5G Automotive Association; Working Group; Trustable Position Metrics for V2X Applications

5GAA Automotive Association
Technical Report

CONTACT INFORMATION:
Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

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

VERSION:	V18
DATE OF PUBLICATION:	
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	14th of September 2023

Contents

1. Scope

The present document focuses on the issue of trustworthiness in relation to position information exchanged in the context of vehicle-to-everything (V2X) communication. In particular, the document focuses on how much trust the ITS-station can place on the received V2X message containing the positioning information. This problem is particularly important when the positioning information, received through the V2X technology, is meant to be used to influence the driving strategy, hence, in the context of Day-2 application. However, in order to start the analysis this work has been focusing on Day-1 applications to understand the problem in the context of the current standard.

The document, thus provides an overview of the current standards related to positioning, including the integrity of the position and confidence levels, and reviews the definitions and metrics used so far. It then provides an analysis of the gaps in the current/available V2X standard related to the confident use of such positioning information.

2. References

[1] ISO 5725-1:1994(en): Accuracy (trueness and precision) of measurement methods and results; Part 1: General principles and definitions

[2] EN 302 637-2, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service”

[3] EN 302 637-3, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service”

[4] TS 102 894-2, “Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary”

[5] 3GPP TS 38.305, “3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN (Release 17),” v 17.1.0, https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/Specifications/202206_draft_specs_after_RAN_96

[6] CEN-CENELEC - EN 16803, “Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)”

[7] ETSI TS 103 246-5, “Satellite Earth Stations and Systems (SES); GNSS-based location systems; Part 5: Performance Test Specification”

[8] ETSI TS 103 246-4, “Satellite Earth Stations and Systems (SES); GNSS-based location systems; Part 4: Requirements for location data exchange protocols”

[9] ETSI TS 103 246-3, “Satellite Earth Stations and Systems (SES); GNSS-based location systems; Part 3: Performance requirements”

[10] ETSI TS 103 246-2, “Satellite Earth Stations and Systems (SES); GNSS-based location systems; Part 2: Reference Architecture”

[11] ETSI TS 103 246-1, “Satellite Earth Stations and Systems (SES); GNSS-based location systems; Part 1: Functional requirements”

[12] ETSI TR 103 183, “Satellite Earth Stations and Systems (SES); GNSS-based applications and standardisation needs”

[13] 3GPP TS 37.355, “LTE Positioning Protocol (LPP)”

[14] 3GPP TR 38.857, “Study on NR Positioning Enhancements”

[15] IEEE P1952, “Resilient Positioning, Navigation, and Timing User Equipment Working Group”

[16] ETSI EN 102 637-1, “Intelligent Transport Systems (ITS) – Vehicular Communications – Basic Set of Applications”

[17] ETSI EN 102 637-2, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirement Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service”

[18] ETSI EN 102 637-3, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service”

[19] EN 102 894-2, “Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary”

[20] ETSI TS 103 324, “Intelligent Transport Systems (ITS); Cooperative Perception Services (CPS)”; v0.0.33

[21] EN 302 890-2, “Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2”

[22] C2C-CC Basic System Profile, https://www.car-2-car.org/documents/basic-system-profile/

[23] 5GAA TR, “Safety Treatment in Connected and Autonomous Driving Functions – STICAD”; https://5gaa.org/sticad-safety-treatment-in-connected-and-automated-driving-functions/

[24] 5GAA_E-210017_XWI_STiCAD_II_v2, “Safety Treatment in Connected Automated Driving Functions phase II”

[25] 5GAA TR, “System Architecture and Solution Development; High-Accuracy Positioning for C-V2X”; https://5gaa.org/system-architecture-and-solution-development-high-accuracy-positioning-for-c-v2x/

[26] https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:5723:ed-1:v1:en

[27] https://5gaa.org/c-v2x-use-cases-and-service-level-requirements-volume-i/

[28] IEEE, “Standard for Low-Rate Wireless Networks, IEEE Std 802.15.4z- 2020 (Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques)”, 2020

[29] Ref: Microwave Journal Article UWB: Enhancing Positioning, Safety and Security for Connected Vehicles September 14, 2021 Kerry Glover and Bror Peterson, Qorvo, Greensboro, N.C

3. Definitions, symbols and abbreviations

3.1. Basic definitions

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

Positioning State Error:	The absolute value of the difference between a positioning state estimated by the positioning system and truth.
Accuracy:	Closeness of the agreement between the Positioning State estimated by the Positioning System and the truth [1].
A% Accuracy of a Positioning State:	The A-th percentile of the Positioning State Errors under specific test conditions.
Accuracy Estimate:	The Accuracy Estimate of a Positioning State represents the positioning system's estimation of the expected Positioning State Error.
Confidence Level (of the Parameter State)**:**	The probability that the estimated parameter state lies between a specified 'Range' for a specific measurement set – the specified range is the **Confidence Interval.**
Confidence Ellipse:	Defines a confidence area centred around the estimated value of a two-dimensional quantity. A Confidence Ellipse is described via a major axis, minor axis, and the orientation of the major axis relative to a reference direction. A Confidence Level of X % (e.g. 95%) means that the Confidence Interval or Confidence Ellipse would contain the true value of the quantity in a long series of measurements in at least X% of the measurements. [2] to[4]
Positioning Integrity:	A measure of the trust in the accuracy of the position-related data and the ability to provide associated alerts.[5]

4. Problem statement

Today, when V2X messages, which include positioning information, are received by the ITS-station, it is unclear what level of trust the vehicle should attribute to the received content and, as such, whether the information can be exploited in the final application, such as the autonomous driving system. The system's default reaction is to display a warning rather than taking active action, limiting the overall value of that V2X information. It is understood that car OEMs need to have the possibility to assess the information (i.e. its trustworthiness) to decide how to use it in their system architecture and for their application.

Current standards related to V2X include the use of positioning information in e.g. Basic Safety Messages (BSM), Cooperative Awareness Messages (CAM), and Decentralised Environment Notification Messages (DENM). However, currently the confidence and trust a receiving vehicle can attribute to the positioning information in those messages is not sufficiently well specified. Moreover, it is not clear whether existing metrics are sufficient to guarantee the trustworthiness of the information in a cooperative environment, to cover real-life driving scenarios as well as cross-OEM position exchange.

The following diagram depicts the problem:

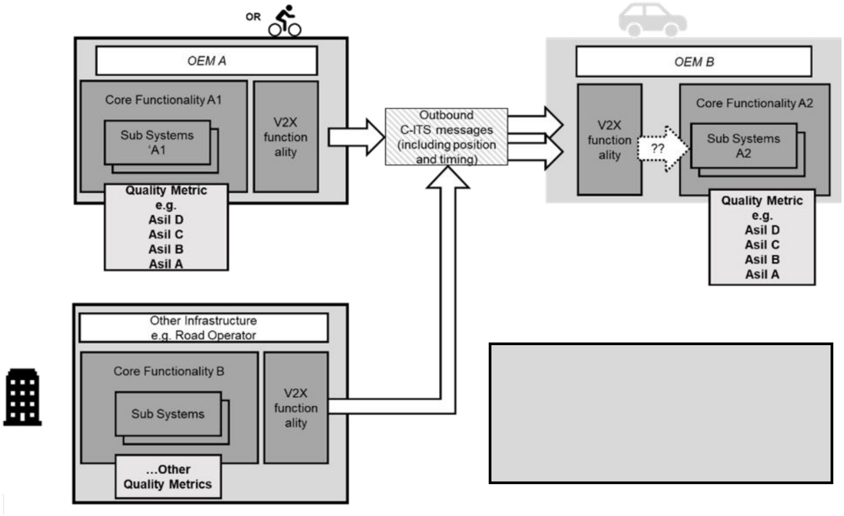


Figure 1. Block diagram representing the problem statement.

This TR provides a survey of existing and on-going standards for position and associated metrics; it defines the terminology needed and used in the document and then analyses the gaps in the current standards while setting the scene for the follow-up work.

5. Literature survey

This section explains the concept of positioning in different V2X standards and associations, and it reviews other standards related to the concept of positioning in the automotive context. In particular CEN CENELEC, ETSI, SAE, ISO, 3GPP and IEEE standards are reviewed below. In addition, the C2C-CC work related to V2X is introduced, together with previous related work in 5GAA. This is not to be considered as an exhaustive description and interested readers are encouraged to consult the formal reference documents for more detail.

5.1. Existing standards

5.1.1. CEN CENELEC 16803 [6]

The CEN CENELEC 16803 standard [6] has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

It addresses the use of GNSS-based positioning for road Intelligent Transport Systems (ITS) and consists of three parts:

- Part 1: Definitions and system engineering procedures for the establishment and assessment of performances
- Part 2: Assessment of basic performances of GNSS-based positioning terminals
- Part 3: Assessment of security performances of GNSS-based positioning terminals

This standard considers two types of road-ITS systems, for which, development may be subject to an official certification/homologation process:

- Safety Critical Systems whose failure may cause human death or injury
- Liability Critical Systems which include financial or regulatory aspects

Such applications include:

- Autonomous driving
- Localised emergency calls (eCall)
- Road management systems, traffic information systems
- Advanced driver assistance systems (ADAS)
- GNSS-based road user charging systems (road, parking zone, urban…)
- Regulated freight transport systems (hazardous substances, livestock, etc.)

The standard proposes a performance management approach to handle positioning-based road-ITS all along the system development, starting with a definition and clear statement of the end-to-end performance expectations and ending with an assessment of actual outcome – how the system performed.

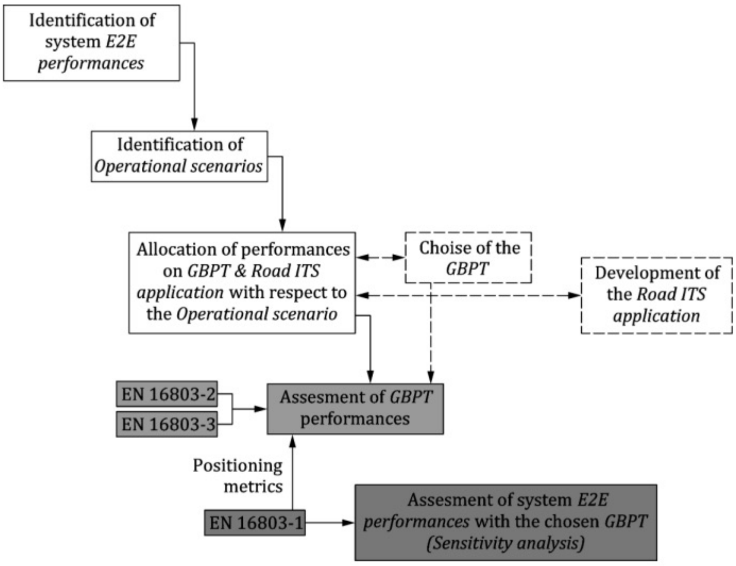


Figure 2. Performance management approach.

In the context of this European standard, a road-ITS system is composed of:

- A GNSS-based positioning terminal (GBPT)
- A road-ITS application

A generic architecture of this system is given in the figure below[6]:

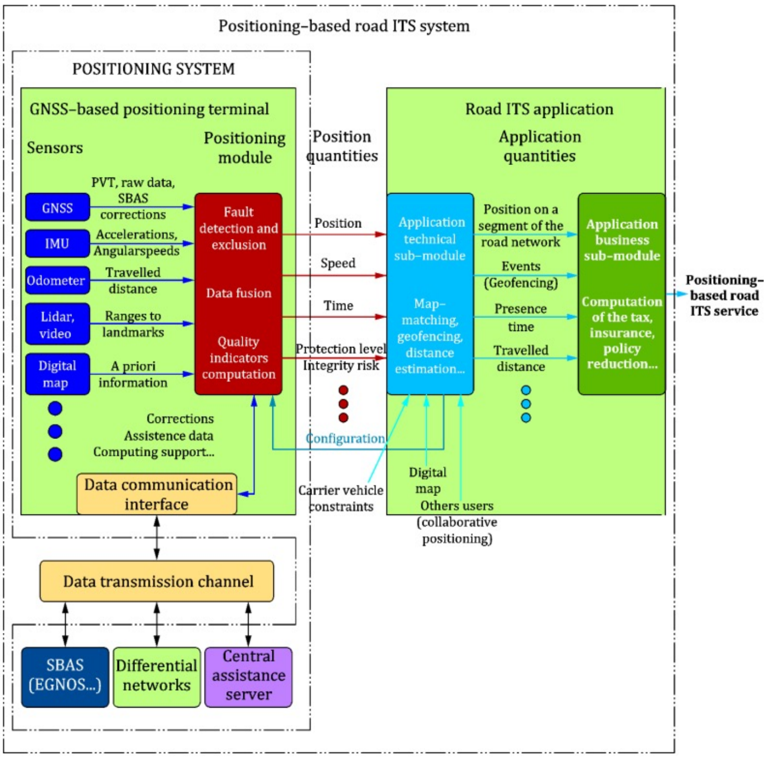


Figure 3. Reference architecture.

The standard provides the following definitions:

- **Outputs of the positioning terminal** are not only position, velocity and time (PVT) together with their components (see Table 1), but also other related parameters that can be of interest to the vast majority of road-ITS applications, such as:
  - **Protection Level (PL)**, which is defined by the value which bounds the error of a given position or velocity component[1] with a given probability, called **Integrity Risk**. According to this standard, the protection level is a real-time and dynamic quantity which may vary from one output epoch to the next.
  - **Integrity Risk (IR)** is the probability that the actual error on a given output component exceeds its associated **Protection Level**. The IR is not to be confused with the Target Integrity Risk (TIR), which is the value not to be exceeded by the integrity risk (as per integrity requirements, which are application-specific). A system which works according to specification should achieve IR values not higher than the TIR. .
- **Inputs to the performance characterisation process** are position, velocity and attitude errors, as well as information related to timing, i.e:

---

[1] Or any other output of interest for which 'error bounding' makes sense, such as for specific headings or trajectories.

  - **Integrity**, which is defined as the trust a user can place in the delivered value of a given position or velocity component. It refers to the characteristics of the Protection Level and its associated **Misleading Information Rate**[2] (MI rate or MIR), in terms of reliability (verification of the risk), but also its efficiency and usability (size of the Protection Level, which is directly related to the intended application).
  - **Time of Output**, is described by the timestamp at which the positioning terminal provides its output. The difference between the parameter and the action timestamp is called the **Output Latency**.
- **Performance Features** are very similar to those identified by the Civil Aviation community regarding Required Navigation Performances (RNP), but with some key differences which reflect the specific needs of road ITS application. Key Performance Features are:
  - Accuracy
  - Integrity
  - Availability
  - Continuity
  - Timing performance
- **Performance Metrics:** those correspond to the metrics used to quantify the different output components, such as:
  - **Protection Level Performance Metric** for a given (e.g. 1e-6) Target Integrity Risk is defined as the (three) statistical values given by the 50th, 75th and 95th percentiles of the cumulative distribution of valid Protection Levels computed for that Target Integrity Risk.
  - **IR and MIR Metrics**:
    - The **Integrity Risk** is the probability that the output's component error exceeds the Protection Level provided that it is flagged as valid.
    - The **Misleading Information Rate** is the empirical rate at which the error exceeds the Protection Level provided that it is flagged as valid.

Table 1. Definition of the output and the corresponding components.

Output	Components
Position	3D, Horizontal, East-West, North-South, Along-Track, Cross-Track, Vertical
Velocity	East-West, North-South, Along-Track, Cross-Track, Vertical
Speed	3D, Horizontal
Attitude	Heading, Pitch, Roll

---

[2] Misleading information rate (MIR) [5]: For positioning terminals providing a Protection Level as an integrity-related quantity, the observed rate at which the actual error on a given output component exceeds its associated Protection Level. The MIR differs from the Integrity Risk (IR) in that it is a purely empirical quantity (e.g. based on observations obtained through field tests), whereas the IR determination also comprises a complete and rational analysis of the system design, its potential weaknesses, threats etc.

5.1.1.1. GNSS environments and threats

The EN 16803 defines six GNSS environment categories:

1. **Flat Rural**, or **Clear Sky**: rural roads in flat countryside with masking angles smaller than 10°, no mountains nor high hills.
2. **Tree-lined Rural**: rural roads with trees and foliage at least on one side, adding a significant attenuation/perturbation to signal reception.
3. **Mountainous**: roads with sharp curves and high mountains around, generally on one side of a valley, with numerous tunnels and sometimes trees, and masking angles between 10° and 80°.
4. **Peri-urban**: suburb or medium-sized city roads and ring roads, with relatively large streets and small- to medium height buildings, and masking angles up to 30°.
5. **Urban**: traditional larger (often older) cities with relatively narrow streets, but sometimes large avenues or ring roads, with buildings from medium height to tall, and masking angles up to 60° –generating frequent multipath and non-line-of-sight (NLOS) phenomena.
6. **Modern Urban Canyon**: business centres with very high modern buildings (constructed mainly with glass and metal), generally large avenues and many tunnels, with masking angles often greater than 60°, and generating frequent NLOS phenomena.

