Safety Treatment in V2X Applications Phase 2

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

Contents

Contents

1. Introduction

The first 5GAA work item on Safety Treatment in Connected and Automated Driving (STiCAD) functions generated guidelines for telecommunication operators, vendors, and other identified stakeholders to enable car OEMs treating safety for the new use cases based on V2X technologies.

This follow-up edition, STiCAD II work item, targets some of the open points not addressed in STiCAD I. The work analyses several use cases that need safety treatment through a simplified approach, focuses on the definition and study of the concept of mutual trust – an essential element for deploying V2X use cases – and provides considerations on potential standardisation inputs from 5GAA to safety-related activities in different standardisation bodies.

2. References

[1]	ISO 26262 'Road Vehicles – Functional Safety – Part 3: Concept Phase', Second edition 2018-12
[2]	5GAA TR T-21009 Safety Treatment in Connected and Automated Driving Functions, Version 1.0, 2021-3-9
[3]	5GAA TR C-V2X Use Cases and Service Level Requirements, Vol. I (6.3.2)
[4]	5GAA TR C-V2X Use Cases and Service Level Requirements Vol. II (5.2.1, 5.4.5, 5.6.4)
[5]	5GAA White Paper, Creating Trust in Connected and Automated Vehicles
[6]	5GAA TR Trustable Position Metrics for V2X Applications

3. Abbreviations

ACC	Automatic Cruise Control
ASIL	Automotive Safety Integrity Level
AVP	Automated Valet Parking
CAM	Cooperative Awareness Message
CPM	Collective Perception Method
DENM	Decentralised Environmental Notification Message
EBW	Emergency Brake Warning
FuSa	Functional Safety
ODD	Operational Design Domain
SLR	Service Level Requirement
SOTIF	Safety Of The Intended Function

4. Problem statement

As more and more driver assistance functions, especially in the framework of automated driving, are using connectivity, some of these functions require safety treatment because failures might cause severe danger to people and thus the probability of residual errors must be kept below a reasonably small value.

Vehicle-to-everything (V2X) systems consist of subsystems that are often independently developed by different parties; when a receiving side wants to use remote information in actions requiring functional safety treatment (e.g. an emergency braking using V2X messages), it is essential that such information can be trusted. The sending side should thus follow appropriate rules in the information-creation process.

These trust requirements have not been thoroughly investigated yet, nor have a set of defined or standardised approaches to sharing and incorporating such 'trust evidence' in V2X functions been elaborated. This document offers potential approaches to tackle this matter.

5. Profile details: ITS messages

P The STiCAD I work item provided an extensive functional safety analysis on Automated Valet Parking (AVP) and Emergency Brake Warning (EBW) use cases following the ISO 26262 standard, confirming that functional safety treatment is necessary to implement those distributed functions.

To prepare the ground for STiCAD II, additional use cases were selected to highlight trust requirements through the description of the information flows necessary to implement such functions.

The following use cases were selected because they represent quite different scenarios, stakeholders and complexities (vehicle-to-vehicle/vehicle-to-network (V2V/V2N) communication, infrastructure, cloud, automated/manually conducted vehicles), with the aim of verifying that the suggested approaches and conclusions are reasonably applicable across all 5GAA use cases:

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

As a first step, a simplified approach to functional safety analysis was defined, useful to derive preliminary safety considerations on V2X distributed functions without running the detailed and exhaustive analysis expected in current standards.

Subsequently, for each use case the involved architecture or elements (e.g. cloud, vehicle) and the data exchanged between them were described, identifying the main potential error sources and related consequences.

This approach helps to identify which data need to be considered for the trust analysis and which entities or items are needed to establish mutual trust.

In general, 5GAA use cases defined by Working Group 1 (WG1) are based on assumptions that require trust among involved entities. Some examples are highlighted in bold:

- 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 **requires high-level accuracy** within the required range, as described in the use case descriptions and Service Level Requirements (SLR), of +-1.5m across open sky.
- **Communication partners are equipped with suitable software and hardware** (e.g. compatible wireless communication technologies) for the use cases.

