position information of vehicles, the manoeuvre and agreed participants could create issues.

5.1.2.3.3 What needs to be trusted?

	HV	RV
Vehicle capabilities	x	x
Entities involved in timing calculation	x	x
Entities involved in position calculation	x	x
Entities involved in data processing	x	x
Entities involved in HV/RV coordination	x	x

Table 6 – Trusted data Coordinated Cooperative Driving Manoeuvre

As an example of the impact of design details on functional safety, RV decisions

- may only depend on HV coordination (high safety impact on incorrect messaging and coordination), or
- can use their in-vehicle sensors to confirm decisions before and during manoeuvres (for instance the RV may decide to stop a manoeuvre at any time based on its own assessment).

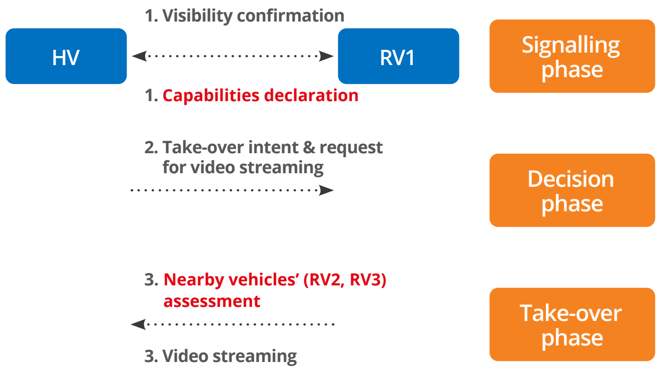
For trust analysis purposes, the worst-case scenario (from safety point of view) is assumed, where RVs heavily rely on HV processing and decisions and follow manoeuvres.

5.1.2.4 See-through for Passing

5.1.2.4.1 How does it work?

For a detailed use case description, please refer to [8].

The attached block diagram shows the information flow between the involved entities, with a short description.


1. Visibility confirmation
HV
RV1
1. Capabilities declaration
2. Take-over intent & request for video streaming
3. Nearby vehicles' (RV2, RV3) assessment
3. Video streaming
Signalling phase
Decision phase
Take-over phase

Capabilities declaration: Streaming capabilities, data rate, latency, range other vehicles positioning…

Visibility confirmation: Confirmation of mutually robust available link (thanks to capabilities declaration)

Take-over intent & video streaming request: HV manouevre declaration and request for video streaming from RV

Nearby vehicles' assessment: Information from RV1 about nearby vehicles' position, speed (optional additional information from RV1 if capable, otherwise the whole decision is left to the video streaming)

Video streaming: High-bandwidth streaming from RV1 to HV; *the first video frames and the previous assessment allow HV to confirm the passing decision*

Figure 8 – See-through for Passing data exchange

For the analysis of this use case, the following assumptions are made on the capabilities of vehicles, HV and RV1:

- The HV is driven by a human driver and must have a high-resolution display.
- The HV and RV1 must be able to send/receive high-bandwidth video and signalling messages (in particular speed and position).
- The infrastructure contribution is informative only: it signals areas where overtaking is possible and allowed.

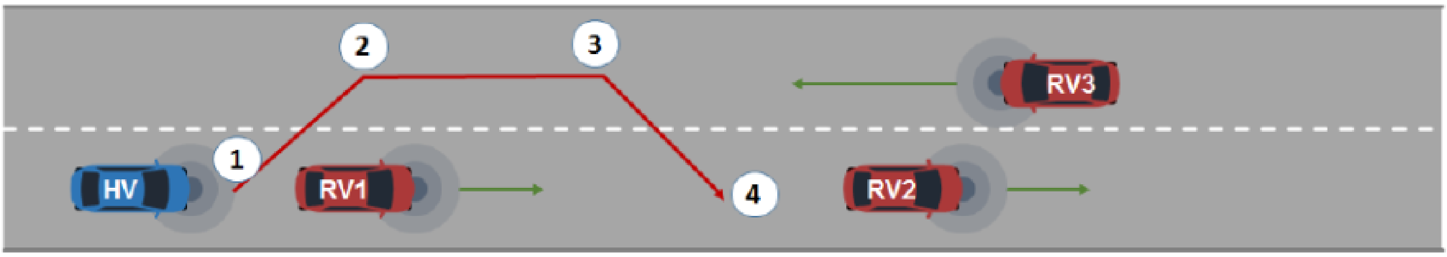


Figure 9 – See-through for Passing schematic

5.1.2.4.2 What might go wrong?

- **Self-declared vehicle capabilities are wrong or inconsistent:** If RV1's capabilities are incorrect, the HV may take wrong decisions on position, speed of arrival and other information that can impact the manoeuvre success.
- **RV and HV are incapable of keeping proper video stream before and during manoeuvres:** If video streaming is not ensured at the proper quality, rate and latency during overtaking of the HV vehicle may experience safety problems.
- **(If present) The RV assessment of th eRV2/RV3 position and speed is wrong or incorrect:** In case there are other vehicles and the RV1 is providing information to the HV on those vehicles in order to implement a take-over, the RV's assessment capabilities (for instance relative distance and speed of other vehicles) must be appropriate to avoid risks to the HV.

5.1.2.4.3 What needs to be trusted

	HV	RV1
Vehicle capabilities declaration		x
Nearby vehicles assessment (if used)		x

Table 7 – Trusted data in See-through for Passing

5.1.3 Generated concept definition

From the analysis performed in the previous chapter of the selected use cases, it is obvious which kind of information should be considered in a general concept about trust in data quality, as defined in Chapter 5.2. Some examples are timing information, position information, and vehicle capabilities. This is all considered in the following chapter to discuss possible approaches including a definition of general trust concepts and how trust can be mutually shared and assured in the typology of distributed systems under consideration.