5.1.1.2. Performance assessment approach

A test methodology is proposed in EN 16803-2, called **Record & Replay** (R&R). This lab-based methodology is designed to assess the basic performance features: Availability, Continuity, Accuracy, Integrity and Time-To-First-Fix (TTFF) of the PVT information. In the **Test Scenario**, R&R is able to review and assess the Global Navigation Satellite Systems' (GNSS) signal-in-space (SIS) datasets, and potentially additional sensor and assistance/correction data gathered under specific operational conditions by test vehicle.

Security tests defined in EN 16803-3 are based on the same methodology. They address the assessment of performances when the GNSS SIS is affected by intentional or unintentional radiofrequency (RF) perturbations, such as jamming, spoofing and meaconing (the interception and rebroadcast of navigation signals).

5.1.2. ETSI GNSS specification

The technical specification, ETSI TS 103 246 [7]-[11], produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES), is a multi-part standard covering the GNSS-based location systems:

- Part 1: Functional requirements
- Part 2: Reference architecture

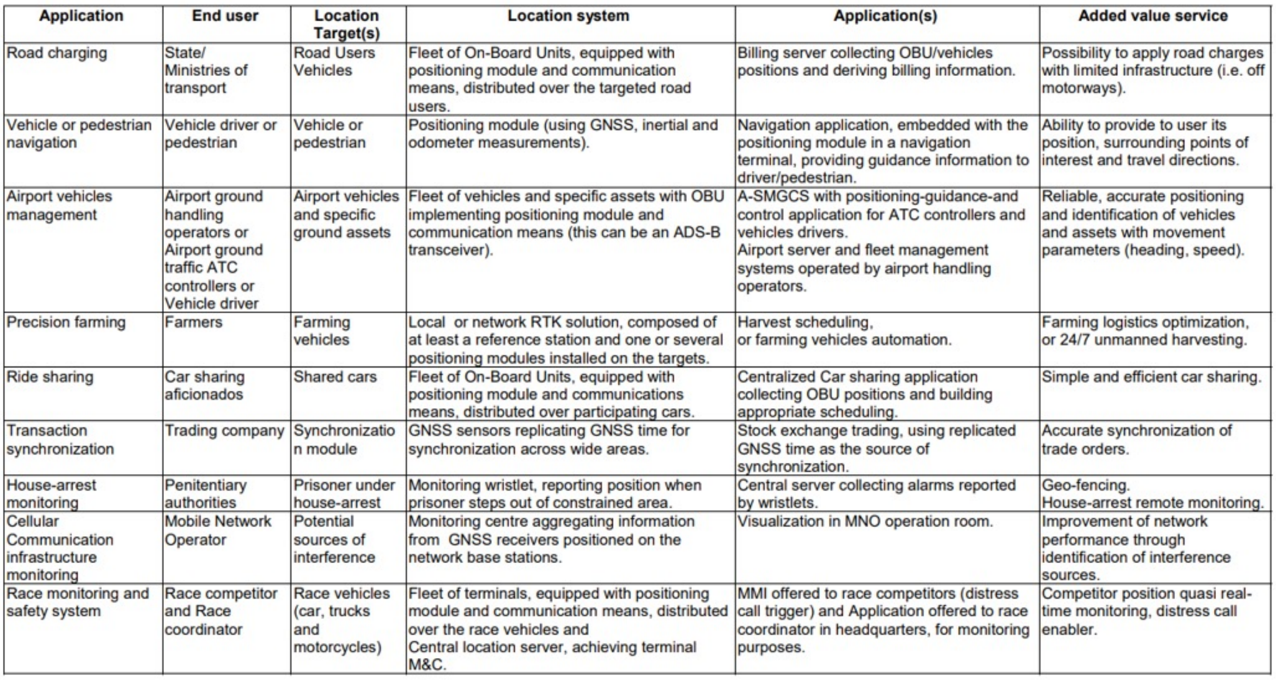
- Part 3: Performance requirements
- Part 4: Requirements for location data exchange protocols
- Part 5: Performance test specification

It addresses integrated GNSS-based location systems (GBLS) that combine GNSS with other navigation technologies, as well as with telecommunication networks in order to deliver location-based services to users. This standard proposes a list of functional and performance requirements and related test procedures. For each performance requirement, different classes are defined to benchmark different GBLS addressing the same applications.

This standard considers several application classes as established in ETSI TR 103 183 [12], such as:

- Location-based charging
- Pay-as-you-drive (PAYD) charging
- Cooperative basic geo-positioning
- Non-cooperative geo-positioning
- Reliable geo-positioning
- (Reliable) Vehicle movement sensing

The figure below describes the different cases of location-based application:



Application	End user	Location Target(s)	Location system	Application(s)	Added value service
Road charging	State/ Ministries of transport	Road Users Vehicles	Fleet of On-Board Units, equipped with positioning module and communication means, distributed over the targeted road users.	Billing server collecting OBU/vehicles positions and deriving billing information.	Possibility to apply road charges with limited infrastructure (i.e. off motorways).
Vehicle or pedestrian navigation	Vehicle driver or pedestrian	Vehicle or pedestrian	Positioning module (using GNSS, inertial and odometer measurements).	Navigation application, embedded with the positioning module in a navigation terminal, providing guidance information to driver/pedestrian.	Ability to provide to user its position, surrounding points of interest and travel directions.
Airport vehicles management	Airport ground handling operators or Airport ground traffic ATC controllers or Vehicle driver	Airport vehicles and specific ground assets	Fleet of vehicles and specific assets with OBU implementing positioning module and communication means (this can be an ADS-B transceiver).	A-SMGCS with positioning-guidance-and control application for ATC controllers and vehicles drivers. Airport server and fleet management systems operated by airport handling operators.	Reliable, accurate positioning and identification of vehicles and assets with movement parameters (heading, speed).
Precision farming	Farmers	Farming vehicles	Local or network RTK solution, composed of at least a reference station and one or several positioning modules installed on the targets.	Harvest scheduling, or farming vehicles automation.	Farming logistics optimization, or 24/7 unmanned harvesting.
Ride sharing	Car sharing aficionados	Shared cars	Fleet of On-Board Units, equipped with positioning module and communications means, distributed over participating cars.	Centralized Car sharing application collecting OBU positions and building appropriate scheduling.	Simple and efficient car sharing.
Transaction synchronization	Trading company	Synchronization module	GNSS sensors replicating GNSS time for synchronization across wide areas.	Stock exchange trading, using replicated GNSS time as the source of synchronization.	Accurate synchronization of trade orders.
House-arrest monitoring	Penitentiary authorities	Prisoner under house-arrest	Monitoring wristlet, reporting position when prisoner steps out of constrained area.	Central server collecting alarms reported by wristlets.	Geo-fencing. House-arrest remote monitoring.
Cellular Communication infrastructure monitoring	Mobile Network Operator	Potential sources of interference	Monitoring centre aggregating information from GNSS receivers positioned on the network base stations.	Visualization in MNO operation room.	Improvement of network performance through identification of interference sources.
Race monitoring and safety system	Race competitor and Race coordinator	Race vehicles (car, trucks and motorcycles)	Fleet of terminals, equipped with positioning module and communication means, distributed over the race vehicles and Central location server, achieving terminal M&C.	MMI offered to race competitors (distress call trigger) and Application offered to race coordinator in headquarters, for monitoring purposes.	Competitor position quasi real-time monitoring, distress call enabler.

Figure 4. Description of the different cases of location-based application [11].

The ETSI standard provides functional requirements applicable to the GBLS. Functional requirements are organised as follows:

- A set of mandatory requirements, which provide the specification any GBLS shall comply with, regardless of the type of application served.
- A set of requirements for optional features, required for some of the targeted application classes.

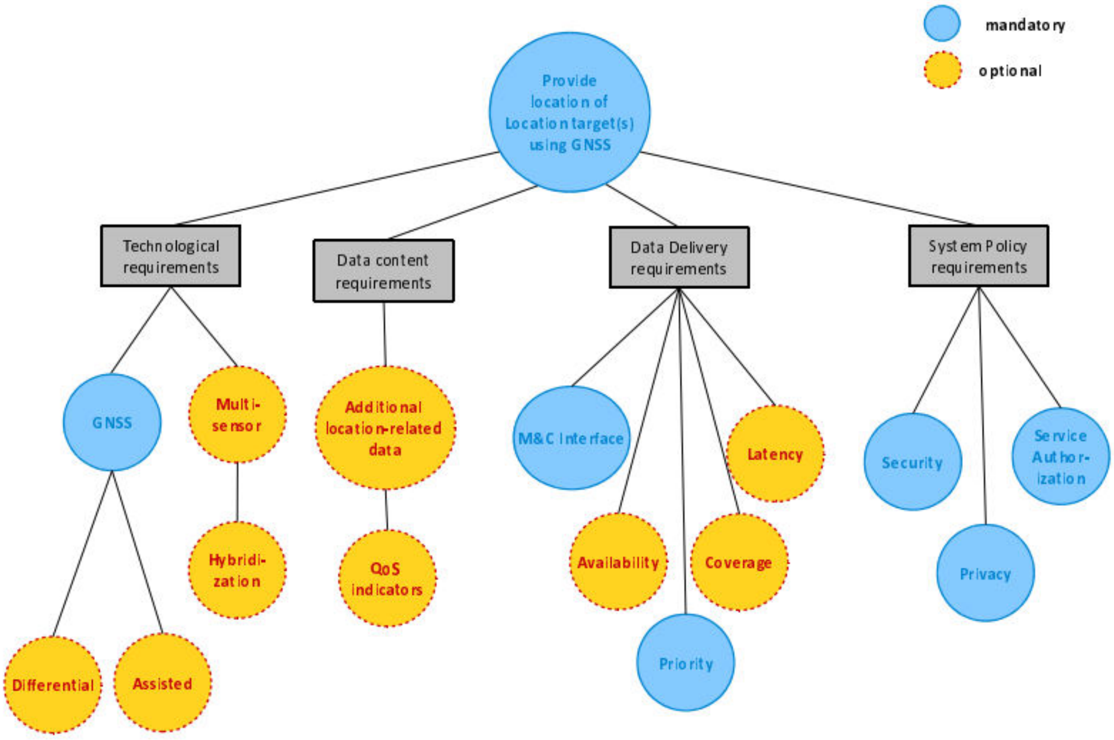


Figure 5. Functional requirements for GNSS-based location systems [10].

Based on those functional requirements, the standard proposes a generic GBLS architecture with mandatory and optional modules. See figure below.

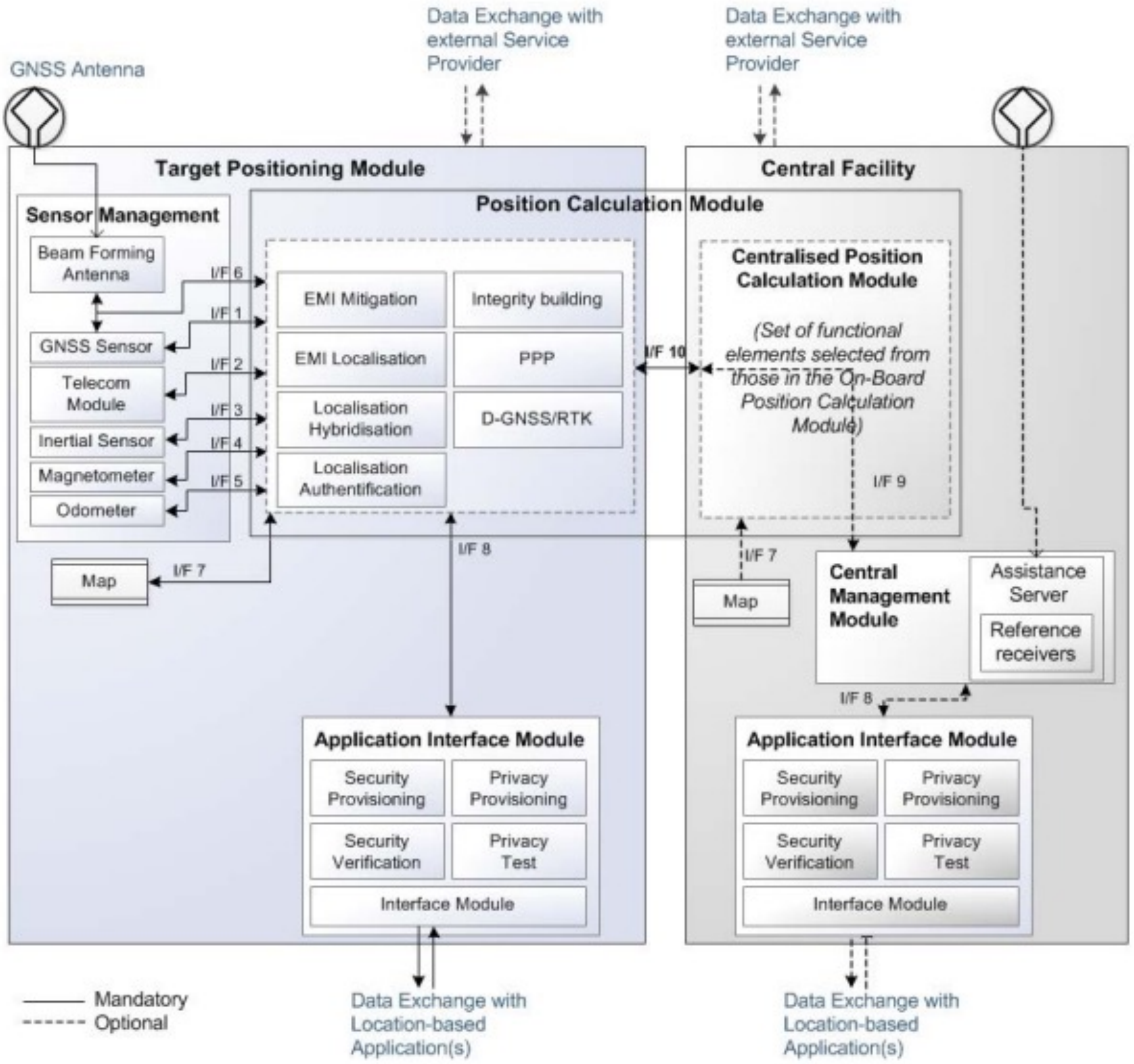


Figure 6. GBLS detailed architecture [10].

Performance requirements to be met by the GBLS, derived from GBLS functional requirements [5] are grouped into categories or performance features:

1. Horizontal Position Accuracy
2. Vertical Position Accuracy
3. GNSS Time Accuracy
4. Time-To-First-Fix
5. Position Authenticity
6. Robustness to Interference
7. GNSS Sensitivity
8. Position Integrity (Protection Level)

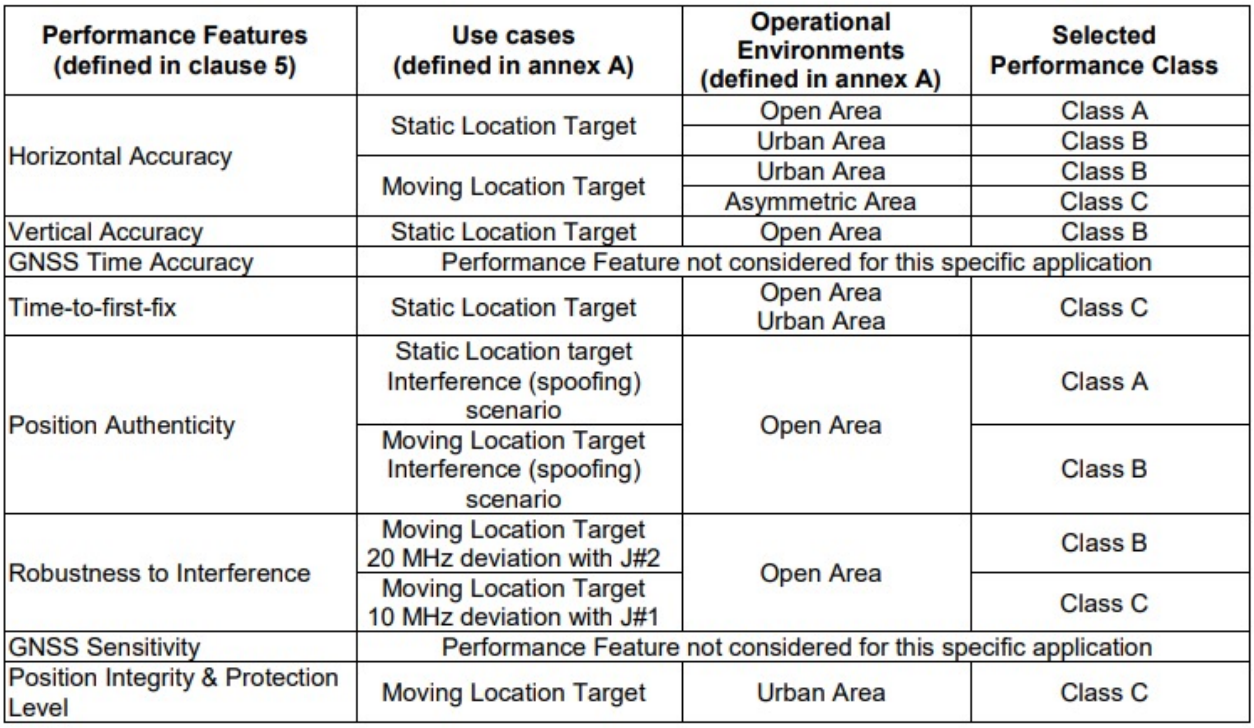
9. Position Day-to-Day Repeatability
10. Time to Fix Ambiguity (TTFA)

A detailed definition of each performance feature with its attributes and metrics is given in [9].