As an example, Figure 1 shows the Group Start use case information exchange flow between the involved entities; trust-impacted information is highlighted in red.

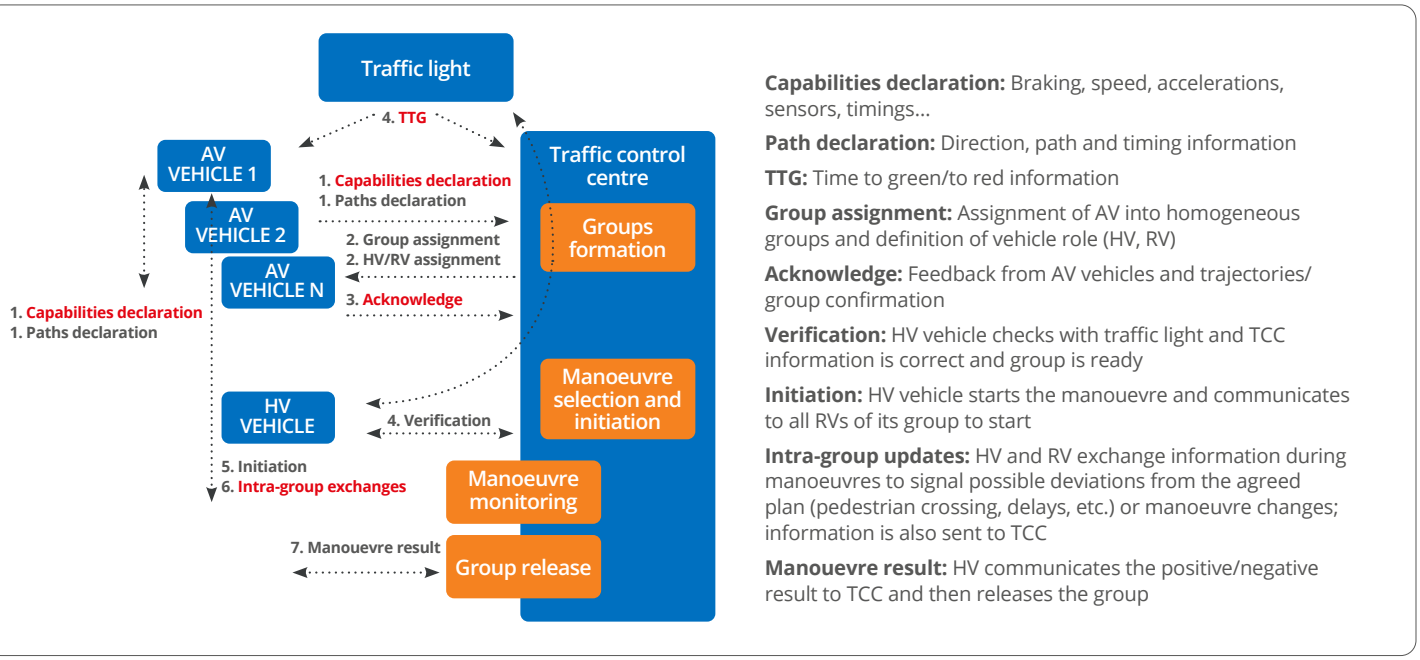

Figure 1 – Group Start data exchange

Following the described approach, it is therefore possible to quickly spot the impact of potential errors, such as *wrong or inconsistent declared vehicle capabilities* (leading, for example, to wrong group formations, where some vehicles are unable to follow the target manoeuvre), *incorrect traffic light information* (leading to wrong vehicle starting decisions, with evident safety impact), or *incorrect timing or position* (leading to wrong trajectories or even collisions).

All such sources of potential errors must therefore be taken into account in the trust analysis; this approach becomes the basis for the considerations and proposals elaborated in the following paragraphs.