5.2 Trust model concept

The meaning of trust might be very different depending on the context in which it is used or applied (e.g. trust in data, trust in devices, trust from an integrity point of view). For clarification of this important definition, a very intensive discussion was carried out in this work item. Together with these discussions, a coordinated approach with the 5GAA work item [10] was performed. It was agreed that a more general definition of the different meanings of trust in certain contexts is carried out in [10] while STiCAD II only considers a certain meaning of trust as needed for the further work in this work item, mostly related to functional safety. Referring to the more general definitions adopted in [10], for STiCAD II trust is formed as a combination of trustworthiness on the trustee side and the ability to prove trust on the trustor side with respect to important properties for functional safety, which in turn is a combination of other properties such as accuracy or robustness.

It has therefore been agreed that the definition given in Chapter 5.2.1 stands for trust in the context of STiCAD II. Additionally, some definitions are needed to avoid misunderstandings as the following terms are sometimes interpreted differently.

5.2.1 Important definitions

5.2.1.1 Resilience

Ability to anticipate, resist, adapt to or quickly recover from a potentially disruptive event, whether natural or man-made. Resilience is a property that extends the time in which a system is available ('availability').

5.2.1.2 Safety

In general, safety is defined as the absence of unreasonable risk. Thus, it is a requirement for robustness suitable to prevent harm in the event of a failure, unintended misinformation or missing information, e.g. subsystem failures or inadequate subsystem implementation. Additionally, redundancy is a well-known safety mechanism to avoid hazards due to a malfunction.

Remark: Intended and malicious misinformation and denial of service are part of the safety concept (security aspects).

5.2.1.2.1 Functional safety

Functional safety, or FuSa, is the absence of unreasonable risk of personal injuries for involved humans (probability of harm occurring and the severity of that harm judged to be unacceptable in certain contexts according to valid societal concepts of morals) caused by a malfunctioning E/E system.

5.2.1.3 SOTIF

Distinguishable from functional safety – avoiding unreasonable risks/hazards caused by a system malfunction – 'safety of the intended function', or SOTIF, targets the avoidance of unreasonable risks due to potentially hazardous behaviours related to functional insufficiencies.

5.2.1.4 Availability

Availability is the property of a system, service, or data to be accessible and operational when requested by authorised users or, in short, 'readiness for correct service' (e.g. with a specified minimum average uptime). It ensures that the necessary resources are reliably and consistently available, with or without (rare) interruptions, failures, deliberate attacks, and thereby enabling the execution of the intended tasks.

5.2.2 Definition of mutual trust

Trust for V2X safety means having faith in the content of received V2X data from the point of view of functional safety and SOTIF. This implies the following about the data and their context:

- Knowledge of the intended use.
- Information about the required quality and accuracy.
- Analysed knowledge of how the data generating subsystem was designed, developed, implemented, maintained, and operated.

5.2.3 Definition of information to classify data

Trust is not a mono-dimensional property, there are different properties of trustworthiness that can be evaluated and not every use case will need to consider all those properties. Each property, in turn, is related to evidence that can be used, for example, to calculate trustworthiness or serve as basic parameter for KPIs. Data such as mean value, standard deviation, and the 95th percentile can function as evidence related to accuracy (or properties of accuracy). Figure 10 provides quite an exhaustive set of known properties and illustrates different possible viewpoints for different use cases (e.g. not all use cases will need to be mindful of data transparency or consider privacy or functional safety). In general, a certain use case will use a subset of trustworthiness properties (maybe weighted with different importance factors) to perform an overall trustworthiness assessment of the data received from a certain trustee.

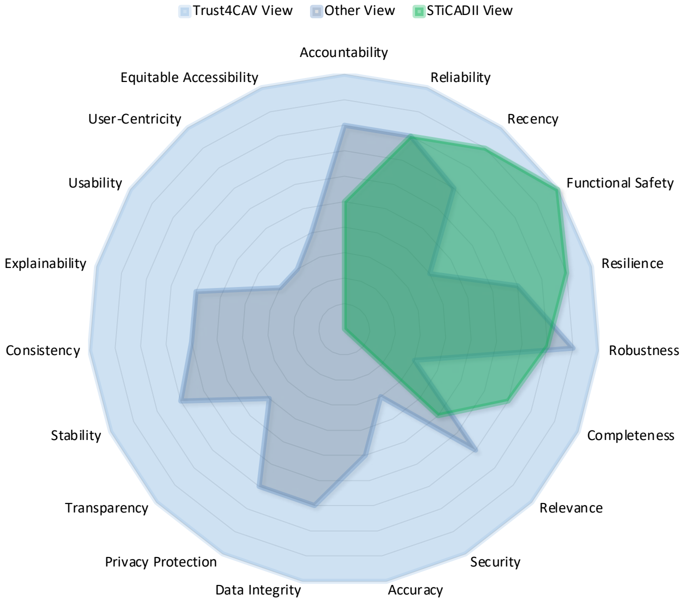


Figure 10 – Trustworthiness properties

Therefore, it is difficult to assemble all of the pieces of evidence for a trustworthiness assessment, and this should be narrowed down to the evidence related to the trustworthiness property under evaluation. This document concentrates on evidence that is needed to assess trustworthiness in a FuSa and SOTIF context as well as on evidence where a reasonable assessment has yet to be exhaustively performed (e.g. an evaluation of how data positioning accuracy can be considered was carried out in work item [11] and does not need to be repeated or data recency considerations and its related data have been studied in a variety of activities).

Some examples of such evidence are:

- Sensor capabilities
- ODD
- Many others (automation level, data provider intention for own data use, state machine information…)

Trust4CAV attempts to provide a more exhaustive approach to assessing generic trustworthiness.

In the rest of this chapter, the aforementioned examples of information will be used to highlight some of the challenges and potential solutions.

5.2.3.1 Sensor capabilities

The data considered here are mainly generated by different types of sensors (RADAR, Cameras, LIDAR, GNSS, etc.). In order to decide on the trustor side about the possibility of using sensor data for a certain ASIL-relevant function, it is necessary to have some knowledge about the sensor's capabilities. For the receiving side it is important not only to interpret the data received from a certain sensor, but it is also necessary to understand the possible limitations of the sensor itself. Examples of such limitations might be the resolution in all data dimensions, its spectral characteristics (e.g. a RADAR sensor) or the technology (CCD or CMOS) used (video sensor). All of this meta information is important to use as evidence on the receiver side in order to judge if and under which conditions data can be used for the intended functions. Other information that might influence data usability is the sensor position and consequent potential occlusions or blind spots together with the sensor health status.