Other additional features identified but left for further study are:

1. Availability of Required Accuracy (probability that PVT data is provided with a certain level of accuracy)
2. EMI Localisation Accuracy (error of location measurement of an interfering signal)
3. GNSS-Denied Accuracy (error in PVT data when there is a loss of GNSS signal reception)
4. Position Integrity or Time-to-Alert (the time from occurrence of an unsafe integrity condition to the issue of an alerting message)
5. Position Integrity or Time-to-Recover-from-Alert (the time from cancellation of an unsafe integrity condition to removal of an alerting message)
6. Accuracy of Speed and Acceleration (horizontal and vertical)

Three classes of performance (A, B and C) are defined in order to categorise the performance level of the GBLS for a given performance feature, with class A being the highest and C the lowest.



Performance Features (defined in clause 5)	**Use cases (defined in annex A)**	**Operational Environments (defined in annex A)**	**Selected Performance Class**
Horizontal Accuracy	Static Location Target	Open Area	Class A
		Urban Area	Class B
	Moving Location Target	Urban Area	Class B
		Asymmetric Area	Class C
Vertical Accuracy	Static Location Target	Open Area	Class B
GNSS Time Accuracy	Performance Feature not considered for this specific application		
Time-to-first-fix	Static Location Target	Open Area Urban Area	Class C
Position Authenticity	Static Location target Interference (spoofing) scenario	Open Area	Class A
	Moving Location Target Interference (spoofing) scenario		Class B
Robustness to Interference	Moving Location Target 20 MHz deviation with J#2	Open Area	Class B
	Moving Location Target 10 MHz deviation with J#1		Class C
GNSS Sensitivity	Performance Feature not considered for this specific application		
Position Integrity & Protection Level	Moving Location Target	Urban Area	Class C

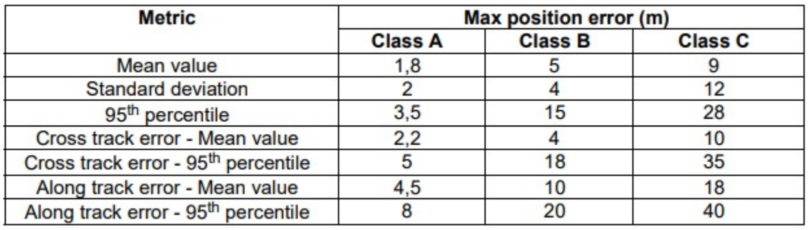
Figure 7. Example of selection of performance class for a specific GBLS application [9].

The standard [9] defines the performance requirements for each of the performance features. Given the operating conditions, and to comply with a Class of performance, the tested GBLS performance shall be equal to or better than the corresponding performance requirements.

The performance features are defined in each case for a range of operating conditions, where applicable, including:

1. Location target operational environments:
    - Open area
    - Urban
    - Asymmetric area
2. Location target motion types:
    - Moving
    - Static
3. GBLS types (Class A, B, C)
4. Clear signal (non-interfered) or signal interference conditions
5. Authenticity threat scenario and parameters
6. Integrity threat scenario and parameters

The information below presents an example of such performance requirements.



Metric	Max position error (m)		
	Class A	Class B	Class C
Mean value	1,8	5	9
Standard deviation	2	4	12
95th percentile	3,5	15	28
Cross track error - Mean value	2,2	4	10
Cross track error - 95th percentile	5	18	35
Along track error - Mean value	4,5	10	18
Along track error - 95th percentile	8	20	40

Figure 8. Example of performance requirements: horizontal position accuracy, moving location target, asymmetric area [9].

5.1.2.1. Position integrity

ETSI standard defines the position integrity as the ability of the GBLS to measure the trust that can be placed in the accuracy of the location target position.

It is expressed through the computation of a protection level associated with a predetermined integrity risk (as a function of the type of end-user application).

According to this standard, the ultimate purpose of an integrity solution is to provide the user with a horizontal protection level (HPL) which guarantees horizontal position error (HPE) bounding up to the required integrity risk, and maximises availability, e.g. the percentage of time that protection levels exist and remain below a predetermined value (the alert limit).

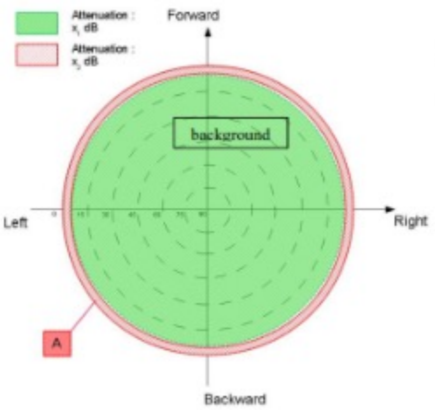
In terms of integrity algorithms, those mentioned by the standard can be based on receiver autonomous integrity monitoring (RAIM), a ground monitoring approach with a GNSS integrity channel (GIC), e.g. EGNOS, or a combination of both.

The integrity performance is defined by:

- The position integrity, expressed in terms of protection level expressed in metres at the 95th percentile.
- The integrity risk, expressed as the probability that the position accuracy exceeds the position protection level given that the position is flagged as valid.

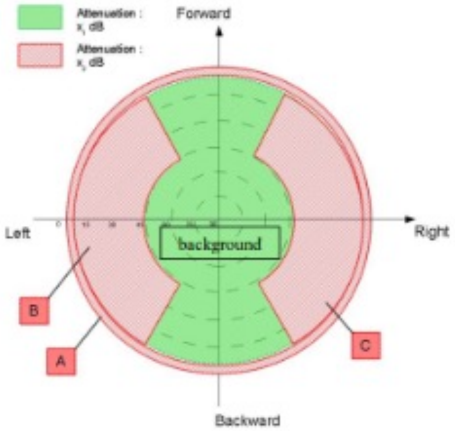
5.1.2.2. GNSS environments and threats

The ETSI standard defines three location target operational environments: open area/urban/asymmetric area (see below).



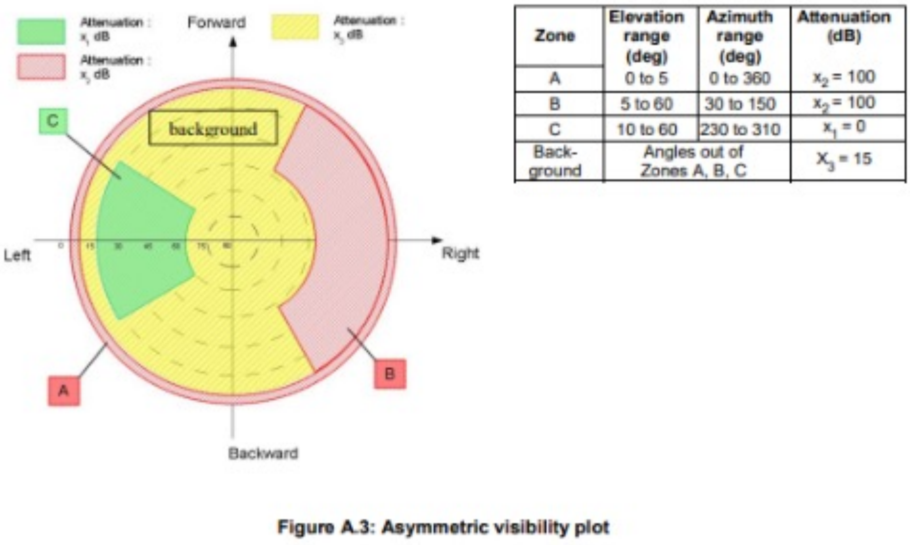
Zone	Elevation range (deg)	Azimuth range (deg)	Attenuation (dB)
A	0 to 5	0 to 360	$x_2 = 100$
Back-ground	Angles out of Zone A		$x_1 = 0$

Figure A.1: Open Sky plot



Zone	Elevation range (deg)	Azimuth range (deg)	Attenuation (dB)
A	0 to 5	0 to 360	$x_2 = 100$
B	5 to 60	210 to 330	$x_2 = 100$
C	5 to 60	30 to 150	$x_2 = 100$
Back-ground	Angles out of Zones A, B, C		$x_1 = 0$

Figure A.2: Urban canyon plot



Zone	Elevation range (deg)	Azimuth range (deg)	Attenuation (dB)
A	0 to 5	0 to 360	$x_2 = 100$
B	5 to 60	30 to 150	$x_2 = 100$
C	10 to 60	230 to 310	$x_1 = 0$
Back-ground	Angles out of Zones A, B, C		$X_3 = 15$

Figure A.3: Asymmetric visibility plot

Figure 9. Skyplots characterising areas according to ETSI 103 246.

It also defines perturbations and threats (multipath, interference, spoofing, non-LOS) to which the GBLS may be exposed.

5.1.2.3. Performance assessment approach

Document [7] from the ETSI standard specifies the procedures for testing the conformance of complex GBLS with the performance requirements specified in [9]. For each performance requirement, different classes are defined allowing the benchmarking of different GBLS addressing the same applications. The tests specified are of a complete GBLS, considered as 'black box', i.e. the tests are made as outputs of the system in response to stimuli applied at the inputs. The tests are defined for laboratory testing only, based on models and simulation, and not in the field.

The document presents the procedures required to test conformance with the performance features defined in [9]:

1. Horizontal Position Accuracy
2. Vertical Position Accuracy
3. Time-to-First-Fix
4. Position Authenticity
5. Robustness to Interference
6. GNSS Sensitivity
7. Position Integrity (Protection Level)
8. Position Day-to-Day Repeatability
9. Time-to-Fix Ambiguity

Clause 11 in [7] defines the tests intended to verify the position integrity performance of the GBLS in terms of:

- Horizontal Protection Level (HPL) expressed as the Position Error (HPE) at 95%
- Integrity risk, expressed as the probability that the horizontal position error exceeds the HPL

Annex A of [7] presents the test configurations to be used depending on the GBLS antenna connector accessibility:

1. Anechoic chamber test configuration, when the connector cannot be accessed.

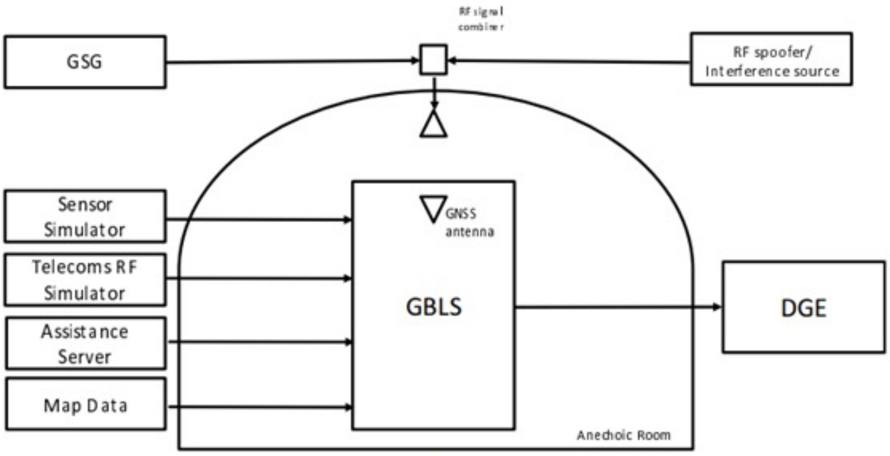


Figure A.1: System set up for tests in anechoic room

Figure 10. Anechoic chamber test configuration from ETSI 103 246-5, [7].

2. Wired connections test configuration, when access to the connector is possible.

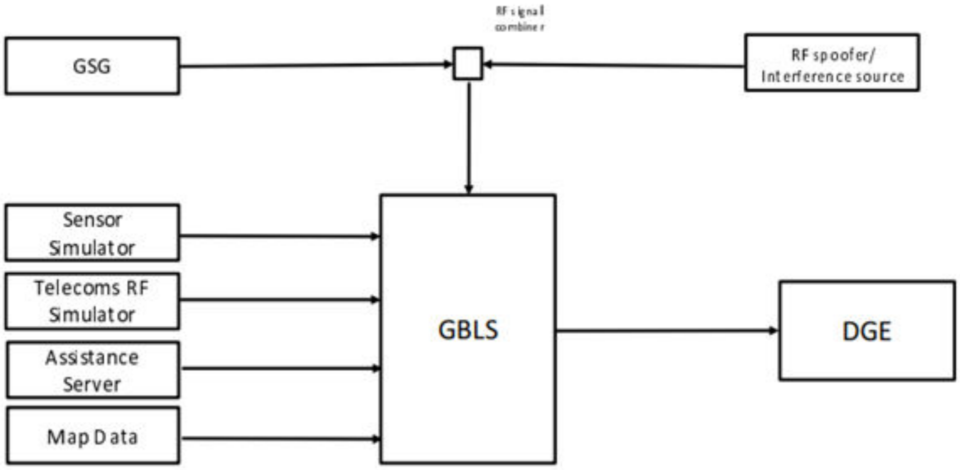


Figure A.2: System set up for tests with wired connections

Figure 11. Wired connections test configuration from ETSI 103 246-5, [7].

5.1.3. 3GPP standard

3GPP defines a standard which focuses on positioning methods and the associated signalling that can be sent via the network to support the positioning calculation. This is tackled in 3GPP TS 37.355, [13].

The specification defines e.g.

- Observed Time Difference of Arrival (OTDOA) based on LTE signals
- Assisted GNSS (A-GNSS) e.g. RTK and SSR signalling
- Enhanced Cell ID (E-CID) based on LTE signals
- Sensors,
- Terrestrial Beacon System (TBS),
- Wireless Local Area Network (WLAN),
- Bluetooth,
- New Radio (NR) E-CID,
- NR Downlink TDOA (NR DL-TDOA),
- NR Downlink Angle of Departure (NR DL-AoD)
- NR Multi-Roud Trip Time (RTT) positioning methods.

The Release 17 version of the specification outlines the 'assistance' information that can be sent via the network to support and enhance the determination of GNSS positioning integrity.

In 3GPP TS 38.305 [5] the following definitions are given:

Positioning integrity:	A measure of the trust in the accuracy of the position-related data and the ability to provide associated alerts.
Protection level (PL):	A statistical upper-bound of the positioning error (PE) that ensures the probability per unit of time of the true error being greater than the Alert Limit (AL), and the PL being less than or equal to the AL for longer than the time to alert (TTA), and less than the required Target Integrity Risk (TIR), i.e. the PL satisfies the following inequality: Prob per unit of time [((PE>AL) & (PL≤AL)) for longer than TTA] < required TIR When the PL bounds the positioning error in the horizontal plane or on the vertical axis then it is called horizontal protection level (HPL) or vertical protection level (VPL) respectively. A specific equation for the PL is not offered as this is implementation-defined. For the PL to be considered valid, it must simply satisfy the inequality above. *NOTE: The PL inequality is valid for all values of the AL.*

TS 38.305 also describes the integrity principle of operation including definitions and functionality relating to the integrity errors, bounds, TTA, and Do Not Use (DNU) flags, residual risks and correlation times specified in the LTE Positioning Protocol (LPP) TS 37.355.

The 3GPP TR 38.857 [14] describes the role of trust and integrity for positioning. Confidence is introduced as a general concept, and its relationship to the topic of integrity is studied in detail with respect to the assistance information that can be provided via the network to mitigate the impact of potential error sources and feared events, with the goal of improving positioning confidence. The study (TR 38.857) does not contain details on how the confidence is computed or conveyed but is the precursor investigation behind the standardised integrity calculations in 3GPP Release 17 (see LPP, TS 37.355).

TR 38.857 [14] also provides a set of use cases and requirements related to the automotive sector with associated integrity related key performance indicators (the table is reported here for completeness):

Table 2. Example of use cases and requirements in TR 38.857, [14].