6. Trust model concept

6.1. Definition of mutual trust

Trust is not a mono-dimensional property; there are different properties that can be evaluated and for each use case only a subset may be relevant. Each property in turn is related to an 'evidence item' that can be used, for example, to calculate trustworthiness or to serve as basic parameters for Key Performance Indicators (KPIs). Data such as mean value, standard deviation, and 95th percentile can function as evidence-based KPIs related to accuracy or properties related it. The following figure provides quite an exhaustive set of known properties derived in [5] and illustrates different possible viewpoints for different use cases (e.g. not all use cases need to be mindful of data transparency or consider privacy or functional safety). In general, a certain use case will use a subset of the properties of trustworthiness (maybe weighted with different importance factors) to perform an overall trustworthiness assessment of the data received from a certain trustee.

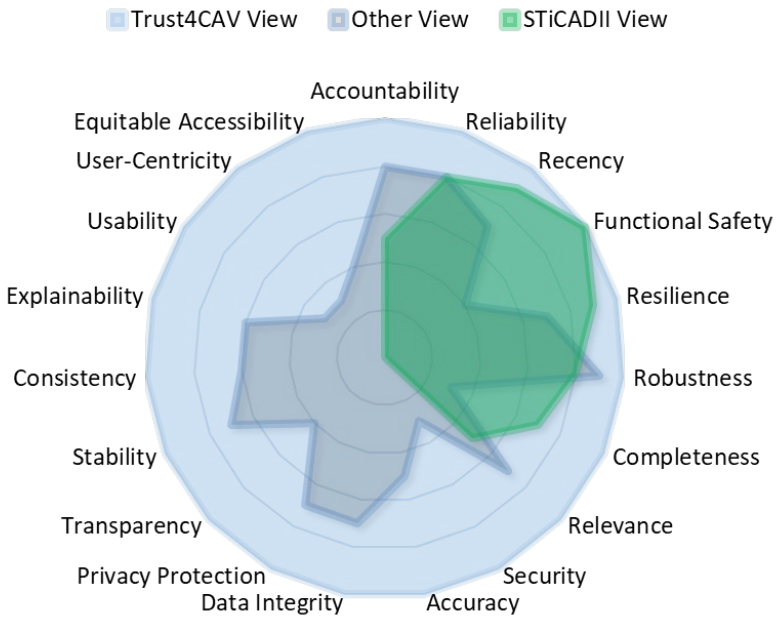

Figure 2 – Trustworthiness properties

In the remainder of this document 'trustworthiness' refers to the subset of properties needed to assess data usability in a functional safety context. This especially implies knowledge of the intended use of data, the required data quality and accuracy, and how the subsystem generating data was designed, developed, implemented, maintained, and operated.

6.2. Data required for trust assessment

It is difficult to define a comprehensive set of 'evidence items' for a general trustworthiness assessment, so it is advisable to narrow it down to those related to the trustworthiness property under evaluation. This document concentrates on evidence items needed to assess trustworthiness in a functional safety context as well as those where a detailed assessment has yet to be fully completed (e.g. [6] has evaluated position accuracy and thus this point does not need to be tackled here). Examples of such evidence items are sensor capabilities, Operational Design Domain (ODD), automation level, intended use of providers' own data, 'state machine' information.

6.2.1. Sensor capabilities

The data being considered are mainly generated by different types of sensors (RADAR, cameras, LIDAR, GNSS, etc.). To allow the trustor side deciding whether to use those sensor data for a relevant Automotive Safety Integrity Level (ASIL) function, it is necessary to have some knowledge about the trustee sensor capabilities. The receiving side not only has to interpret the data received from a certain sensor, but it also needs to understand its possible limitations (e.g. sensor type, sensor position).