Why all this is important can be illustrated through a simple example. Assume that the sender has installed a sensor for an automatic cruise control (ACC) function. In this case the sensor will be mainly optimised to detect objects and their speeds in the longitudinal direction because other characteristics, such as the object's transversal speed, are not important, and the sensor is installed in a way that best fits this function. In this example, the receiver wants to use the sensor information for a different function such as lane keeping. In this case, the sensor blind spots that are tolerable and unimportant for the ACC function might be unacceptable for the lane-keeping function, and the absence of knowledge of this sensor characteristic makes the data less trustworthy or even unusable. However, if the receiver becomes aware of the blind spots, it could decide how extensively it can use the data or if it needs to complement them with additional information.

An important consideration is that pure transmission of the evidence/information alongside the standard data may be virtually impossible for several reasons. The following table lists some problems and provides potential approaches to overcome them.

Problem	Potential solutions (combinations might be considered)
Data volumes leading to very high required data rates	As some inputs are static and do not change frequently, they might be only transmitted once in a special initial 'advertise' message. Sensor characteristics could be broken down into standardised sensor classes. The sender would therefore only need to transmit the class of the sensor since the characteristics of each class would be known by the receiver.
The sender does not want to share details on its implementation	Using the class approach described above, the sender could hide part of the detailed information. The sender could only send secondary information, e.g. detected objects (including free space areas) with related quality indicators – in this case the sender can use its existing sensor knowledge to generate quality information.
All data would need to be standardised	Class approach would limit the amount of data standardisation but would imply standardising the classes according to their underlying characteristics.

Table 8 – Problems and potential solutions

5.2.3.2 Operation design domain

For safety considerations relating to a certain function, it is important to define the operational design domain or ODD. The ODD describes 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 functional system 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 active the respective actions defined in the safety concept (such as 'safe stop') need to be safely performed/concluded.

A receiver wishing to use data from a sender in an ASIL-relevant function needs to know the ODD of the sender's sensors so that it can blend it with its own ODD. An ODD can also be complex (see [3]) and faces similar kinds of problems as those affecting sensor capabilities, thus also similar solutions could be used. In addition, if the sender and the receiver are very far apart from each other, the conditions (like weather or road conditions) at the sending and the receiving end might be different, so the sender would also need to provide information about weather conditions.

Another approach could be that the sender evaluates its ODD and sends data only if it is inside its own ODD and informs the receiver otherwise. This approach would be more convenient when the receiver and the sender ODDs are the same or similar, of course under the assumption that ODD definitions are aligned.

5.2.3.3 Others

There is a lot of other information that can be used by the receiver as evidence to assess the trustworthiness of received data with respect to functional safety. The amount of information is huge and cannot be exhaustively discussed in this report, however there are some important additional points that should be mentioned.

One important aspect is data completeness. There is a big difference between not having any information about a certain area relevant for an automotive function and. Therefore, limiting information is always critical as the receiver is unaware if it was available at the sender side and/or was intentionally not provided (e.g. to save data capacity in the case of a congested channel) or if data were not received. Consequently, in communicating functional safety-relevant functions, data completeness should always receive high priority. It is important to make the receiver of data aware of certain conditions or details about the transmission, such as a sensor blind spot on the sending side.

Another important piece of information is to indicate to a receiver what kind of functions the sender is performing based on its data (e.g. if the sender is to perform active driving operations based on its own data). Knowing that the usage of such data involves critical applications/measures and thus strict data quality on the sender side, the recipient of that information can assume it is of higher trustworthiness. Closely related is the automation level capability of the sending vehicle. A sender that has the capability to drive in L3 or above can be better trusted to generate reliable data. Of course, this only works if data are related to autonomous driving and depend on the sender ODD when such data were generated.

Another type of information that might be important in this context concerns the status of the sender 'state machines'. In a closed system where sensor data and the function are on the same side, the state information and implicit knowledge of the state machine design are often used in making decisions. In the distributed systems under consideration, this information is not known at the receiver end and thus cannot be used. Transferring the complete state machine information as additional metadata looks rather unrealistic as it would disclose a lot of proprietary information and is unlikely to be acceptable for the sender. Nevertheless, the receiver needs to take into account this uncertainty of the sender states during its functional design.

5.2.4 General data qualification base

It is quite unrealistic to assume that all types of evidence/data can be transferred together with the sensor information. There are different reasons why this is unlikely including, for example:

- Excessive data volume (a complex ODD definition might extend the pure sensor data by orders of magnitude).
- Privacy and security issues (very complex metadata might, for example, be used to derive the identity and the intentions of a sending vehicle, and could be a potential source of security attacks).
- Liability issues (a sender could not want to assume liability for all the metadata).
- Industrial secrets (sending information about the state machines implemented on the sending side would generate deep knowledge on the receiver side, which is not intended to be shared)

Therefore, it is necessary to discuss possibilities to transport a certain type of information from the sender to the receiver without explicitly sending delicate information. For some information it might, however, make sense to add metadata to the user data. The following passages provide some options on how this problem might be overcome.

5.2.4.1 Possibilities to send metadata

Data related to the evidence might be sent on request or broadcasted from the sending side. Both approaches have advantages and disadvantages. The following figure and table show examples and comparisons for the different approaches.