AUTOMOTIVE EXAMPLES				
APPLICATION CATEGORIES	**TIR**	**AL**	**TTA**	**Integrity Availability**
Safety Critical Applications -Warnings (red light, obstacle, queue, curve speed, blind spot lane change, pedestrians etc) -Automated Driving (lane-level or better) -Emergency Brake Assist -Forward Collision Avoidance	Typical range: $\geq 10^{-8}$/hr to $\leq 10^{-6}$/hr	Typical range: ≥1.5m to <5m	Typically ranges from 100s of milliseconds to <10 seconds	Typically ranges from 95% to 99.9% or greater
Payment Critical Applications - Road User Charging (RUC) - Pay Per Use Insurance - Taxi Meter - Parking Fee Calculation	Typical range: $\geq 10^{-6}$/hr to $\leq 10^{-4}$/hr	Typical range: ≥1.5m to <25m		Typically ranges from 95% to 99.9% or greater
Smart Mobility - Freight and Fleet Management - Cargo/Asset Management - Vehicle Access/Clearance - Emergency Vehicle Priority - Speed Limit Information - In-Vehicle Signage - Reduce Speed Warning - Dynamic Ride Sharing				

5.1.4. IEEE SA P1952, [15]

IEEE P1952 has been established to produce a standard for resilient positioning, navigation, and timing (PNT) for related user equipment (UE). This standard will create a common vocabulary and framework for evaluating PNT UE resilience, the degree to which such equipment continues to perform its mission in the face of adversity.

Discussion surrounding P1952 have helped to clarify several aspects. Currently there is no generally accepted standard of “Resilient PNT user equipment”. There are many threats to PNT and many claims of resilience, but there are limited standards to test such claims. In most general sense, resilience is a “toughness” or “capacity to recover quickly from difficulties” or “the degree to which a system continues to perform its mission in the face of adversity”.

The standard effort (P1952) refers to the definition of resilience in US Presidential Policy Directive (PPD-21): “*ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions*”.

The goals of the standard are:

- Fostering and formalising a culture of resilience in the civilian PNT community

- Creating resilience language to ease engagement/communication between stakeholders
    - Helping users know what to ask for in resilience
    - Helping vendors communicate with each other about resilience
    - Drawing distinctions between concepts such as ‘resilience’, ‘robustness’, ‘accuracy’, etc.
    - Define expected PNT system behaviours and outcomes
- PNT resilience should apply to all critical infrastructure sectors, all applications, all PNT sources or services, and all threats (‘agnosticism’ or ‘independence’)
- Increase attention paid to resilience within the PNT industry, including the whole lifecycle of development and deployment

The standard focuses on the PNT user equipment boundaries, and it does not specify the internal behaviour, or will not standardise PNT infrastructure.

The key aspects are:

- Many concepts come from the Resilient PNT Conformance Framework, developed by many PNT stakeholders led by US Department of Homeland Security,
- Key concepts
    - Outcome-based: focusing on the boundary of PNT user equipment, not internals (allowing innovation)
    - Cumulative: successive resilience levels build upon previous ones
    - Generalised: independent (if possible) to threat type, use case, etc.
- To make resilience future proof and broadly applicable resilience is separate from threats, application performance needs, and from PNT sources,
- End-users should select the resilience level that is appropriate based on their risk tolerance, budget, and application criticality.

5.1.5. ETSI V2X standard [16]-[20]

ETSI has a dedicated Technical Committee (TC) responsible for standardisation to support the development and implementation of Intelligent Transport System (ITS) services for transport networks, vehicles and transport users, including interface aspects, multiple modes of transport and interoperability between systems and networks. The specification provided by ETSI becomes part of the European standard for ITS.

This committee is working on stage 1 with the definition of the basic applications, stage 2 with functional requirements and operational requirements, and stage 3 that provides detailed specifications for higher layer protocols.

The access technology is developed by 3GPP for cellular-based V2X technology and IEEE for the 802.11-based family of technologies. The basic architecture is provided in the following figure, [16].

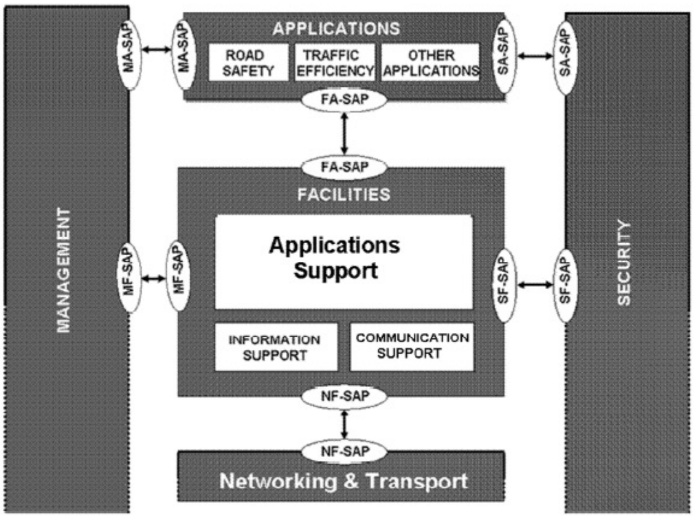


Figure 12. Reference architecture, ETSI ITS standard.

ETSI has standardised, in particular, the services at facility layers which convey the status information (via the cooperative awareness messages, CAM), event information (via the decentralised environmental notification messages, DENM), or information about the vision of a specific vehicle (via the cooperative perception message, CPM) from one ITS station to another.

In both CAM and DENM messages, the position information is transmitted in a very similar manner. As such, in the following paragraphs, the analysis is based on the CAM message. A brief review of the CPM message is also provided. In addition, the ETSI specification introduces the Positioning and Timing (PoTi) service facility layer. The essential information is also provided.

5.1.5.1. Cooperative Awareness Message (CAM), [17]

The CAM message is generated according to the following figure.

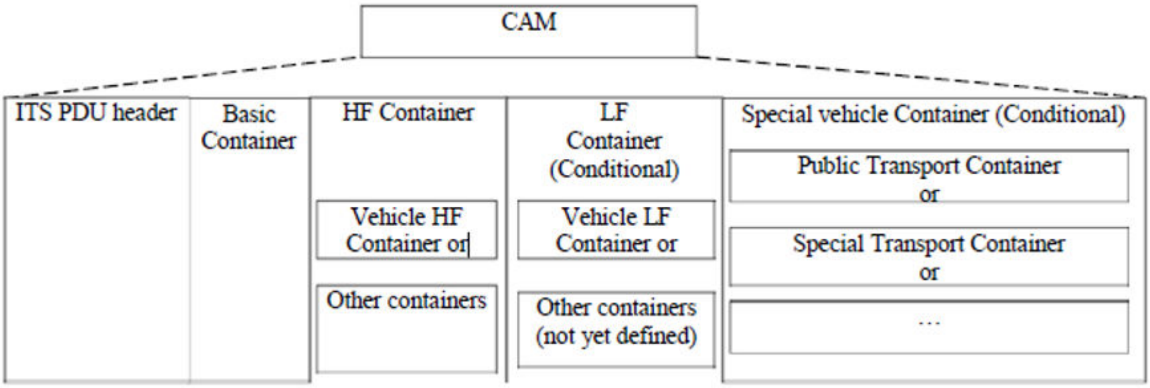
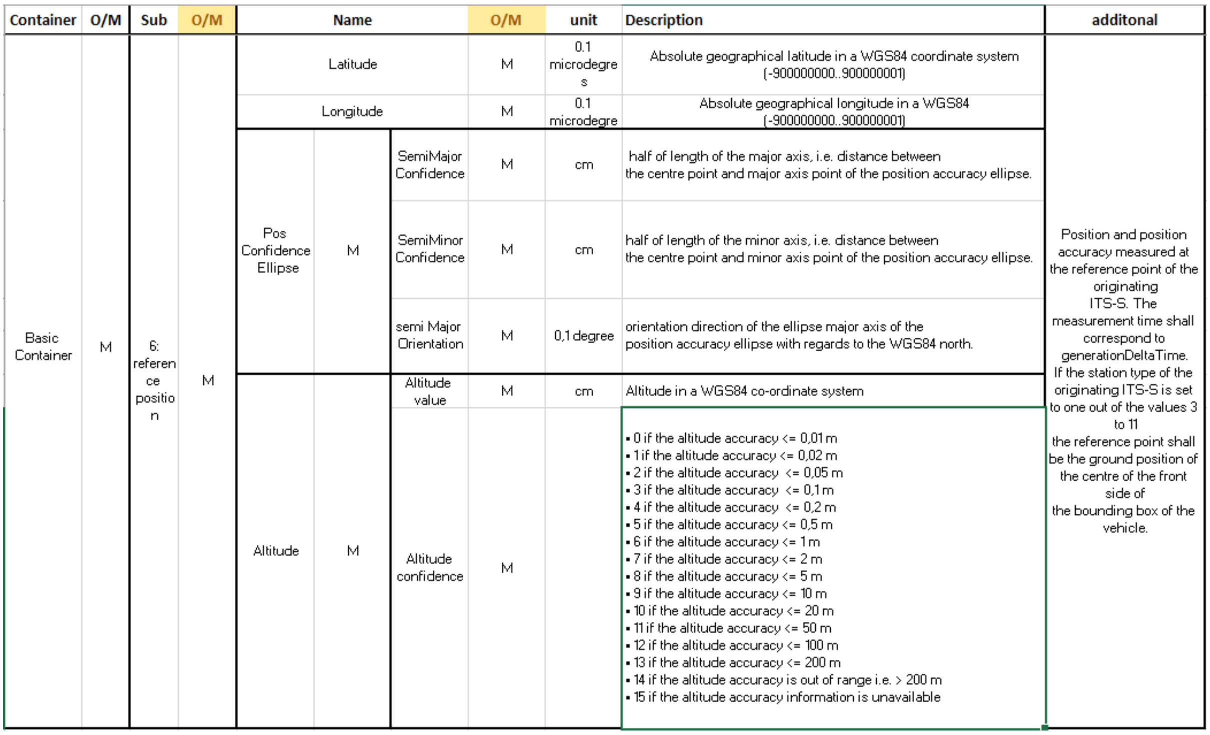


Figure 13. Structure of CAM.

Information related to the position are contained in the basic container, in the high-frequency container and in low-frequency container.

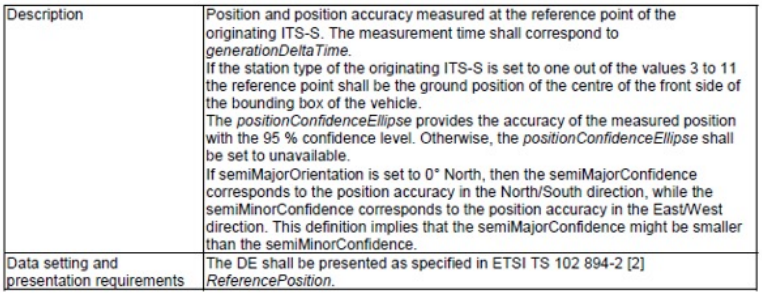
The basic container introduces the ITS station 'ReferencePosition' Date Element (DE), which is structured as follows.



Container	O/M	Sub	O/M	Name			O/M	unit	Description	additonal
Basic Container	M	6: reference position	M	Latitude			M	0.1 microdegres	Absolute geographical latitude in a WGS84 coordinate system (-900000000..900000001)	Position and position accuracy measured at the reference point of the originating ITS-S. The measurement time shall correspond to generationDeltaTime. If the station type of the originating ITS-S is set to one out of the values 3 to 11 the reference point shall be the ground position of the centre of the front side of the bounding box of the vehicle.
				Longitude			M	0.1 microdegre	Absolute geographical longitude in a WGS84 (-900000000..900000001)	
				Pos Confidence Ellipse	M	SemiMajor Confidence	M	cm	half of length of the major axis, i.e. distance between the centre point and major axis point of the position accuracy ellipse.	
						SemiMinor Confidence	M	cm	half of length of the minor axis, i.e. distance between the centre point and minor axis point of the position accuracy ellipse.	
						semi Major Orientation	M	0,1 degree	orientation direction of the ellipse major axis of the position accuracy ellipse with regards to the WGS84 north.	
				Altitude	M	Altitude value	M	cm	Altitude in a WGS84 co-ordinate system	
						Altitude confidence	M		▪ 0 if the altitude accuracy <= 0,01 m ▪ 1 if the altitude accuracy <= 0,02 m ▪ 2 if the altitude accuracy <= 0,05 m ▪ 3 if the altitude accuracy <= 0,1 m ▪ 4 if the altitude accuracy <= 0,2 m ▪ 5 if the altitude accuracy <= 0,5 m ▪ 6 if the altitude accuracy <= 1 m ▪ 7 if the altitude accuracy <= 2 m ▪ 8 if the altitude accuracy <= 5 m ▪ 9 if the altitude accuracy <= 10 m ▪ 10 if the altitude accuracy <= 20 m ▪ 11 if the altitude accuracy <= 50 m ▪ 12 if the altitude accuracy <= 100 m ▪ 13 if the altitude accuracy <= 200 m ▪ 14 if the altitude accuracy is out of range i.e. > 200 m ▪ 15 if the altitude accuracy information is unavailable	

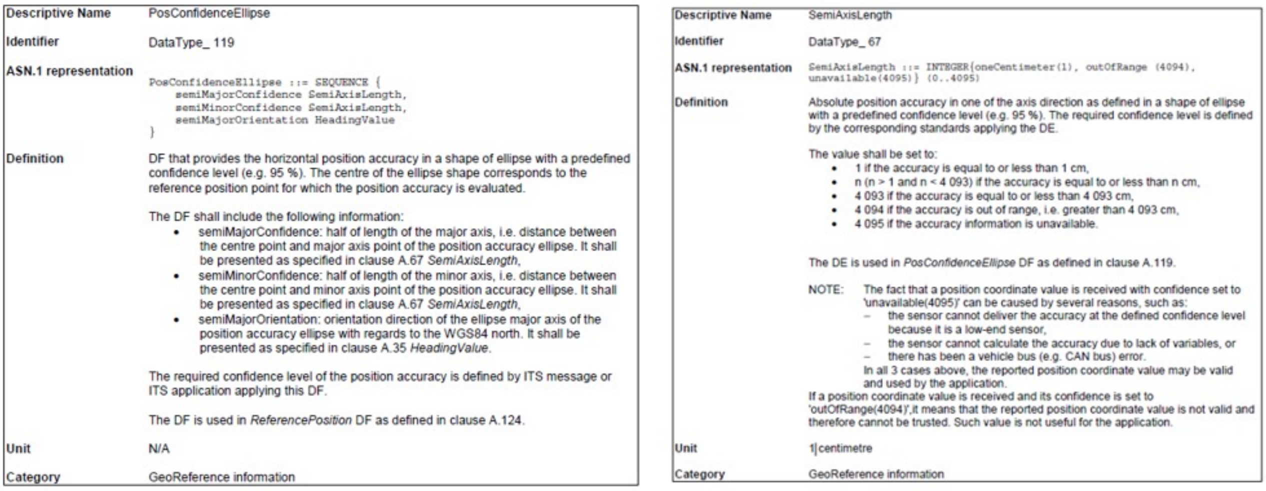
Figure 14. Structure of the DE 'ReferencePosition' in CAM messages.

As can be seen, the reference position provides not only the latitude, longitude and altitude value, but also the confidence information, under the Data Frame (DF) 'PosConfidenceEllipse'. The definition of the DE 'ReferencePosition' can be found in Figure 15, while the definition of 'PosConfidenceEllipse' and its representation can be found in Figure 16.



Description	Position and position accuracy measured at the reference point of the originating ITS-S. The measurement time shall correspond to *generationDeltaTime*. If the station type of the originating ITS-S is set to one out of the values 3 to 11 the reference point shall be the ground position of the centre of the front side of the bounding box of the vehicle. The *positionConfidenceEllipse* provides the accuracy of the measured position with the 95 % confidence level. Otherwise, the *positionConfidenceEllipse* shall be set to unavailable. If semiMajorOrientation is set to 0° North, then the semiMajorConfidence corresponds to the position accuracy in the North/South direction, while the semiMinorConfidence corresponds to the position accuracy in the East/West direction. This definition implies that the semiMajorConfidence might be smaller than the semiMinorConfidence.
Data setting and presentation requirements	The DE shall be presented as specified in ETSI TS 102 894-2 [2] *ReferencePosition*.

Figure 15. Definition of the DE 'ReferencePosition', [17].