A simple example can illustrate the importance of this additional information. Assume that the sender is equipped with a sensor for an Automatic Cruise Control (ACC) function; in this case the sensor will be installed and optimised to detect objects and their speeds in the longitudinal direction, as other characteristics like an object's transversal speed are less important. In this example, the receiver wants to use the sensor information for a different function such as lane-keeping. Here, the sensor blind spots that are tolerable or unimportant for the ACC function might be unacceptable for the lane-keeping function, and the lack of knowledge of this sensor characteristic makes data less trustworthy or even unusable. However, if the receiver is informed of the blind spots, it could decide to what extent those datasets are usable or if they need to be complemented with additional information.

Since data-sharing requirements might generate excessive data rates it seems reasonable to distinguish between static and dynamic data, and to transfer static data less frequently or define standardised sensor classes and only transmit a class identifier (see 6.3 for further details).

6.2.2. ODD

For safety considerations relating to a certain function, it is important to define the ODD, which establishes conditions and constraints under which the considered function is intended to work in a safe manner.

A receiver willing to use data from a sender in an ASIL-relevant function needs to know the ODD of the sender so that it can blend it with its own ODD. An ODD can also be exhaustive (see [2]) and faces the same type of problems discussed for sensor capabilities; thus, also similar solution approaches could be used. In addition, if the sender and the receiver are very far apart from each other, the conditions they are experiencing (like weather or road status) might be quite different, and so the sender would also need to provide them.

In another possible approach, the sender could send only the data falling inside its own ODD and inform the receiver otherwise. This approach is convenient when receiver and sender ODDs are identical or similar – and of course under the assumption that ODD definitions are aligned.

6.2.3. Other information

A lot of other information can be used by a receiver as evidence to assess the trustworthiness of received data with respect to functional safety. The volume of information is huge and cannot be exhaustively discussed here, but it is worth elaborating on two specific concepts.

The **first** is **data completeness**. There is a big difference between *lacking information* on a certain area or aspect relevant for an automotive function and *knowing* that the area is free from other objects. Therefore, data completeness should always receive high priority. The importance of informing the receiver that the sender sensor has a blind spot was stressed in 6.2.1.

The **second** concept to consider here is the intended use of data. It is very important to communicate to a receiver how data should be used by the sender (e.g. if the sender would perform active driving operations based on its own data). Knowing that certain applications imply strict quality and severity measures on the sender side, the receiver can assign higher trustworthiness to the received data when such information is available.

6.3. Data grouping

Looking at the data flows of 5GAA use cases (see for example the Group Start diagram in Figure 1), the exchanged information can be grouped into different classes based on the potential changes that data can experience.

6.3.1. Static data

Some information needed to evaluate trustworthiness is not subject to change and therefore is considered as static. Examples are information to evaluate the quality levels classified in the trustee's system, such as the ASIL level applied in the design of system components (hardware and software) or sensor capabilities, as in the Group Start use case.

Such data does not need to be exchanged frequently and thus can be included in an initial message. Here, the concept of exchanging special certification information generated during vehicle homologation and issued by the homologation authority is proposed. Potentially, different certificates may be needed to distinguish between different applications or sensor types (e.g. there might be an individual certificate for the sensors and each of the computation units involved in data generation). These certificates would be sent in the capability declaration phase of the function.

6.3.2. Slow-changing data

In some cases data may change or need to be changed infrequently, such as information sent from inside the sender ODD. In principle, the sender could also send its ODD and the receiver could evaluate on its own if those ODD conditions are met; in this case the ODD would be considered static data.

However, it is proposed that the sender evaluates whether it is inside its own ODD in order to ensure that the conditions on the sender side are properly considered. As this kind of information is event-based, a special message (e.g. a special type of Decentralised Environmental Notification Message, DENM, or a special dedicated message type) is proposed 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.