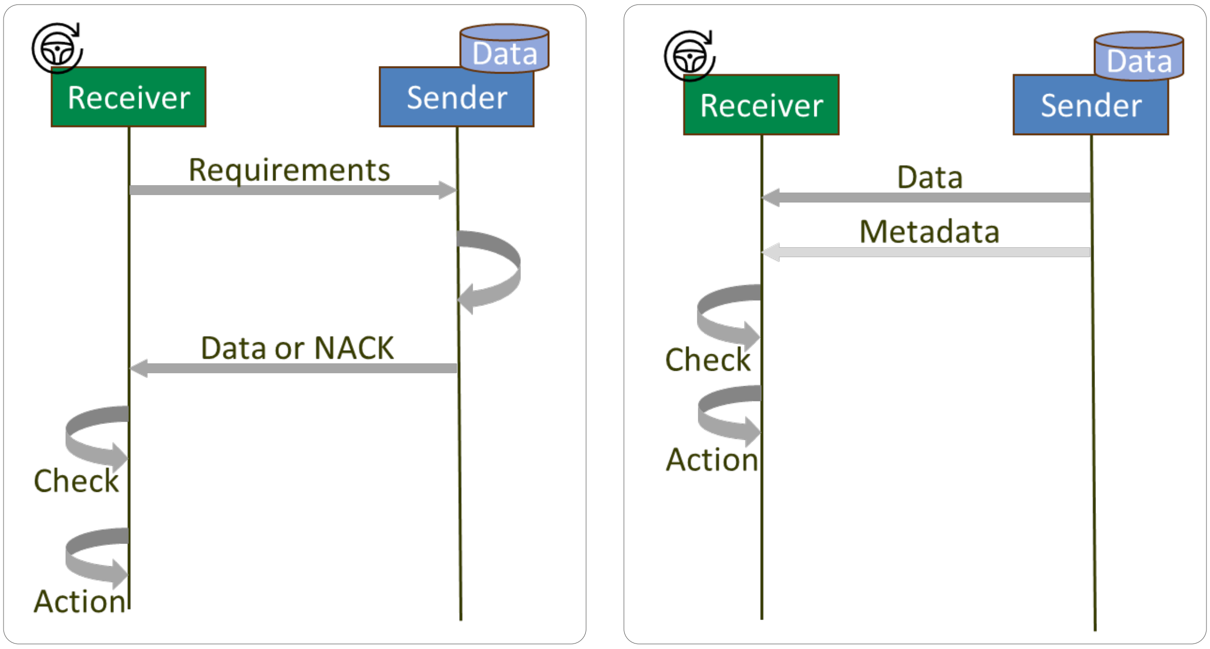


Figure 11 – Handshake vs. broadcast

Handshake		Broadcast	
Sender knows exactly what the receiver wants to do (this is an advantage as the sender can use this information to better tailor its information and also inform the receiver about potentially critical usage)	+	No information on intended data use from sender side (sender cannot consider this in the data it sends)	-
Transmitter can tailor its data for the intended purpose (as the sender most probably best knows about its own data, the sender can benefit from data provided in a way tailored best for the intended use at the receiver end)	+	Transmitter sends data as is, with no tailoring	o
Transmitter provides some form of commitment (as the sender can decide not to react to the request if it does not regard its data as sufficient to meet it, sending shows that the transmitter provides some commitment)	o	No commitment given by transmitter	+
Both sides have additional information (the knowledge of the intended use on both sides can be used to improve the quality and appropriateness of the data)	+	Information flow just in one direction	o
Handshake needs more time and is more complex (several rounds of data exchange need more time, acknowledgements need to be generated which adds complexity)	-	Less complex	+

Table 9 – Handshake vs. broadcast comparison

5.2.4.2 Potential approaches

One of the main problems discussed in the previous paragraphs is that sending a large amount of evidence-related data might not be possible due to channel capacity limitations. Besides, it might not be feasible to process big volumes of data at the receiver end under strict time constraints, especially for functions needing to exchange data at high update rates and very low latency.

One approach to overcome this issue is to send at least the data not subject to frequent changes in a sort of initialisation/update phase, and store the resulting evaluation – i.e. a trustworthiness class or value or the pure property of sent data – in a repository on the receiver side, and then map it against the user data in order to judge if such data can be trusted or not. The way this could actually be implemented depends on the protocols used. In a V2X scenario, for example, it would make sense to couple this mutual exchange and update of evidence data with the first occurrence of a certain station in the communication, and then at least update it whenever there is a pseudonym change. It might also make sense to extend the protocol with a sender-driven update announcement that informs all potential recipients about changes of its trust-related properties and data. Such an approach would lead to a kind of 'stateful system', at least at the receiver end, but this would have several drawbacks as well (e.g. more storage needed, management of the states, timeouts, etc.).

Another related approach would be to standardise attribute classes and only send an identifier for the sender's corresponding class. This would lead to a small amount of data to be sent but on the other hand would need a standardised data structure that can be used to expose specific encoded values.

A further approach to avoid sending big amounts of metadata is to evaluate and certify the trustworthiness – at least for the properties not subject to frequent changes – in the homologation phase of a vehicle. In this case, the homologation service provider could check all relevant properties and map the result of this evaluation against a certain degree of trustworthiness. The achieved trustworthiness level would then be tied to a certificate issued by the homologation service provider, and that certificate would be used in the communication to mutually inform the participants about trustworthiness. The advantage here is that functional safety-related properties could be taken into account as well. The homologation process would actually verify if all measures needed for a certain ASIL level are fulfilled and could confirm it by issuing a certificate. Such an approach would need an agreed common governance context involving many stakeholders (see Chapter 5.2.6), which would require both commercial and political willingness to implement.

These approaches could of course be combined by treating, for example, the static part of the trustworthiness properties in a certification-based setup while still sending the dynamic parts of data (either classified or as pure data) to complement the information.

The following table summarises the advantages and disadvantages for the different approaches discussed.

Approach	Advantages	Disadvantages	Comment
Sending evidence data only when necessary	• Reduced communication payload	• May limit function implementation due to lack of information at critical moments	
Sending harmonised attribute classes	• Reduced communication payload • Lower processing load at receiver side	• Classes standardisation required	
Use homologation and certificates	• Higher control of 'certified' trustworthiness	• Complex ecosystem involving several stakeholder and political decisions	

Table 10 – Comparison of different data exchange approaches

5.2.5 Trust validity contexts

Trust is strongly related to the context in which it is defined. In terms of sensor information it is related to the ODD of the sensor and thus cannot be taken as universally granted. It is important to know and take into account the context in which certain data are valid. Potential contexts are:

- The function to be performed based on the data (e.g. the trust in data generated for a longitudinal control function might need to be higher than for lower functions)
- The ODD of the sensors (e.g. trust in camera sensors might be high at daytime but lower during the night or in a foggy environment)
- The device that generated and sent the data (e.g. the same data sent by a homologated vehicle might be trusted more than if the sending device is a prototype)
- The owner or manufacturer of the device that sent the data (e.g. trust might be different depending on whether the owner of the sending device is known and trusted or if it is unknown)

This list is only meant to give some examples and is not exhaustive.