Descriptive Name	PosConfidenceEllipse
Identifier	DataType_ 119

ASN.1 representation

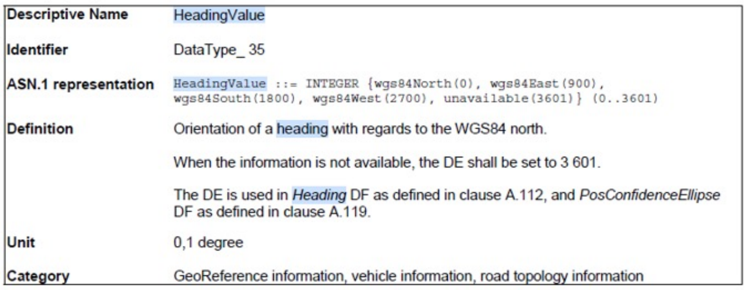
```
PosConfidenceEllipse ::= SEQUENCE {
    semiMajorConfidence SemiAxisLength,
    semiMinorConfidence SemiAxisLength,
    semiMajorOrientation HeadingValue
}
```

Definition	DF that provides the horizontal position accuracy in a shape of ellipse with a predefined confidence level (e.g. 95 %). The centre of the ellipse shape corresponds to the reference position point for which the position accuracy is evaluated. The DF shall include the following information: • semiMajorConfidence: half of length of the major axis, i.e. distance between the centre point and major axis point of the position accuracy ellipse. It shall be presented as specified in clause A.67 *SemiAxisLength*, • semiMinorConfidence: half of length of the minor axis, i.e. distance between the centre point and minor axis point of the position accuracy ellipse. It shall be presented as specified in clause A.67 *SemiAxisLength*, • semiMajorOrientation: orientation direction of the ellipse major axis of the position accuracy ellipse with regards to the WGS84 north. It shall be presented as specified in clause A.35 *HeadingValue*. The required confidence level of the position accuracy is defined by ITS message or ITS application applying this DF. The DF is used in *ReferencePosition* DF as defined in clause A.124.
Unit	N/A
Category	GeoReference information

Descriptive Name	SemiAxisLength
Identifier	DataType_ 67
ASN.1 representation	`SemiAxisLength ::= INTEGER{oneCentimeter(1), outOfRange (4094), unavailable(4095)} (0..4095)`
Definition	Absolute position accuracy in one of the axis direction as defined in a shape of ellipse with a predefined confidence level (e.g. 95 %). The required confidence level is defined by the corresponding standards applying the DE. The value shall be set to: • 1 if the accuracy is equal to or less than 1 cm, • n (n > 1 and n < 4 093) if the accuracy is equal to or less than n cm, • 4 093 if the accuracy is equal to or less than 4 093 cm, • 4 094 if the accuracy is out of range, i.e. greater than 4 093 cm, • 4 095 if the accuracy information is unavailable. The DE is used in *PosConfidenceEllipse* DF as defined in clause A.119. NOTE: The fact that a position coordinate value is received with confidence set to 'unavailable(4095)' can be caused by several reasons, such as: – the sensor cannot deliver the accuracy at the defined confidence level because it is a low-end sensor, – the sensor cannot calculate the accuracy due to lack of variables, or – there has been a vehicle bus (e.g. CAN bus) error. In all 3 cases above, the reported position coordinate value may be valid and used by the application. If a position coordinate value is received and its confidence is set to 'outOfRange(4094)',it means that the reported position coordinate value is not valid and therefore cannot be trusted. Such value is not useful for the application.
Unit	1 centimetre
Category	GeoReference information

Figure 16. Definition of DF "PosConfidenceEllipse" (left) and DE "SemiAxisLength" (right) [18].

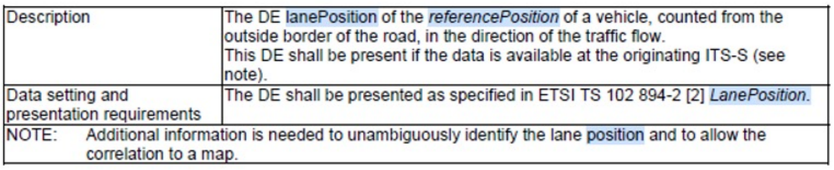
Note that the 'semiMajorOrientation' corresponds to the heading value which is described as follows:



Descriptive Name	HeadingValue
Identifier	DataType_ 35
ASN.1 representation	`HeadingValue ::= INTEGER {wgs84North(0), wgs84East(900), wgs84South(1800), wgs84West(2700), unavailable(3601)} (0..3601)`
Definition	Orientation of a heading with regards to the WGS84 north. When the information is not available, the DE shall be set to 3 601. The DE is used in *Heading* DF as defined in clause A.112, and *PosConfidenceEllipse* DF as defined in clause A.119.
Unit	0,1 degree
Category	GeoReference information, vehicle information, road topology information

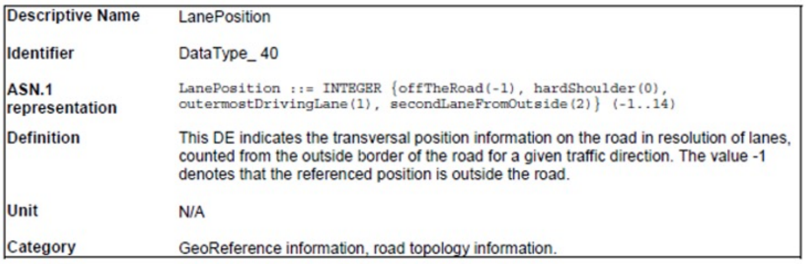
Figure 17.DE "HeadingValue", [18].

The high-frequency container provides one DE to exchange the lateral position in the resolution of lanes. In [18] this DE is considered to be OPTIONAL. The lane position is provided as a lane number where the ITS station is located. This is described in the following figures.



Description	The DE lanePosition of the *referencePosition* of a vehicle, counted from the outside border of the road, in the direction of the traffic flow. This DE shall be present if the data is available at the originating ITS-S (see note).
Data setting and presentation requirements	The DE shall be presented as specified in ETSI TS 102 894-2 [2] *LanePosition*.
NOTE:	Additional information is needed to unambiguously identify the lane position and to allow the correlation to a map.

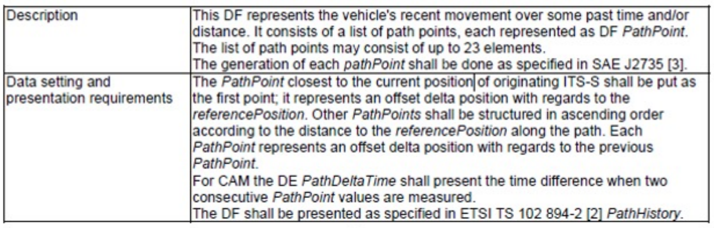
Figure 18. Definition of the DE 'lanePosition', [17].



Descriptive Name	LanePosition
Identifier	DataType_ 40
ASN.1 representation	`LanePosition ::= INTEGER {offTheRoad(-1), hardShoulder(0), outermostDrivingLane(1), secondLaneFromOutside(2)} (-1..14)`
Definition	This DE indicates the transversal position information on the road in resolution of lanes, counted from the outside border of the road for a given traffic direction. The value -1 denotes that the referenced position is outside the road.
Unit	N/A
Category	GeoReference information, road topology information.

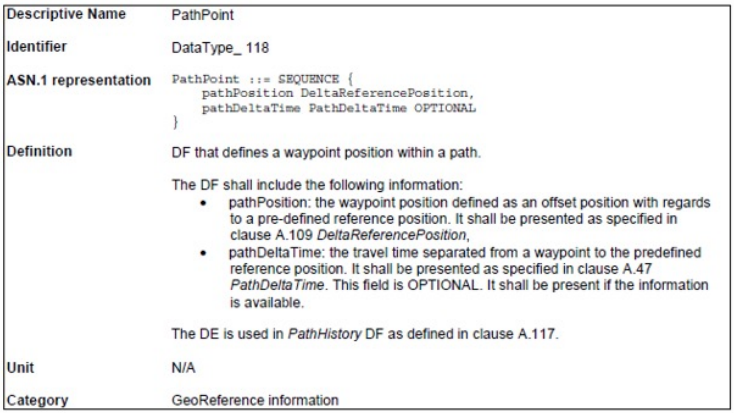
Figure 19. Definition of the data frame 'LanePosition' in [18].

Lastly, ETSI specification also introduces the concept of path history, i.e. a list of path points that correspond to the previous (max.) 23 previous delta positions with reference to the ITS reference position. Whenever this container is present the path history is intended to be present. This is shown in the following figures.



Description	This DF represents the vehicle's recent movement over some past time and/or distance. It consists of a list of path points, each represented as DF *PathPoint*. The list of path points may consist of up to 23 elements. The generation of each *pathPoint* shall be done as specified in SAE J2735 [3].
Data setting and presentation requirements	The *PathPoint* closest to the current position of originating ITS-S shall be put as the first point; it represents an offset delta position with regards to the *referencePosition*. Other *PathPoints* shall be structured in ascending order according to the distance to the *referencePosition* along the path. Each *PathPoint* represents an offset delta position with regards to the previous *PathPoint*. For CAM the DE *PathDeltaTime* shall present the time difference when two consecutive *PathPoint* values are measured. The DF shall be presented as specified in ETSI TS 102 894-2 [2] *PathHistory*.

Figure 20. Definition of the DE 'PathHistory', [17]



Descriptive Name	PathPoint
Identifier	DataType_ 118

ASN.1 representation

```
PathPoint ::= SEQUENCE {
    pathPosition DeltaReferencePosition,
    pathDeltaTime PathDeltaTime OPTIONAL
}
```

Definition	DF that defines a waypoint position within a path. The DF shall include the following information: • pathPosition: the waypoint position defined as an offset position with regards to a pre-defined reference position. It shall be presented as specified in clause A.109 *DeltaReferencePosition*, • pathDeltaTime: the travel time separated from a waypoint to the predefined reference position. It shall be presented as specified in clause A.47 *PathDeltaTime*. This field is OPTIONAL. It shall be present if the information is available. The DE is used in *PathHistory* DF as defined in clause A.117.
Unit	N/A
Category	GeoReference information

Figure 21. Definition of DF 'PathPoint', [18].

5.1.5.2. Collective Perception Message (CPM), [20]

ETSI has standardised messages to exchange objects detected by sensors with nearby vehicles as Collective Perception Messages (CPM) [21]. Vehicles equipped with CPM capability can receive sensor-based object lists from other road users or road infrastructure. In turn, the enhanced information exchange leads to a higher redundancy in the sensor fusion. Hence, the reliability of the sensor fusion is increased as well.

The CPM, as discussed in ETSI TS 103 324 v0.0.33 [21], describes a message consisting of multiple message containers.

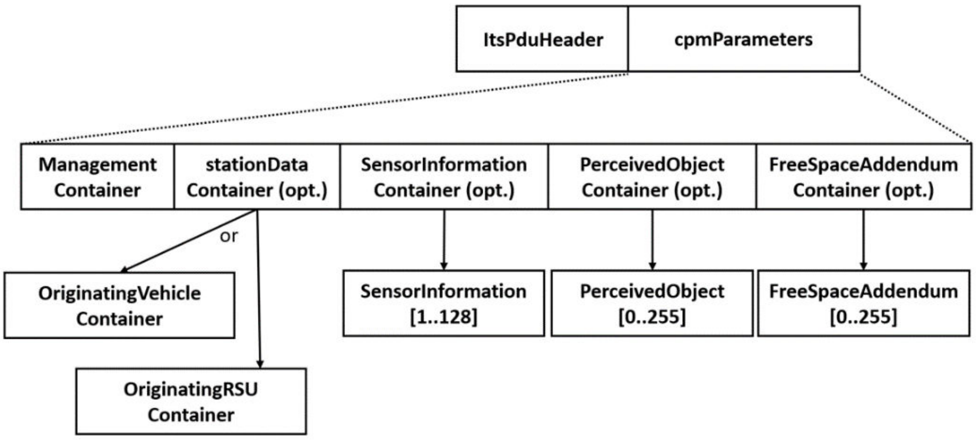


Figure 22. CPM Message Structure.

Within the message containers different notions of confidence exist as expressed in the following table:

Table 3. Confidence information in the CPM message.

Detection confidence	Refers to the sensor or sensor system output to describe the certainty with which a detection was successful.
Object existence confidence	Quantification of the confidence that a detected object exists, i.e. has been detected previously and has continuously been detected by a sensor.
Free space existence confidence	Quantification of the confidence that a detected free space exists.
Confidence level	Probability with which the estimation of the location of a statistical parameter (e.g. an arithmetic mean) in a sample survey is also true for the population.

5.1.5.3. Positioning and Timing (PoTi) service, [21]

The Positioning and Timing (PoTi) service, as defined in [21], specifies the high-level architecture and requirements for ITS station positioning information generation.

In the facility layer, the PoTi service is used to harmonise position and timing information for different services, such as the Cooperative Awareness (CA), and exchange data between the management entity, security entity, and with the transport and network layer.

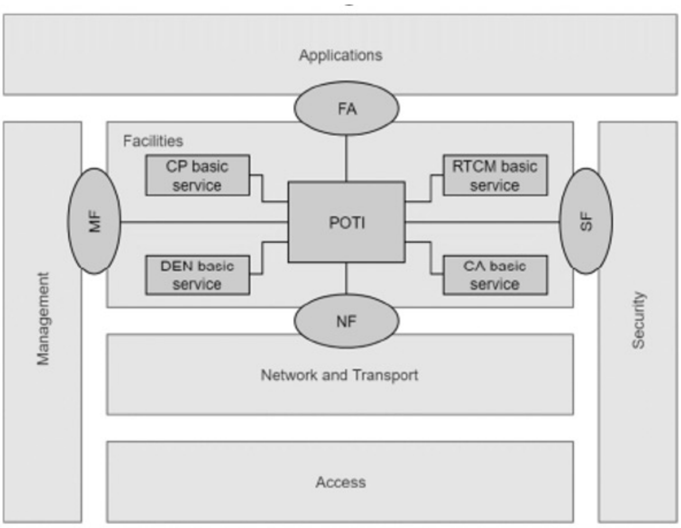


Figure 23. PoTi architecture, [21].

The PoTi feature also specifies the reference position for passenger cars, trucks, buses, motorbikes, pedestrians, etc. This is considered as the anchor point of a bounding box. Note that the reference position does not necessarily correspond to the GNSS antenna position.

PoTi specification also provides the definition of the confidence ellipse: "A confidence ellipse defines a confidence area, centred around the estimated value of a two-dimensional quantity. A confidence ellipse is described via a major axis, minor axis and orientation of the major axis relative to a reference direction. A confidence level of X% means that the confidence interval or confidence ellipse would contain the true value of the quantity in a long series of measurements in at least X% of the measurements".

5.2. SAE standard

Two SAE reports should be considered as references: SAE J2945/1 developed for Dedicated Short-Range Communication (DSRC), and J3161/1 developed for LTE-V2X, but references much of J2945/1. Key features of the standard include:

- Positioning accuracy of 1.5m over 68% of measurements under open sky test conditions.
- The estimated absolute position is provided together with semi-major, semi-minor confidence ellipse and semi-major axis orientation, but the requirements for estimating these are outside the scope of this TR – i.e. the way to estimate the confidence ellipse.
- There is no plan to extend or rework the definition of confidence or trustworthiness of the position in SAE.
- The Basic Safety Message (BSM) was defined with the intention to exchange information between ITS stations which are located at distance such that

mild requirements on positioning are acceptable (not at very short distance)

- The positioning and confidence will be more important for advanced use cases, such as those related to CPM and when the information is considered in the decision chain of the vehicle.
- When defining the BSM specification in SAE, the main interest was relative positioning; as an example when two vehicles follow each other, it does not matter whether their individual absolute position error is large as long as the relative position is accurate. Stations located in similar sky visibility conditions might experience similar ionospheric and tropospheric delays and hence could be affected by those impairments in a similar manner (considering similar receiver type with no assistance or correction services). Under SAE J2735 the data element 'posConfidence' of type 'PositionConfidenceSet' is an optional part of the 'FullPositionVector', which is optional itself. SAE J2945/1, meanwhile, does not even mention 'posConfidence'.
- Further, under SAE J2735 the data element accuracy of type 'positionalAccuracy' is a non-optional part of 'BSMcoreData' and therefore part of every BSM. Whereas in SAE J2945/1 the system sets the values in the 'DF_PositionalAccuracy' data frame of the BSM with values corresponding to its accuracy estimate for the vehicle position data included in the corresponding BSM. SAE J2945/1A thus confirms through a manufacturer report that 'DF_PositionalAccuracy' is set with the values corresponding to its accuracy estimate for the vehicle position data.

5.3. Chinese-related standard

For the position information and position confidence in the V2X messages, a national standard under research in China has observed that the accuracy of a vehicular positioning system in open sky area should reach 1.5m at a 68% degree of confidence. The position confidence in BSM message is defined to represent the type of positioning deflection plug-in unit, i.e. high-precision unit and normal-precision unit.

5.4. Relevant works in other organisations

Other organisations are also working on the V2X standard. In particular, the CAR 2 CAR Communication Consortium (C2C-CC) is contributing to the development and specification of ITS by defining Basic System Profiles (BSP) that indicate how the standard should be used in the ecosystem. In the following passages, specific parts of the BSP that refer to the positioning information are reviewed.