6.3.3. Fast-changing data

This describes data that change very quickly and at any time could be exchanged as 'evidence data' together with the user data themselves. In Group Start, for example, the position should always contain information about its accuracy (as already existing in the message protocols as confidence levels). There is other information not yet included in the existing message protocols for Cooperative Awareness Message (CAM) or Collective Perception Method (CPM), such as error monitoring results or the health states of the components involved in the calculation of the data sent inside of the messages. For this case there are two possible options. One would be to simply avoid sending the message whenever an error is detected or when the health state reaches some critical level. Another approach would be to transfer this information as 'evidence values' in the messages. This would allow the receiver to make informed decisions as to how much trust to place in the values, whether to perform important functions (e.g. validate or check own-sensor data) when the received trust level might be low. An additional advantage of always sending data is that the receiver can check if the communication is broken when messages are sent with a known repetition frequency, and data completeness is also improved.

6.4. Data and trust validity contexts

Trust, as defined here, is strongly related to the context in which information is generated. Trusting sensor information is thus related to the sensor ODD and cannot be taken as universally applicable. It is important to know and consider the context in which certain data are valid. Several potential contexts include (non-exhaustive):

- The function to be performed based on the data (e.g. trust in data generated for the purpose of longitudinal control might be suitable for that function but insufficient for others).
- The ODD of the sensors (e.g. trust in camera sensors might be high during the day but might be low at night or in foggy conditions).
- The device that generated and sent the data (e.g. the same dataset sent by a homologated vehicle might be trusted more than the one sent by a prototype device).

- The owner or manufacturer of the device that sent the data (e.g. trust might be different depending on whether the sending device owner is known and trusted or if it is unknown).

As trust is context dependent, it is important to know the data validity context before deciding to use such 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 should 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 on the function using its own data, that function might be different from the one intended to be performed by the receiver and a direct decision if those data can be trusted from a safety standpoint is therefore difficult).

Furthermore, the context might differ a lot for different setups (in a vehicle the context might be completely different from that applying to infrastructure or other non-vehicle systems). Therefore, it could be reasonable to generate a sort of 'context catalogue' agreed among the relevant stakeholders (OEMs, infrastructure operators, homologation service providers, regulators, etc.), to map the data trustworthiness against each catalogue element with information attached to each entry indicating the actual context. This would need standardisation activities to agree upon the catalogue and standardise it.

6.5. Data qualification – possible approaches

It appears unrealistic to assume that all 'evidence items' can be transferred together with sensor information. There are different reasons why this is unlikely:

- Excessive data volumes (a complex ODD definition might extend the pure sensor data by orders of magnitude).
- Privacy and security issues (very complex metadata and uses, e.g. to derive the identity and intentions of a sending vehicle, which could be a potential security weakness or prone to attacks).
- Liability issues (a sender may not want to assume liability for metadata).
- Industrial secrets (sending information about 'state machines' implemented on the sending side would provide the receiver with deep knowledge that is not intended to be shared).

Therefore, it is advisable to consider transporting certain data from the sender to the receiver without explicitly sending sensitive information. However, for some information it may make sense to add metadata to user data. Some options on how this problem might be overcome are discussed in the following passages.

A major issue is the limitation of sending large amounts of evidence-related data due to the available channel capacity; and the receiver may not be capable of processing such vast amounts of data under strict time constraints, especially for functions needing high update rates with very low latency.

A possible solution could be sending at least the data not subject to frequent changes in a type of initialisation/update phase, and storing the resulting evaluation (which could be a 'trustworthiness class' or value or the pure property of sent data) in a database or repository at the receiver side and, later, map it against the user data in order to judge if such data can be trusted or not.

Implementation would depend on the protocols used. In a V2X scenario, for example, it would make sense to couple this mutual exchange and update of evidence data at the first appearance of a certain communication participant, 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 informing all potential recipients about changes to its trust-related properties and data. Such an approach would lead to a kind of 'stateful system' at least on the receiver side – but this may come with some drawbacks (more storage needed, management of the states, timeouts, etc.).