As the trust depends on the context, it is important to know the data validity context before it can be decided to use the data in a certain safety-relevant function. The information about the trust validity context could be provided together with other metadata by the sender. However, it is not clear how such context information can be generated, parameterised, and interpreted. In addition, it might not be easy to map a certain arbitrarily defined context on the sender side to the intended use by the receiver (e.g. even if the sender provides information about the function it uses its own data for, this function might be different from the one intended to be performed on the receiver side, and a direct decision if the data can be trusted from a safety point of view is therefore difficult). Furthermore, the context might differ a lot for different setups (in a vehicle the context might be completely different than for infrastructure-related systems). Therefore, it would be reasonable to generate a 'context catalogue' agreed among the relevant stakeholders (OEMs, infrastructure operators, homologation service providers, regulators, etc.), and to map the data trust to a catalogue entry and thus provide information on each of these contextual elements. This would need activities on the standardisation side to agree upon the catalogue and have it certified for widespread use.

5.2.6 Stakeholders and roles

The following image provides an introductory (inexhaustive) overview of potential stakeholders in the context of ASIL for connected functions and their potential role in this context.

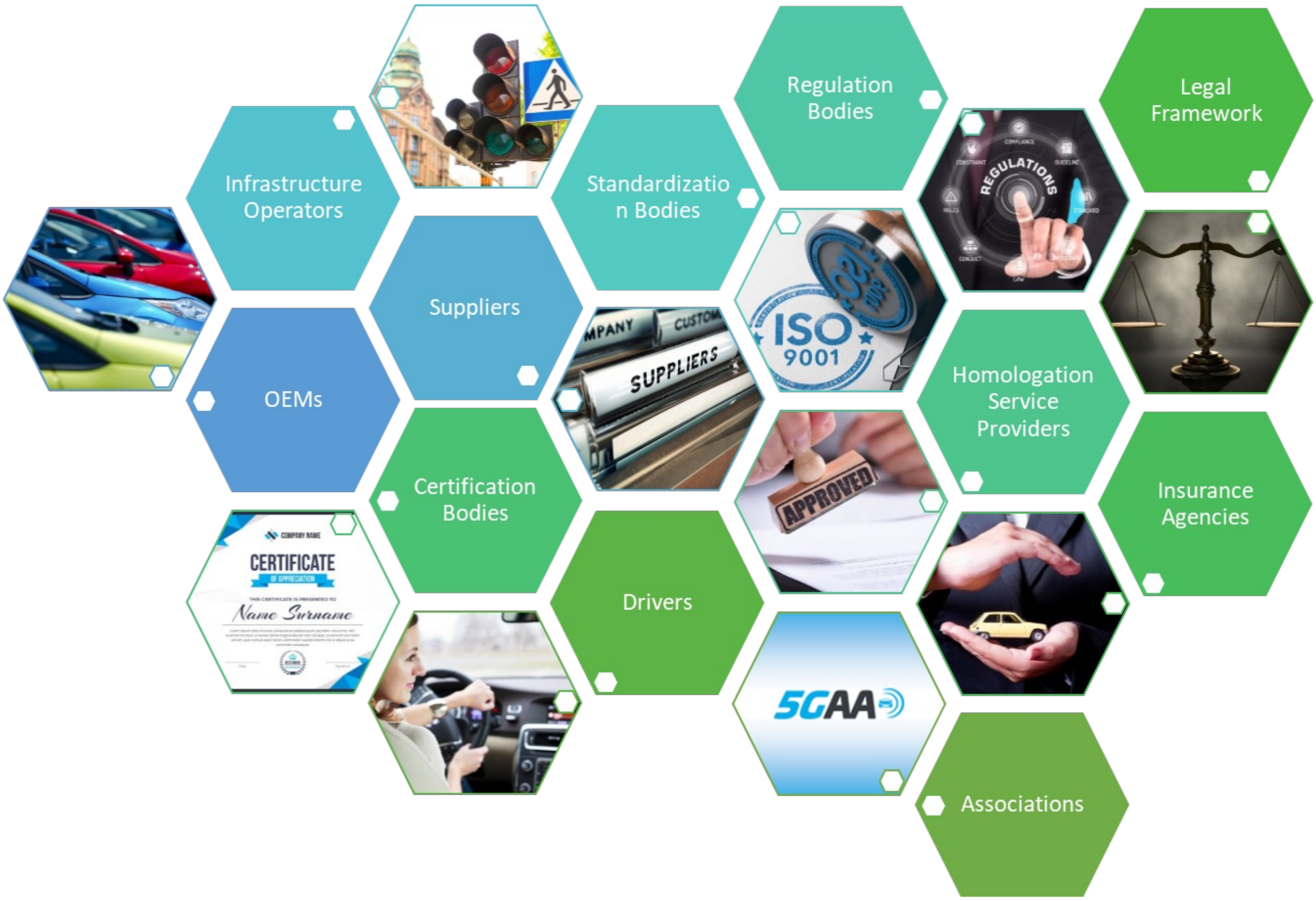


Figure 12 – Stakeholder overview

Stakeholder	Role	Comment
OEMs	Data user Data provider Functional safety responsible Overall system responsible	
Suppliers	Function developer Functional safety manager (Certified) Hardware provider	
Homologation service providers	Homologation provider Certificate issuer Tester	
Drivers	Function user Insurance holder	
Standardisation bodies	Standard developer Standard maintainer	
Insurance agencies	Insurance provider	
Regulation bodies	Certification governance Homologation governance	
Certification bodies	Certification governance operator Certification service provider	
Associations	Support and discuss potential standards and solutions	
Legal framework	Provide legal and governance framework	
Infrastructure operators	Data user Data provider Functional safety manager Overall system manager	

Table 11 – Stakeholders and roles

5.3 Sample application, concept to use case

In order to better illustrate the concepts mentioned in previous chapters and to provide ideas on feasibility, this section uses one of the use cases from Chapter 5.1.1 to apply some of these concepts. It must be noted that there is not just one solution for this. Therefore, the application example provided here should be taken as one possible way to approach the problem of trust and is by far not exclusive.