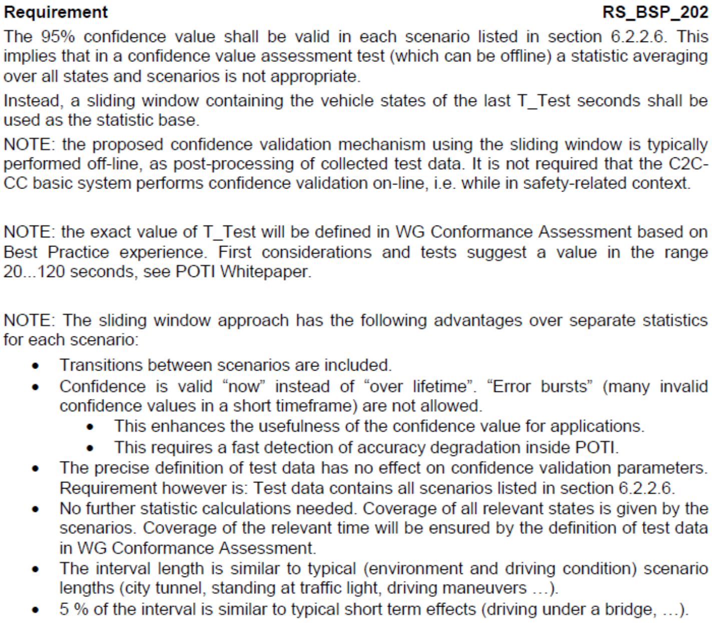
5.4.1. Car 2 Car Communication Consortium (C2C), [22]

The ‘RS_BSP_291’ of the BSP [22] indicates that “a vehicle C-ITS station shall transmit CAMs when position confidence information (see RS_BSP_535) is available and the station clock adheres to RS_BSP_206”. Confidence is not mandatory, but CAMs can only be sent if confidence information is available, as described in RS_BSP_535.

Section 6.2.2.3 of the BSP introduces the requirements on the validation of the confidence information related to the reference position.

RS_BSP_199 states that the “accuracy estimation shall yield valid 95% confidence values”.

The RS_BSP_202 indicates the following:



Requirement **RS_BSP_202**

The 95% confidence value shall be valid in each scenario listed in section 6.2.2.6. This implies that in a confidence value assessment test (which can be offline) a statistic averaging over all states and scenarios is not appropriate.

Instead, a sliding window containing the vehicle states of the last T_Test seconds shall be used as the statistic base.

NOTE: the proposed confidence validation mechanism using the sliding window is typically performed off-line, as post-processing of collected test data. It is not required that the C2C-CC basic system performs confidence validation on-line, i.e. while in safety-related context.

NOTE: the exact value of T_Test will be defined in WG Conformance Assessment based on Best Practice experience. First considerations and tests suggest a value in the range 20...120 seconds, see POTI Whitepaper.

NOTE: The sliding window approach has the following advantages over separate statistics for each scenario:

- Transitions between scenarios are included.
- Confidence is valid “now” instead of “over lifetime”. “Error bursts” (many invalid confidence values in a short timeframe) are not allowed.
  - This enhances the usefulness of the confidence value for applications.
  - This requires a fast detection of accuracy degradation inside POTI.
- The precise definition of test data has no effect on confidence validation parameters. Requirement however is: Test data contains all scenarios listed in section 6.2.2.6.
- No further statistic calculations needed. Coverage of all relevant states is given by the scenarios. Coverage of the relevant time will be ensured by the definition of test data in WG Conformance Assessment.
- The interval length is similar to typical (environment and driving condition) scenario lengths (city tunnel, standing at traffic light, driving maneuvers …).
- 5 % of the interval is similar to typical short term effects (driving under a bridge, …).

Figure 24. RS_BSP_202, [22]

Different scenarios are defined in the BSP with specific requirements associated to those. The confidence level is computed according to a time window, but the value is not precisely specified (it is in the order of minutes).

In particular there are two requirements for confidence:

First requirement: Confidence error bound

$$\textbf{Prob}\,(\textbf{Horizontal Error}_{\text{EPOCH t}} \le \textbf{Ellipse(semiMinorConfidence, semiMajorConfidence)}_{\text{EPOCH t}}) \ge \textbf{95\%}$$

This bound should be valid according the ETSI and SAE requirements, and according to C2C-CC BSP.

ETSI and SAE do not indicate how this should be specifically verified and tested. C2C BSP indicates in RS_BSP_202 that “the 95% confidence information shall be valid in each scenario listed in the BSP RS_BSP_209”. The transmitter has to satisfy the confidence bound and the proposed methodology considers a “statistical population according to [a] sliding window consisting of all the vehicle states (see RS_BSP_428) over the last ‘pPotiWindowTime’ seconds instead of one large dataset containing all scenarios (up to 120s)”.

This is represented in the figure below:

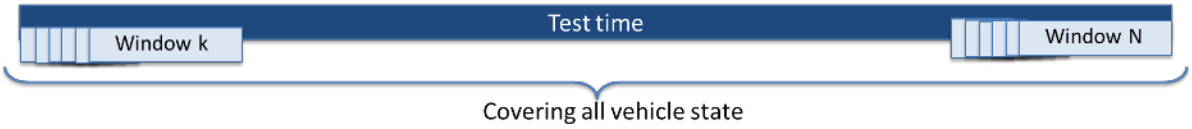


Figure 25. Representation of the test methodology in BSP.

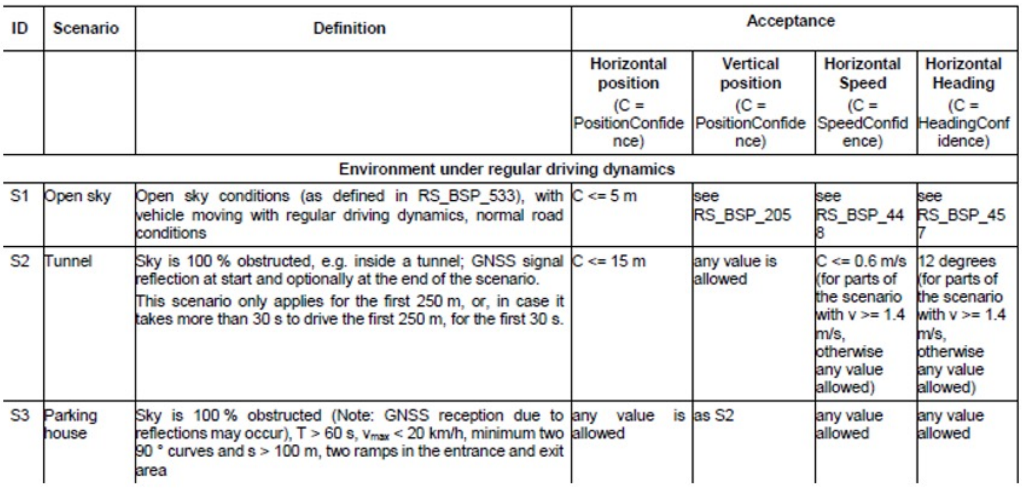
Second requirement: Maximum confidence requirements that guarantees minimum performance in a variety of scenarios

This is present only in the C2C-CC BSP and it does not depend on the application/use case, but rather depends on the scenarios.

$$\mathbf{Prob\ (semiMinorConfidence/semiMajorConfidence_{EPOCH,t} \leq C_{scenario}) \geq 95\%}$$

Here, ‘$C_{scenario}$’ is the maximum of ‘semiMajorConfidence’ and ‘semiMinorConfidence’. The condition shall be fulfilled with at least 95% probability in the given scenario.

The scenarios and the acceptance criteria are partially shown in the following figure (‘$C_{scenario}$’ is simply called ‘C’ in the figure below)



ID	Scenario	Definition	Acceptance			
			Horizontal position (C = PositionConfidence)	Vertical position (C = PositionConfidence)	Horizontal Speed (C = SpeedConfidence)	Horizontal Heading (C = HeadingConfidence)
Environment under regular driving dynamics						
S1	Open sky	Open sky conditions (as defined in RS_BSP_533), with vehicle moving with regular driving dynamics, normal road conditions	C <= 5 m	see RS_BSP_205	see RS_BSP_448	see RS_BSP_457
S2	Tunnel	Sky is 100 % obstructed, e.g. inside a tunnel; GNSS signal reflection at start and optionally at the end of the scenario. This scenario only applies for the first 250 m, or, in case it takes more than 30 s to drive the first 250 m, for the first 30 s.	C <= 15 m	any value is allowed	C <= 0.6 m/s (for parts of the scenario with v >= 1.4 m/s, otherwise any value allowed)	12 degrees (for parts of the scenario with v >= 1.4 m/s, otherwise any value allowed)
S3	Parking house	Sky is 100 % obstructed (Note: GNSS reception due to reflections may occur), T > 60 s, v_{max} < 20 km/h, minimum two 90 ° curves and s > 100 m, two ramps in the entrance and exit area	any value is allowed	as S2	any value allowed	any value allowed

Figure 26. Extract from C2C-CC RS_BSP_209, [22].

Note: The table is not represented exhaustively.

5.5. Other relevant work in 5GAA

5GAA conducted serval works which are relevant in the context of positioning: in particular the use cases master list which give the service level requirements related to positioning and the accuracy that the application requires. The relationship between position, accuracy and confidence in these use cases is discussed later in this document.

Other work items are considered as relevant for this work, in particular:

- STiCAD: Safety Treatment in Connected and Automated Driving Functions,
- V2XHAP: System Architecture and Solution Development; High-Accuracy Positioning for C-V2X.

5.5.1. Safety Treatment in Connected and Automated Driving Functions, STiCAD

The purpose of the first STiCAD work item in 5GAA [23] 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 original equipment manufacturers (OEMs) to better treat safety in new use cases enabled by V2X technologies. STiCAD reporting has helped to identify what standardisation needs may exist related to safety in V2X systems and what conclusions should be reached from the investigation.

Two representative use cases were selected to gain insight into this question:

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

The pre-eminent existing automotive safety engineering standard, ISO 26262, is written from the perspective that the largest item (system to be safety engineered) is a single vehicle. Therefore, it can be seen that the safety engineering of V2X systems moves the automotive industry into a new safety engineering paradigm. The conclusion reached by the work item is that ISO 26262 needs to be updated if it is to be used to tackle the safety engineering of cars that are connected using V2X communications.

Despite the above observation, STiCAD used the basic framework provided by ISO 26262, and it was found to be broadly fit for purpose, despite some anomalies in the use of terms such as ‘ASIL’ (Automotive Safety Integrity Level) when describing and discussing systems comprising components in multiple vehicles, despite the fact that such trans-vehicle systems are currently outside the scope of ISO 26262. The study has shown that it is critical that safety be managed rigorously in at least some V2X use cases.

A new work item is ongoing with the goal of further defining an overall framework to exchange information between two ITS stations while ensuring mutual trust, [24].

5.5.2. V2XHAP

Document [25] provides the results of the WID high-precision positioning for V2X. This study focused on research into high-accuracy positioning (HAP) for V2X services.

The relevant Technical Report describing this work gives an overview of the importance of the positioning information in the context of V2X. In particular, it outlines the positioning requirements for several use cases and shows the spread of requirements ranging from 0.1m at 99.7% (3σ) for tele-operated driving to 30m or 50m at 68% (σ) for software updates or for HD content delivery. The importance of reliability, accuracy, and integrity is also explained.

In the TR, three different architectures are proposed: UE-based positioning, UE-assisted positioning, and sidelink positioning together with different technologies such as GNSS-based location services using sensors and HD MAP, SLAM approaches, terrestrial ranging approaches, location services based on cellular networks, sidelink positioning, cooperative positioning, 5G millimetre-based positioning, etc. Results from these investigations are all provided in the report.

It is important to note that the work item also provided a list of KPIs which are important for positioning. The complete list can be found in the TR and includes: positioning accuracy, availability, latency, TTFF, update rate, continuity (likelihood that the positioning system functionality will be available during the complete duration of the intended operation if the positioning system is functioning at the beginning of the operation), reliability (measure of the ability of a positioning system to provide the position-related data under stated conditions for a specified period), integrity, time to alert, etc.

6. Definition of the methodology and analysis

The scope of the current work was to understand and define methods to increase the trustworthiness of the position information received by the V2X application in order to decide how to use this information, i.e. purely as 'information' for the driver or as part of the driving strategy decision chain for an assisted or autonomous vehicle.

During the discussion it was highlighted that some OEMs have already or are going to soon deploy V2X for Day 1 applications and, as such, this work should aim to avoid delaying further deployments. Nevertheless, if gaps are identified, this should be considered as the basis for the definition of a solid framework for Day 2 applications, and beyond.

The work has been structured in the following manner:

- Defining the boundaries of the work
- Defining the architecture of the work as a baseline reference for positioning-related work
- Defining trustworthiness
- Analysing the gaps
  - Analysis of stakeholder expectations
  - Existing metrics
  - Testing
- OEM feedback on confidence metrics (collected via an internal survey)
- Recommendations
- Discussing next steps

6.1. Defining the boundaries of the work

During the discussion two different approaches were proposed:

1. **Shorter-term approach:** The group would concentrate on the analysis of available metrics in the standard to analyse the gaps and understand whether a certain level of trustworthiness can be achieved with minimal work and impact on near-term deployment plans and, hence, not having to modify the current definition of the message structure. The main goal would be to align the main problem statement and the interpretation of the current standards related to positioning and confidence, to highlight if additional available metrics could be used to improve the current situation. This could be considered as a first step which would require an extension of the work to make more extensive usage of the V2X information within the ADAS system thanks to the introduction of additional metrics, if deemed necessary.

2. **Longer-term approach:** According to this option the group would focus directly on a more comprehensive approach which starts from a hazard analysis and risk assessment (HARA) to derive safety goals, similar to what has been done in STiCAD WID [23], and following the same methodology to then define solutions that satisfy the safety goals. This is also linked to the work in the currently open STiCAD [24] WID, which aims at defining a trustable framework between ITS station entities. It is expected to have major implications on the standard.

Considering the timeline required for this work and that the current STiCAD WID is already working on the overall framework from a more comprehensive point of view, it was decided to focus this study on the shorter-term approach, i.e. clear definition of the gaps related to the current standard with reference to position trustworthiness. This can be considered a necessary step to frame follow-up work focusing specifically on the level of trust needed when using the received V2X position information in the ADAS/AD chain, and within a trustworthy framework defined under the new STiCAD WID.

6.2. Defining the architecture

The following architecture is considered as the baseline for discussions related to positioning in the context of this work and follow-up works related to positioning.

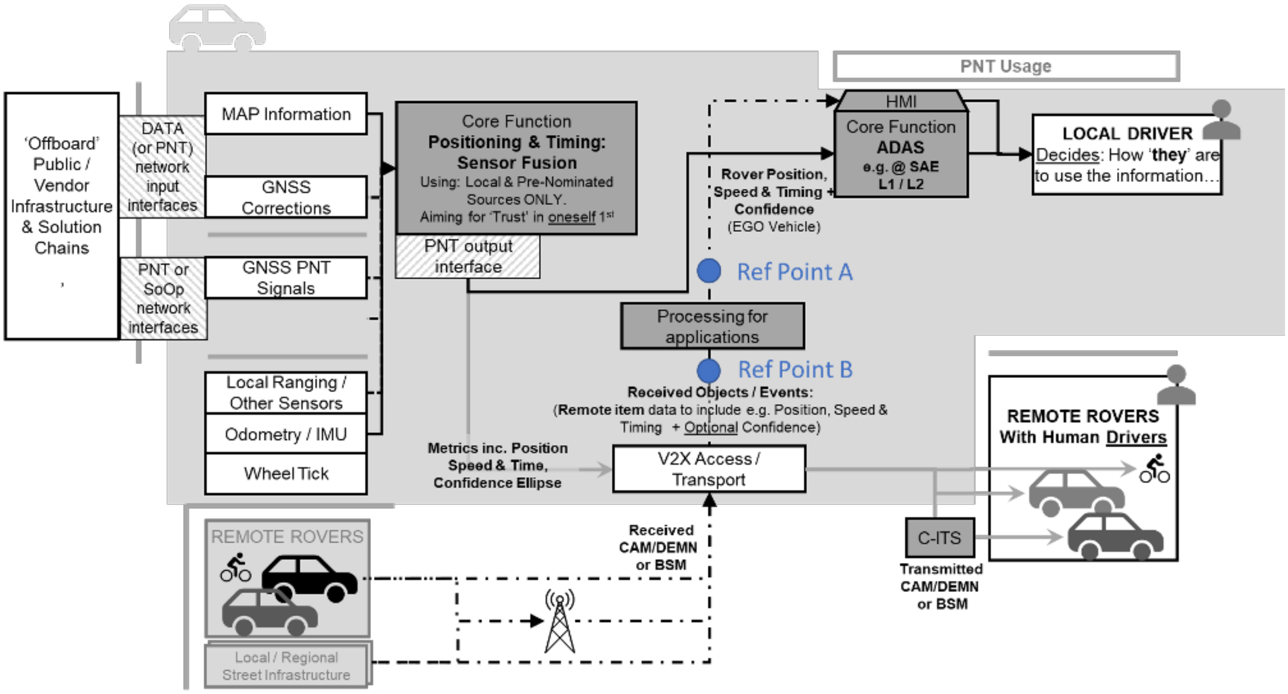


Figure 27. Basic reference architecture

The core PoTi function is responsible for the computation of the positioning and timing information (calculated based on implementation-specific sensors, e.g. GNSS, IMU, wheel tick, local/terrestrial ranging sensors, with the addition of assistance data or PPP/RTK correction services), delivering it to applications that exploit the information locally and also to the V2X protocol stack where the facility layer processes the data to create the V2X message (CAM, DENM, BSM, CPM etc.). The data is delivered to other ITS stations via the V2X access layer. Other ITS stations receive the information and decode the V2X message. We have highlighted a so-called 'processing for application' functionality at the receiver end that processes the data in order to build specific use cases. The information is used either to warn the driver in an HMI or it can be exploited in the ADAS/AD decision stack, depending on the implementation.