Another related approach could be to standardise 'attribute classes' and only send an identifier of the sender's corresponding class. This would limit data transmission but need a standardised data structure to expose specific encoded values.

A further approach could be to completely omit sending large amounts of metadata and instead evaluate and certify the trustworthiness – at least for the properties that are 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 assign a certain trustworthiness level based on the evaluation results. The achieved trust level would then be tied to certification information issued by the homologation service provider, and the certificate would be used in the communication to mutually inform the participants in the exchange. The benefit of this approach is that functional safety-related properties would be concurrently available with data. The homologation process would verify if all the measures needed for a certain ASIL are fulfilled and could confirm it by issuing certification information. However, this approach would need an agreed common governance context which would involve many stakeholders and require commercial and political willingness to implement.

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

6.6. Final considerations

The proposals and concepts elaborated in this chapter leave room for potential variants. It is beyond the scope of this work to delve into the machinations for each case. Details will need to be provided in standardisation and functional implementation, starting from the proposals in this document.

In general, it is worth underlining that the responsibility for implemented actions stays as close as possible to the side performing the action (i.e. mainly the Remote Vehicles in the Group Start use case). They should receive as much information as needed to make suitable decisions. It is therefore always preferred to send information as 'evidence data' instead of leaving the sender to ultimately decide whether to send or not (e.g. no data transmission due to unclear states or requirements).

7. Standardisation

Several standardisation bodies are relevant in the context of this document and some of them are already carrying out related activities. The closest standards to the context of this White Paper are ISO 26262 for Functional Safety, ISO 21448 for Safety Of The Intended Functionality (SOFTIF), IEC 61508 for Safety Considerations Outside the Vehicular Domain as well as the standardisation activities of ETSI ITS and corresponding SAE bodies.

A potential next step could be to initiate discussions with some standardisation groups based on the information presented here, and clear candidates would be the ISO 26262 and ISO 21448 groups. Another good option would be ETSI ITS TR 103917, where a dedicated Working Group is already discussing safety aspects of ITS data-exchange based on V2X.

8. Conclusions

This White Paper introduces the information flow among the entities involved in four different use cases representing different 5GAA application scenarios and identifying a subset of the exchanged data that is relevant for trust considerations.

The trustworthiness of received V2X data from the standpoint of Functional Safety and SOTIF, and as the basis of a 'mutual trust definition', is discussed in Section 6.1. It offers a brief account of the overall trust work done in [5].

The major takeaways of STiCAD II work can be summarised as follows:

- For a trust analysis of a use case in the context of functional safety a subset of all possible information must be identified. Typical relevant data examples are sensor capabilities, ODD, and the intended use of data.
- Not all necessary data may be transmittable due to excessive size, privacy and security issues, and limitations due to liability or industrial secrets; therefore, dedicated strategies must be put in place to manage such constraints.
- Data validity and trust are context dependent, so it is necessary to add additional information (metadata) to the exchanged data to facilitate proper decisions at the user side.
- Data can be classified based on their frequency of variation during use-case execution; the proposal here is to split data into static, slow-changing and fast-changing, with data and metadata transmission strategies (and related implications) proposed for each category.
- There is an evident need for standardisation to promote and protect the consistent and reliable exchange of functional safety metadata and information.

The considerations and proposals contained in this White Paper and its related TR document offers a solid basis for the standardisation activities necessary to ensure interoperability across the different stakeholders involved in 5GAA use cases. Existing groups working on ISO 26262 and ISO 21448 standards or ETSI ITS TR103917 are likely candidates to take up the challenge of complementing and extending these first proposals covering the complex task of making connected functions safe, and ultimately necessary for the deployment of V2X functions into series-production vehicles.

5GAA bridges the automotive and telecommunication industries in order to address society's connected mobility and road safety needs with applications such as automated driving, ubiquitous access to services and integration into intelligent transportation and traffic management. For more information such as a complete mission statement and a list of members please see https:/5gaa.org


5GAA
Automotive Association