5.3.1 Use case overview

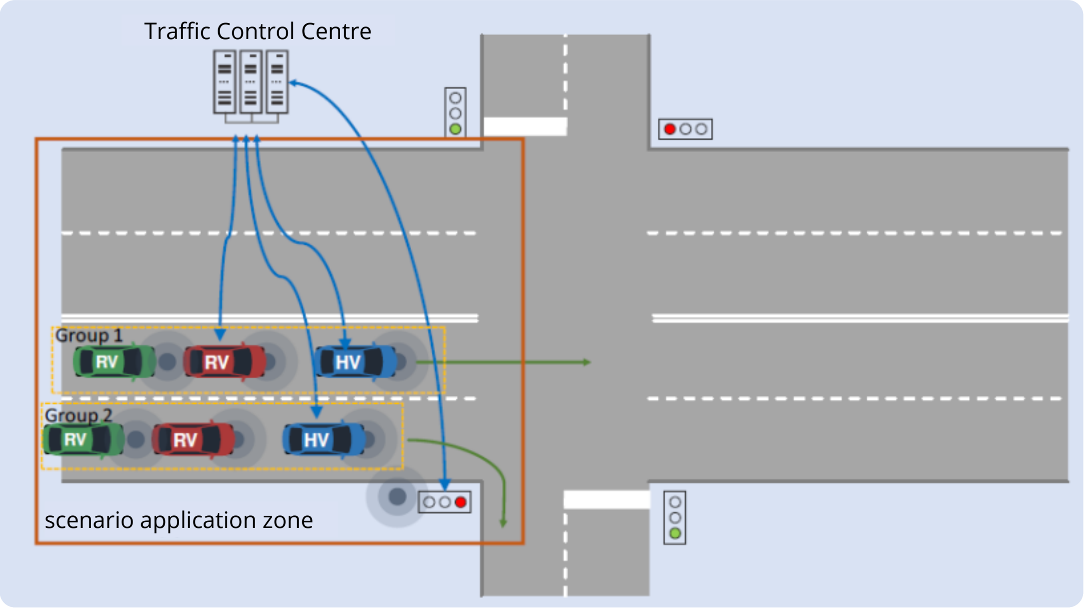
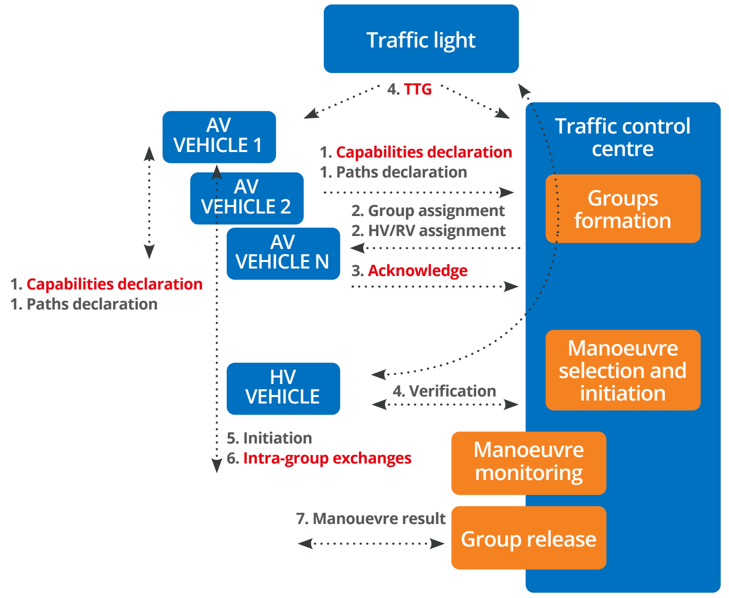


Figure 13 – Group Start schematic@de.bo... - 5GAA - 5G...



Capabilities declaration: Braking, speed, accelerations, sensors, timings...

Path declaration: Direction, path and timing information

TTG: Time to green/to red information

Group assignment: Assignment of AV into homogeneous groups and definition of vehicle role (HV, RV)

Acknowledge: Feedback from AV vehicles and trajectories/ group confirmation

Verification: HV vehicle checks with traffic light and TCC information is correct and group is ready

Initiation: HV vehicle starts the manouevre and communicates to all RVs of its group to start

Intra-group updates: HV and RV exchange information during manoeuvres to signal possible deviations from the agreed plan (pedestrian crossing, delays, etc.) or manoeuvre changes; information is also sent to TCC

Manoeuvre result: HV communicates the positive/negative result to TCC and then releases the group

Figure 14 – Group Start data exchange

The figures provide an overview of the use case and show the different data exchange possibilities. The same conditions and setup as Chapter 5.1.2.2 are considered here. This mainly treats the vehicles as AV vehicles and assumes that those vehicles have some kind of own sensors that might also be involved in the driving task. In addition, we also consider direct data exchange between the vehicles as this includes an additional form of trust to be considered. All details of this use case can be found in [9].

5.3.2 Trust relations

In a first step the different types of entities involved in the use case are checked. Each participant does not have to be checked individually but only those communication partners that are different with respect to their role in the communication and the use case.

The following entities can thus be identified:

- HVs, the vehicles leading other vehicles.
- RVs, the vehicles following the HV.
- Roadside Units (RSUs) like traffic lights with communication capabilities.
- Traffic Control Centre (TCC) which receives/sends information to the involved entities.

After this, the identified entity classes exchanging information need to be taken into account. The following table shows the different combinations possible.