Reference point A and B are introduced in this figure and will be referenced when discussing the stakeholder expectations in Section 6.4.1.

6.3. Defining trustworthiness

Several definitions of trustworthiness exist in the literature; however we will offer the generic description found in ISO/IEC5723, [26]: **"Ability to meet stakeholders' expectations in a verifiable way."**

In order to be trustworthy, position information needs to have:

- Clear definition of the requirements, which in the context of positioning can be defined in a generic manner and/or per scenario and/or per application/use case/user story and/or depending on how the information is used in the decision chain (Day 1, Day 2 or beyond)
- Definition of a methodology to verify that the received information meets the requirements.

The characteristics of trustworthiness defined in ISO/IEC 5723 are as follows:

- Accountability
- Accuracy
- Authenticity
- Availability
- Controllability
- Information security
- Integrity
- Privacy
- Quality
- Reliability
- Resilience

- Robustness
- Safety
- Transparency
- Security
- Usability

Considering the definitions of position and confidence information that is provided through the current messages defined in the standard, only a few of the above characteristics are addressed (excluding cybersecurity related characteristics which are out of scope for the current work item):

Accuracy: measure of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true.

Reliability: ability of an item to perform as required, without failure, for a given time interval, under given conditions.

Robustness: ability of the system to maintain its level of performance under a variety of circumstances.

In the context of positioning, a specific notion of integrity is defined in the literature. This differs from the notion of accuracy. The following section provides the definition of integrity and it explains the difference in relation to accuracy.

6.3.1. Definition of integrity

Integrity is one of the Required Navigation Performance (RNP) criteria that a navigation system must achieve or demonstrate, together with e.g. **accuracy, availability, and continuity.** The integrity concept is introduced already in Section 5.1.1 and 5.1.3. Here we propose the definition of integrity that we propose to be used in follow up work in 5GAA.

Integrity refers to the reliability of the position delivered by the positioning systems and measures the confidence a user can place in the correctness of the information supplied by a navigation system. Integrity includes the ability of the system to provide timely warnings to users when the system should not be used by safety-critical applications.

To be more specific, an application with GNSS integrity functionality can configure three required attributes enabling integrity assessments based on information about the position error distribution, the Alert Limit (AL), the Target Integrity Risk (TIR), and the Time To Alert (TTA). The measure of integrity is directly linked to the definition of Protection Level (PL). We use the following definition as a reference (3GPP TS 38.305 [5]):

Protection level (PL) [5]: A statistical upper-bound of the Positioning Error (PE) that ensures the probability per unit of time of the true error being greater than the Alert Limit (AL) and the PL being less than or equal to the AL, for longer than the TTA, is less than the required TIR, i.e. the PL satisfies the following inequality:

Prob per unit of time [((PE>AL) & (PL<=AL) & no Alert) for longer than TTA] < required TIR

Where:

- **Alert limit**: the maximum allowable positioning error such that the positioning system is available for the intended application
- **Time to alert**: the maximum allowable elapsed time from when the error exceeds the bound until an alarm flag must be issued

When the PL bounds the positioning error in the horizontal plane or on the vertical axis then it is called Horizontal Protection Level (HPL) or Vertical Protection Level (VPL), respectively. Note that other components more suitable for terrestrial applications, such as along-track (along the heading) and cross-track (cross-heading), could be considered.

The concept of integrity differs from that of accuracy. Typically, the positioning system reports the distribution of the errors under the form of an error percentile which represents the accuracy. The **A% accuracy of a positioning state is the A-th percentile of all the positioning state errors under specific test conditions**, e.g. 1m accuracy is achieved for 95% of the samples while for 5% of the samples the accuracy is not bounded.

3GPP TR 38.857 [14] explains that each time a position is provided, positioning integrity can be used to quantify the trust on the provided position. Positioning integrity is therefore a method of bounding these errors and this can be done to a much higher level of confidence. For example, a target integrity risk (TIR) of 10^{-7}/hr translates into a 99.99999% probability that no hazardously misleading outputs ([((PE>AL) & (PL<=AL) & no Alert) for longer than TTA]) occurred in a given hour of operation. The PL is a real-time upper bound on the positioning error at the required degree of confidence, where the degree of confidence is determined by the TIR probability.

The integrity information is considered as relevant to ensure reliable position information. However, considering the current version of the standard, the relevant information (Alert, PL, AL, TIR) is not supported by the standard. A follow-up analysis would be required to determine how the concept of integrity could be used in the context of the V2X communication. For example, the PL is real-time bound of the position error, as such, the confidence ellipse data frame 'PosConfidenceEllipse' could be adapted in order to convey information such as PL.

In the following section, an analysis of the gap is provided from the point of view of stakeholder expectations and the metrics based on the definition of trust provided in previous sections and considering the definition of integrity introduced above.

6.3.2. Current definition of confidence

The following figure explains the concept of the confidence ellipse as defined in the current V2X specification reviewed in the previous sections.

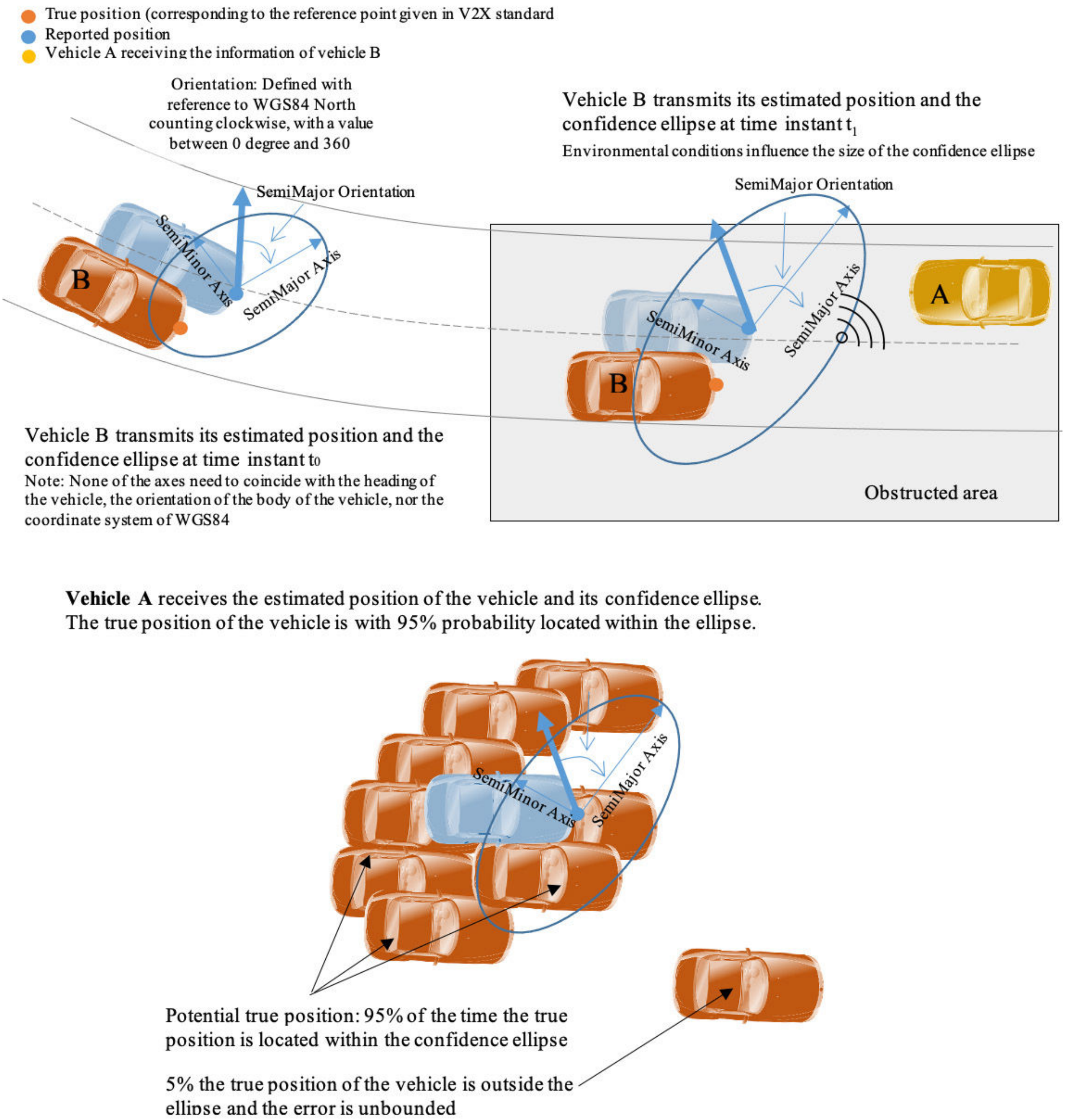


Figure 28. Confidence ellipse depicted.

The horizontal position confidence is described using an ellipse shape, as illustrated in Figure 28. The ellipse is defined by its semi-major and semi-minor axis, and the orientation of the semi-major axis. The 'semiMajorOrientation', is defined by an angle with respect to WGS84 north of the semi-major axis.

Note 1: To prevent fluctuation by 90 degrees of the orientation of the axes, the semi-minor axis is allowed to be larger than the semi-major axis.

Note 2: None of the axes need to coincide with the heading of the vehicle, the orientation of the body of the vehicle, nor the coordinate system of WGS84.

According to Figure 28 the orange vehicle estimates a position at each time instant and reports its absolute position (the blue point in the drawing) as well as the confidence ellipse. The confidence ellipse is computed to guarantee that 95% of the time the true position is located within the confidence ellipse boundary. As such the confidence ellipse is not static information delivered one time, but changes depending on the environment; e.g. it shrinks in the event of favourable conditions, such as good sky visibility, or it may increase in challenging environments (very poor visibility).

The Remote Vehicle (RV, the yellow vehicle A in the figure) receives the estimated position information of vehicle B (Host Vehicle, the blue dot) together with the confidence ellipse. The yellow vehicle knows that with 95% probability the true position of vehicle B is within the confidence ellipse boundaries. However, in 5% of the cases the vehicle B can be located elsewhere.

In the current definition of the standard the confidence metric is the only metric identified directly linked to the definition of trustworthiness.

6.4. Analysing of the gaps

6.4.1. Definition of stakeholder expectations

Typically, the acceptable level of requirements should be defined for each application/ use cases and require a top-down analysis. From that perspective, it is important to minimise the following events every time the position information is updated:

1. The RV is reported to be in the same lane or on the same road as the HV while instead it is located in a different lane or on a different street (false alarm).
2. The RV is reported to be in a different lane or on a different street while instead it is located on the same lane/trajectory as the HV and, hence, it should be reported as a possible collision (error).

This is depicted in the figure below.

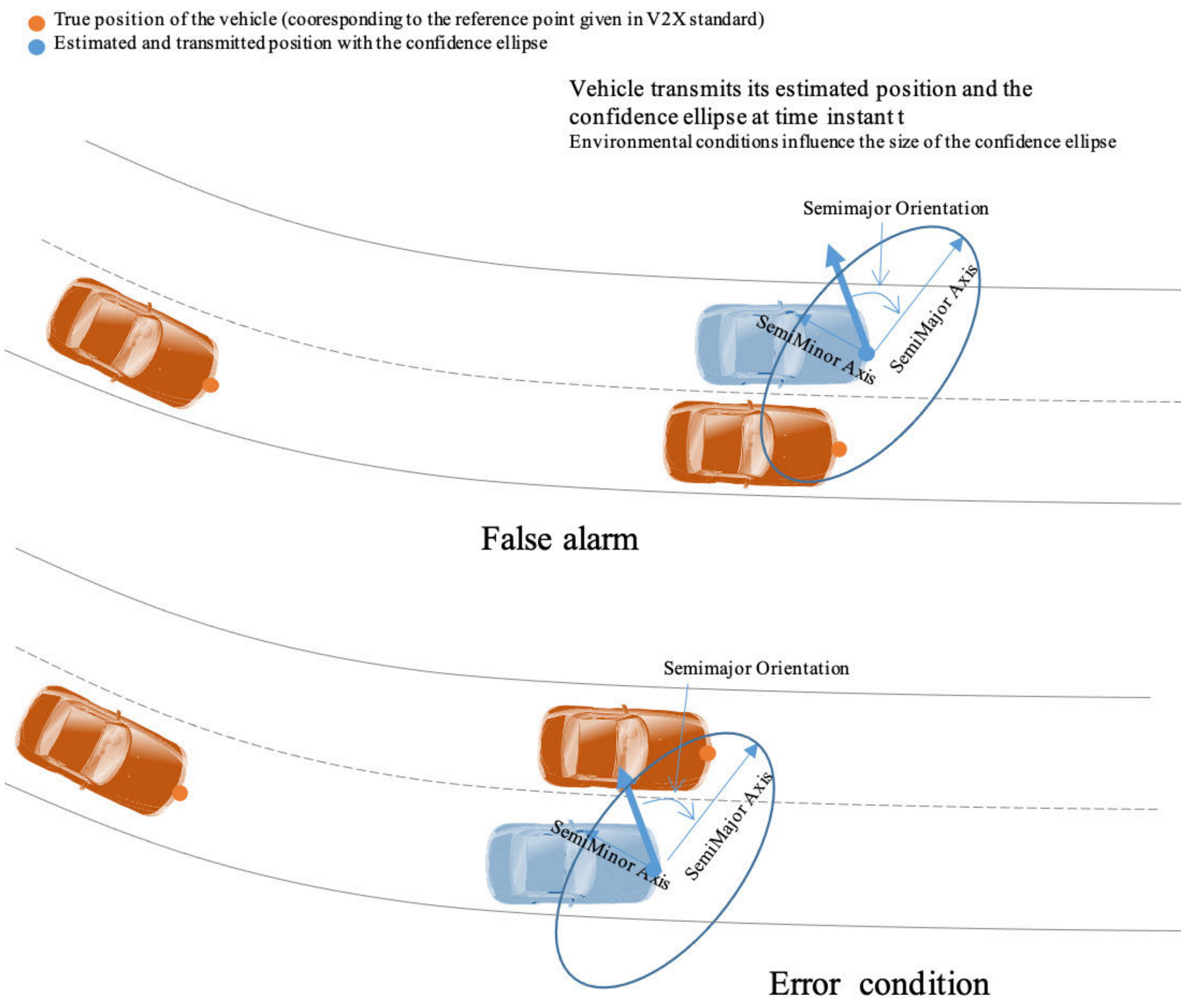


Figure 29. Representation of the false alarm and error condition

These events need to be avoided to minimise the probability of triggering a warning/ manoeuvre when it is not needed or not triggering the warning/manoeuvre when clearly needed. Typically, this is directly linked to the integrity level associated with the position information. Considering the current version of the specification, i.e. no integrity information is available, the requirements associated to false alarm and error probability translates into specific confidence ellipse and confidence level requirements.

Today, the only stakeholder expectations (requirements) we can refer to, are provided in the use case description Technical Report in the form of accuracy requirements [27] for each V2X use case or the minimum requirements in the V2X specification (ETSI, SAE, BSP), or in the 3GPP TR 38.857, [14].

In order to analyse the gap related to stakeholder expectations, a set of example use cases has been selected.

While it is understood that CAM/DENM and BSMs are defined with the main purpose of informing the driver about the presence of other ITS stations or about a danger, it is clear that the information contained in these messages can also be valuable in an automated decision-making process. Moreover, warning the driver because of a possible danger requires a certain level of trust in the information displayed in an HMI. Considering also the complexity of the CPM, the suggestion is to select an initial use case where the position information is critical to deciding a suitable manoeuvre, e.g. Electronic Emergency Break Light (EEBL), obstacle on the road (e.g. stationary vehicle), left-turn assist, blind-spot warning, intersection collision warning, without involving CPM/sensor-sharing which might complicate the discussion. Use cases can be selected following the list in [27].