Type	Description	Level of trust	Comment
HV – RV	Direct exchange of information between vehicles, mainly HV information (speed, position, time, acceleration). There might also be an exchange of vehicle capabilities.	If RV bases actuation directly on HV information; a high trust level for all mentioned data is needed (ASIL relevant).	
HV – RSU	Direct exchange of information between RSU (mainly traffic lights) and HV. This mainly includes SPAT and MAP messages.	If HV vehicle bases actuation directly on RSU information; a high trust level for all mentioned data is needed (ASIL relevant).	
HV – TCC	Exchange of information from HV to cloud. This would be the same kind of information as for HV – RV for monitoring as well as control information like driving and manoeuvre or deviations from initial plans.	The vehicle capability data used to assign and set up groups need a high trust level. Data sent from TCC to HV for group formation and verification also need a high trust level (ASIL level). All other data (monitoring) might need a lower level of trust.	
RV – TCC	Exchange of information from RV to cloud. This would be the same kind of information as for HV – RV for monitoring as well as control information like driving and manoeuvre or deviations from initial plans.	The vehicle capability data that are used to assign and setup groups need high trust level. Data sent from TCC to HV for group formation and verification also need high trust level (ASIL level). All other data (monitoring) might need lower level of trust.	
RSU – TCC	Exchange of information between traffic lights and TCC. This mainly includes SPAT and MAP messages.	As this mainly includes monitoring, only a lower level of trust is needed.	

Table 12 – Group Start trust relations

5.3.3 Potential approach

The information exchanged can be grouped into different classes. These classes are formed according to the potential changes that the data might undergo. Some information will be static (e.g. the quality levels, sensor capabilities), other information might be variable but not change frequently or fast (e.g. ODD), while finally some information nay well change frequently or very quickly (e.g. position, speed, time, acceleration). As the frequency of change will have a high influence on potential ways to secure trust, the following classes of exchanged data will be considered.

5.3.3.1 Static data

Some information needed to evaluate trustworthiness is not subject to change and therefore is treated as 'static'. Examples include information to evaluate quality levels already established in the setup of the trustee's system. Typically, that information could be the ASIL level applied in the design of system components (hardware and software) or sensor capabilities. That data does not need to be exchanged frequently and thus can be included in an initial message exchange. As mentioned in Chapter 5.2.4.2, exchanging direct evidence data has several drawbacks leading to a proposal to exchange special certificates generated at the homologation of the vehicle which are issued by the homologation authority. Potentially, there are different certificates needed to distinguish between different applications or sensor types (e.g. there might be an individual certificate for the sensors and each of the involved computation units in generating the data). These certificates would be sent in the capability declaration phase of the function.

5.3.3.2 Slow-changing data

Some data will undergo changes but not change very frequently. One example of this kind of data is information if the sending side is inside its ODD for the sent data. In principle, the sender could also send its ODD and the receiver would evaluate on its own if the ODD conditions are valid, in this case the ODD would fall into the 'static data' class. However, it is proposed to let the sending side evaluate if it is inside its own ODD or not, and thus make sure the conditions at the sender position are factored in. As this kind of information has an event-like character, it is further proposed to send it in a special message (e.g. a special type of DENM or dedicated message type) whenever the state changes (from inside the ODD to outside, and vice versa). For other slow-changing data, the same kind of exchange is proposed.

5.3.3.3 Fast-changing data

Data that changes very fast (happening instantaneously at any time) should be exchanged as 'evidence data' together with the user data themselves. For example, the position should always contain information about the accuracy of the information (already existing in the message protocols as confidence levels). Other information is not yet included in the existing message protocols for CAM or CPM. Examples are results of the monitoring of errors or health states for components involved in the calculation of the data sent inside the messages. Here, we see two possibilities: one would be to simply not send the message whenever an error is detected or when the health state gets into some critical level; another approach would be to transfer this information as ‘evidence values’ in the messages. The latter would allow decisions on how to use the values, e.g. to validate or check own-sensor data even though their trust level is lower. An additional advantage of always sending would be that the receiving side can check if the communication is broken when messages are sent with a known repetition/frequency.

5.3.4 Conclusion

The proposals in this chapter are keeping some potential variants for the used concepts. It is outside the scope of this work to generate a unique proposal for the use case. However, different possibilities for the necessary setup have been shown, and details need to be carried out in standardisation and function implementation based on these proposals. Generally, the responsibility for actions taken is on the side performing the action (mainly the RV vehicles in this case), which should have as much information as needed to make such a decision. It is therefore always preferential to send information as evidence data instead of making decisions on the sending side (e.g. not sending data due to unclear states or requirements on the sending side).

6 Standardisation analysis and proposal

This chapter will discuss for which of the proposed trust considerations mentioned in Chapter 5 standardisation is necessary. It will cover what evidence data needs to be included in the standardisation and which body is the most reasonable one to drive this standardisation. An overview of currently known activities for standardisation related to the topics are also discussed in the chapter.

6.1 Known standardisation and regulation activities in the trust for safety context

Name	Number	Body	Scope	Comment
Road vehicles. Functional safety	26262	ISO	Functional safety for automotive electrical/electronic systems. Including interaction of the systems.	
Functional safety of electrical/electronic/ programmable electronic safety-related systems	61508	IEC	Functional safety for electrical/ electronic/programmable systems	
Road vehicles. safety of the intended functionality	21448	ISO	General argumentation framework and guidance on measures to ensure safety of the intended function of electrical/ electronical systems	
Road vehicles – Cybersecurity engineering	21434	ISO/SAE	Cybersecurity engineering of electrical and electronic systems within road vehicles	
Road vehicles – extended vehicle methodology	20077	ISO	Includes all on-board and off-board data and systems required to perform a vehicles function	
SAE J 3061	3061	SAE	Framework for cybersecurity engineering of connected vehicles and systems	
W3C Vehicle information accessory specification		W3C	Guidelines for accessing and managing vehicle data and privacy controls	
IEEE 1609.2	1609.2	IEEE	Security and privacy in vehicular communication systems	
SAE J 2945/1	2945/1	SAE	Message sets for V2V communication including privacy and security considerations	
ETSI WI functional safety in ETSI TC ITS	TR 103917	ETSI	Work on functional safety topics for use cases, applications and features in ETSI TC ITS	
UN ECE R 155	R 155	UN ECE	Requirements for risk analysis and cybersecurity management systems	
UN ECE R 79	R 79	UN ECE	In particular relevant for homologation of complex electronic vehicle controls systems	
UN ECE R 157	R 157	UN ECE	Automated lane-keeping systems	

Name	Number	Body	Scope	Comment
SAE J 3016	3016	SAE	Definitions and taxonomy for on-road motor vehicles' automated driving systems	
Road vehicles – Safety and artificial intelligence	PAS8800	ISO	Safety requirements for AI systems	
Safety for automated driving systems – design verification and validation	TS 5083	ISO	Application specific standard for automated driving systems SAE L3 and L4	
NHTSA Cybersecurity best practices		NHTSA	Set of best practices for cybersecurity in motor vehicles	

Table 13 – Standardisation bodies

6.2 Data to be standardised and proposed standardisation bodies

According to the information provided in Chapter 5.2, some information and concepts should be taken into account in standardisation. The table below lists these and proposes the potential standardisation bodies that might work on this.

Topic	Change	Description	Data type	Standardisation Body proposed	Comment
Static data to identify trust in	Static	Information on how the data generating subsystem was designed, developed, implemented, maintained, and operated	Certificates provided in the homologation phase	ISO	Beyond the standardisation there will also be a need to influence the regulation and homologation bodies
Static data on intended use	Static	Information on how the sending entity is using the data it sends	Standardised data packages Could be related to defined use cases (e.g. from ETSI ITS)	ISO ETSI SAE	
Static ASIL Level information	Static	As ASIL levels are bound to functions, it might be useful to get the ASIL levels for the information provided in the line before (intended use)	Standardised data packages, according to the rules of ISO26262	ISO ETSI SAE	
ODD Validity	Slow Dynamic	Information about if the sending device is inside the ODD of the sensors and computation parts involved in generating the data	Standardised data packages Could be either one binary value generated by the sender or several values (distinguishing e.g. sensors and ECUs involved)	ISO ETSI SAE	
ODD values	Slow Dynamic	Information defining the ODD of the sensors and computation parts involved in generating the data	Standardised data packages The data would contain certain ODD properties that are necessary for the ODD validation and for each property a threshold	ISO ETSI SAE	

Topic	Change	Description	Data type	Standardisation Body proposed	Comment
Data completeness indicator	Fast Dynamic	Information on whether the data sent is having a complete view or if there are blind spots where the status is unknown	Standardised data packages There are some examples already existing e.g. free space information sent in CPMs	ISO ETSI SAE	
Internal states of state machines	Fast Dynamic	Information about states inside the state machines on the sending side	Unknown	Unknown	This needs to be further evaluated; it is simple to find data formats that could transport the states, but complex to transport the information about the state machine itself (which would be needed to understand the states)

Table 14 – Proposed standardisation bodies for different data classes

A potential next step for progressing on standardisation would be to initiate discussions with some standardisation groups based on the information presented in this document; a good starting point for this would be ISO 26262 and ISO 21448 groups. Another good candidate would be ETSI ITS TR 103 917, where a dedicated working group already discusses the safety aspects of ITS data exchange based on V2X. This would trigger discussions on standardisation and 5GAA would then gain insight into what is happening outside the Association. Based on such an initial exchange, dedicated standardisation activities in the respective bodies might be triggered/ fostered.

6.3 Conclusion

This chapter has shown standardisation bodies and activities related to the kind of mutual trust needed between a trustee and a trustor. Those bodies are potential candidates to do the standardisation work to achieve that.

7 Summary

This Technical Report examined questions not yet answered in the context of functional safety for connected vehicular functions. A detailed methodology was provided for analysing safety needs affecting V2X functions. A so-called 'Quick HARA' approach was offered as a simplified Hazard Analysis and Risk Assessment (HARA) analysis to achieve a first and rough estimation of the ASIL level of 5GAA use cases. That methodology is based on [1]-3 Concept phase, clauses 5 and 6 covering the Item Definition and HARA, respectively. This methodology was then applied to the use case of automated valet parking (AVP) to prove that it provides reasonable results, as AVP has undergone a detailed HARA in earlier projects, which provides a kind of 'ground truth'.

In the next step, 5GAA offered definitions or its perspective on how trust should be considered as part of the overall 'trustworthiness' work done in [10]. This document concentrated on 'mutual trust' in the context of received V2X data and from the point of view of the functional safety and safety of the intended function, as defined in Chapter 5.2.2. After this, potential data that could be used to derive 'trust evidence' was identified. This was done by analysing different use cases with respect to wrong or inadequate data that could cause severe functional/operational problems. The chosen functions were:

- Automated Valet Parking (AVP)
- Group Start
- Coordinated Cooperative Driving Manoeuvres
- See-through for Passing

For each of the functions it was identified which data received by a (foreign) sender was critical for functional safety. This led a data subset further considered in the analysis of potential ways to exchange information needed for trust evidence in the 5GAA context.

Next, it was discussed which information can be used to classify data, on what basis the data can be classified – as exchanging an exhaustive set of information might not be reasonable – and several possible contexts in which the data is valid (per function, per device, etc.) were developed. A list of stakeholders and roles involved in the overall ecosystem of functional, safe, connected functions was also provided. Finally, a use case (Group Start) was applied as an example of how data relevant to mutual trust in this automated driving context can be exchanged.

As many of the identified data exchanges are likely to be standardised, the final chapter explored standardisation bodies that might reasonably work on standards for the different identified data classes (static, slow dynamic, fast dynamic).

It should be made clear that this document only touches on what is essential a very complex task – making connected functions reliable, trustworthy, and above all safe. However, the discussions and proposals presented in the report will hopefully serve as a valuable starting point in the work that needs to be carried out before such functions might be brought into series-production vehicle development.

Annex A: Change history

Date	Meeting	TDoc	Subject/Comment
2023-01-11			First issue. Description of methodology. Missing part related to application to use cases.
2023-01-19			Accepted review comments. Added example of application of methodology.
2023-01-25			Minor updates after review comments.

5GAA
Automotive Association