Table 4. Selected use cases summary

Use Case	User Story	Category	Position Accuracy	Comment
Forward Collision Warning	Warn HV that is on a trajectory to collide with a lead RV that is stopped or moving at a slower speed.	Safety	1.5m @ 99.7% confidence	
Emergency Brake Warning	Alert HV that a lead RV is undergoing an emergency braking event.	Safety	1.5m @ 99.7% confidence	HV needs to know whether the hard braking vehicle in front is in the same lane.
Left-Turn Assist	Assist HV attempting to turn left across traffic approaching from the opposite direction.	Safety	1.5m @ 99.7% confidence	In order to perform lane-accurate positioning, a provisions of around 1 m should be made.
Real-Time Situational Awareness and High-Definition Maps	An autonomous or semi-autonomous vehicle is driving on a road (route), heading towards a road segment, which presents unsafe and unknown conditions ahead. A HV is made aware of situations detected and shared by remote vehicles. Situations may include such things as accidents, weather, traffic, construction.	Safety/ automated driving	0.5 < 5	Typical positioning accuracy to confirm traffic lane. For non-lane-specific information, less accurate localisation is acceptable.

In different use cases, different range, latency, and scenarios are applicable. In the first three use cases, the requested positioning accuracy is 1.5m@3σ, while for the hazardous location warning within the real-time situational awareness use case, the requirement is 0.5m (without indication at which confidence level).

In all the cases the position of the host vehicle and the remote vehicle is important to decide whether a warning should be provided to the driver or, if it is an autonomous vehicle, and whether the vehicle should act upon, i.e. to decide whether the danger is relevant for the HV. For example, in the forward collision warning use case the HV needs to receive an alert when it is on a trajectory that is likely to collide with a lead remote vehicle stopped or moving at a slower speed on a street. As such the position of the remote vehicle is fundamental to decide whether there is a potential risk of collision or not. The service level requirement (SLR) indicates that in order to have sufficiently reliable warning the position accuracy has been set to 1.5m@3σ.

The following gaps and clarifications are identified:

- The SLRs in Table 4 provide the requirements, i.e. "accuracy" with a specific confidence, while the specification allows the exchange of information in terms of the confidence ellipse.
- Several requirements in the SLR master list require a specific accuracy and high level of confidence, while the specification allows only to transmit confidence information at 95% level. There is a **mismatch between what the specification allows to deliver and what the use case requires.**
- This is observed in reference point A in Figure 26. The current requirements defined by 5GAA are defined independently of the technology, and they do not correspond to the requirements at the output of the V2X facility layer.
  - It is understood that the extra processing at the receiver end could compensate for the gap between the information delivered by the V2X message and the requested level of performance for a specific use case.
  - If no extra processing at the receiver is applied, the requirements in the example use cases cannot be achieved with the current specification.
  - The extent of improvement in performance owing to additional processing is implementation dependent and no simulations have been carried out to validate whether the requirements can be achieved or whether additional information is required to be transmitted via the V2X message to achieve these requirements.
- The position requirement is intended as valid at the moment when the use case is triggered, not as an average requirement covering the whole scenario. A requirement of 1.5m@99.7% means that the specific use case requires lane level accuracy, as such it is agreed in 5GAA that this is to be interpreted as an approximation of the ellipse size that this use case would require to work under typical operating conditions.
- The requirement should be interpreted as a "ballpark", not as a minimum requirement.

To deal with these anomalies, it is proposed that

- 5GAA introduces clear requirements in terms of the maximum size of the confidence ellipse at a certain confidence level that needs to be achieved for the use case to work properly (minimum requirement)
- 5GAA derives appropriate requirements that should be satisfied by the V2X technology and not only at the application level
- For advanced use cases (Day 2) the SLR should provide minimum positioning requirements for the application to work properly, while defining the reference usage in the vehicle (e.g. how the V2X information is assumed to

be used in the vehicle when setting the requirements)

- The specification should then adapt to deliver the information and achieve the SLR (e.g. allowing for more granularity in terms of confidence level). Impact in the standard is to be expected.

The requirements in the list in [27] depend on the use cases. Considering that it does not know which use cases the receiver will implement, the transmitter should not stop sending information if the use case-specific positioning requirement is not met. It is the responsibility of the receiver to select which V2X information is used, and when. 5GAA acknowledges that the only reason to stop transmitting is if the positioning information is out of reasonable range (to avoid wasting channel bandwidth). It should be noted that C2C-CC BSP does require that CAM are no longer transmitted if at least one of the 'semiMajorConfidence'/'semiMinorConfidence' axis or 'semiMajorOrientation' is set to "unavailable" or if both confidence ellipses are out of range (RS_BSP_535):

- "Out of range" means > 40.93m (ETSI EN 302 637-2)
- "Unavailable" means, for example, 95% cannot be achieved (ETSI EN 302 637-2) – see annex

5GAA agrees with the general methodology. This work does not discuss the validity of the out-of-range values introduced in the standard.

6.4.2. Existing metrics and testing limitations

Confidence ellipse is the only metric that can be associated to or with trustworthiness considering the current available standard. Other metrics such as 'PathHistory' and 'LaneIdentification' are avenues to contribute to improve the level of trust in the received information.

The following gaps are identified:

- Reporting confidence is not always mandatory in the current version of the specifications. Only the C2C-CC BSP includes confidence as mandatory information, but this is not harmonised across the different standards, e.g. C2C-CC BSP mandates the use of confidence ellipse while SAE requires accuracy but not confidence.
- 'LaneIdentification' and 'PathHistory' fields are not mandatory in all the standards.
- The only specification that provides an implicit definition of the confidence information is the C2C-CC BSP. This does not mandate a way to compute the confidence, allowing for implementation freedom, but gives a common way to interpret the information.
- No test specification is publicly available.
- There is no publicly available methodology to convey the information that the transmitting vehicle has a positioning solution complying with definitions and minimum requirements.

This work item's conclusions are:

- 'SemiMinorConfidence/SemiMajorConfidence' axis should always be present in the V2X message (it could be 'unavailable' or 'out of range').
- 'LaneIdentification' information as well as 'PathHistory' can be easily used in the receiver to verify if consistent information is sent. A best practice is to include 'LaneIdentification' and 'PathHistory'.
- The definition of confidence ellipse should be harmonised, i.e.

  Confidence error bound: Prob (error$_{\text{EPOCH t}}$ ≤Ellipse(semiMinorConfidence/ semiMajorConfidence$_{\text{EPOCH t}}$)) ≥ 95%
- Satisfying the conditions/definitions for every window of length during the test time depends on the parameters/scenario/data set chosen. In particular, samples can be heavily correlated during the 'pPotiWindowTime' (20-120s). The shorter the 'pPotiWindowTime' the higher the number of sensors that should be used in order to ensure robust samples are collected during the window and, hence, mitigate the effects of error bursts occurring because of specific environmental and driving conditions.
- It is proposed to consider the following guiding principle
  - make sure that the methodology to verify the correctness of the definition is according to a repeatable process (e.g. using a set of recorded data)
  - consider a window length that contains enough independent samples (e.g. 200s could be considered as a valid approach)
  - As it is recognized that pPotiWindowTime length (20s to 120s) might have been chosen in a way to comply with specific use cases, an alternative proposal is to allow for some tolerance in fulfilling the definition above (i.e. the definition should be valid up to e.g. 95% of the time windows).
- The maximum 'semi-MajorConfidence/semiMinorConfidence' performance requirement would be considered as a performance metric, but not as a definition of the confidence (i.e. **Prob (semiMinor/ semiMajorConfidence$_{\text{EPOCH}}$ ≤ C$_{\text{scenario}}$) ≥ 95%**). This can be defined by specific profiles if deemed necessary.

Considering the constraints agreed on by the group to avoid having to modify the standard at the start, this work item decided to publish a best-practice paper that indicates how the transmitting vehicle should behave.These conclusions were briefly presented to OEM group to collect feedback, which is summarised in the following Section.

6.5. Feedback from OEMs

6.5.1. Feedback on confidence metrics

Feedback related to the TPM4V2X questions, as provided by OEMs are given below.

- **Question 1: Is the position confidence parameter, introduced in the CAM/DENM and BSM message, used in current (or near future) deployments to discriminate whether the position indicated in the message is valid for the final application?**

Answer 1:

The position confidence parameter is currently used and will play a role in future use cases but cannot be decoupled from the required position accuracy.

For different use cases, the position confidence is required in a different range. Some require high, while others may work with less accuracy in terms of the vehicle itself, but also the information received from other vehicles. The higher the accuracy, however, the more effective the use cases would be. Certain use cases can use the position confidence to discriminate whether positions in the messages are valid for them.

Use cases with short distance actions require a much higher certainty and much higher precision, while other use cases can work with less localisation precision

Answer 2:

It is mandatory for a V2X device to send a position in its CAMs which is inside its 95% confidence ellipse using a *sliding window. See for example, RS_BSP_202, RS_BSP_200, RS_BSP_429 in the below document.*

https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.2/C2CCC_RS_2037_Profile.pdf

Thus on the receiving side, this behaviour can be expected by the applications.

It is also assumed that if the confidence ellipse does not match, no CAM/BSM is sent out from the V2X device of the concerned RV.

Answer 3:

Always and for all applications.

A message or a packet without an estimated confidence is just spam.

Answer 4:

Company X has not looked into this feature yet. We plan to use CAM/DENM and BSM messages via PC5 from 2025. We are currently at the architectural level. It is worth noting that we do plan to add a confidence measurement system. Log a message (stationary vehicle), vehicle recognises that the message was correct (camera data), log findings in Company X cloud. Some use cases cannot be confirmed. For example, slippery road. If Company X receives a slippery road message, Company X will carry out powertrain adjustments to prevent the car from slipping at the same place, with or without the customer knowing. Thus, it would not be possible to verify a slippery road when the vehicle has taken mitigation action. The idea of the confidence process is to give ADAS proof that the data is valid and if they are not using the information that is being shared, we would have to ask the question as to why. It has *value. The second reason is to use this data to push back suppliers with low ratings. Demand improvement etc. The third reason is to allow the vehicle to actively switch off and on use cases that have poor confidence ratings. Reducing false positives et al. We would like to use the confidence parameter to do this but can work without it if we need.*

- **Question 2: By what standard means is the confidence interpreted at the receiver?**

Answer 1:

Interpretation of confidence: a percentage value … from a distribution within an area, where an ellipse defines the area that contains that percentage value of samples.

Answer 2:

The interpretation is partially covered by the aforementioned document (see question 2), but EN 302 890-2 should also be used/referenced, where e.g. '6.3.1 General requirements related to confidence' deals with this topic.

https://www.etsi.org/deliver/etsi_en/302800_302899/30289002/02.01.01_20/en_30289002v020101a.pdf

Answer 3:

As an estimated error or a zone (ellipse) where the object or the event is realistically located.

A 'circular' ellipse for a supposedly moving object is considered as highly suspect.

Answer 4:

We have not started to look into this in detail. We assumed it did not exist and started to look at a bespoke solution for Company X. But we are happy to use this feature when available.

I am not able to answer this question because we do not currently have any standard means at this time.

6.5.2. Additional feedback

The following provides the questions that have been asked to the OEM group as well as the answers.

1. **Do you think that a best practices paper published by 5GAA influencing how the transmitter should behave, or could be useful in a first step to harmonise the way the information is introduced?**
    a. **Assuming that the confidence information is always transmitted with the V2X message, do you think that harmonising the definition of confidence across the standards (worldwide) is a useful step to unify the interpretation of this parameter at the receiver end ?**

Answer: OEMs agree that a best practices paper is a good idea, however this must come with some guidance. They all agreed that the definition of confidence should be understood in the same manner. The suggestion was to look into the work done in Car 2 Car regarding best practices.

2. **Do you think that the introduction of a conformance testing approach for the verification of the confidence ellipse information (related to the positioning) is necessary to guarantee that the definition/ requirements are met?**
   a. **Do you think that there is the need to have a third party that certifies the positioning solution?**

Answer: OEMS agree that certification is not wanted nor needed if the requirements are well defined and tested via self-testing. Instead of certification, the work should look into a wider framework to have the certification on a higher level. Moreover, it was clarified that OEMs do not believe that automotive certification in the form of 'type approval' is needed, however the positioning information cannot be treated in isolation, and therefore an overarching conformance assessment scheme may be preferable (such as described by WG3 or Omniair).

6.6. Discussing next steps

This section considers areas to further explore and as potential follow-up works.

(a) Test methodologies, such as those defined in [6] and [7], could be considered as a reference and analysed in more detail to evaluate their relevance and reusability if a conformance assessment scheme is introduced, which includes the positioning solution.

(b) This document considers only Day 1 use cases and basic messages. More analysis is needed to extend this to more advanced use cases and message types, such as Day 2 scenarios or elaborated use cases, collective perception messages, vulnerable road user protection messages, etc.

(c) Additional metrics to those highlighted in this document could increase the level of trust; as such, they could be analysed and developed with simulations to demonstrate the additional benefit for each new proposed metric and associated KPIs to identify trustworthiness. For example, this document has reviewed the concept of integrity. The integrity information is relevant to ensure reliable and trustworthy position information. However, relevant information such as Alert, AL, TIR, PL, are not currently supported by the standard. A follow-up analysis would be required to determine how the concept of integrity could be used in the context of the V2X communication in order to guarantee trustworthy position information. The PL is real-time bound of the position error. As such, the confidence ellipse data frame 'PosConfidenceEllipse' could be adapted to convey PL and related information. The use of an integrity concept would require modification of the V2X message data structure.

(d) Other methodologies to increase the trust ascribed to the received information could be considered. Examples are provided in the following section.

6.6.1. Examples of alternative methodologies to increase the trust at the receiver for further study

Initial trust is established by the V2V system in that each vehicle has a digital signature. All vehicles have a list of trusted signatures which are periodically updated through a central database. In addition, misbehaviour detection mechanisms are in place to identify vehicles known to be misbehaving, and thereafter revoke their certification. This makes it more difficult to spoof the system intentionally, thereby increasing trust.

While this provides a basic system of trust, there needs to be other methods to establish a higher level of trust between two vehicles before making a potentially life-threatening decision. As described in the rest of the TR, one way of increasing trust is to demand confidence information be added to the CAM/BSM/DENM message. Another way is to verify specific information contained within the messages sent. As stated before, initial trust is established in exchanging V2X certificates. The next level of trust could be established by verifying the validity and coherence of that information. There are several ways in which this can be implemented.

Areas for further study include the use of different technologies and techniques to validate the information received via V2X. This includes:

- On-board sensors: vehicles can carry out an internal sensor fusion to detect surrounding objects and determine their position in relation to the vehicle. This information could be correlated with the position obtained via V2X.
- Infrastructure-based sensors: infrastructure equipped with sensors (e.g. radar, lidar, cameras) could be used to validate accurate positioning information (similar to sensor fusion inside an automobile) to identify objects enroute. Areas for further study would again include correlating objects from the sensor fusion with V2V positional information. However, with infrastructure, one solution could be to have sensors in tolling booths. As a vehicle passes under the toll system, it checks the V2V information transmitted and then provides feedback on the accuracy of that information. The accuracy could also be recorded in a central database.
- V2V-based information: this data coming from several ITS stations could be used to detect the plausibility of the received information (e.g. distinguishing if/when two independent ITS stations place two vehicles in the same position).
- Wireless-based location detection: vehicles could use wireless technology (e.g. 3GPP sidelink, Bluetooth/WiFi or Ultra-wideband) to enable location measurements. This can be considered as another method to establish trust. Here, an RF link establishes a two-way distance measurement session to establish the position between two nodes. RF links have the benefit that both vehicles are involved in the transaction and, thereby, establish mutual trust (in both directions). The RF link examples (SL, Bluetooth/WiFi, and UWB) are further addressed below.

6.6.1.1. Wireless-based location detection

The 3GPP sidelink provides methods for carrying out distance measurements between base stations and the UE. In Release 17, the target accuracy is <1m. This is based on

3.5GHz operation (band n77) and 100 MHz bandwidth (3GPP TR 38.857 [14]). Essentially, the process is to issue a request to the positioning system to determine the distance from the base station. The base station then provides a position reference signal (PRS) to the UE. The UE in return provides an SRS positioning signal. The positioning server then uses the resulting measurements to compute and provide the distance back to the client. Information from three base stations is required to triangulate a position. If all of the conditions are met, then the 5G system can determine the UE location. Sidelink positioning based on the V2V link is preferred when the bandwidth is above 10MHz, for greater accuracy. Even at 10MHz bandwidth the position coupled with angle of arrival may be able to determine if a vehicle is in the approximate position indicated, which may be enough to enhance trust. The 3GPP Release 19 work related to sidelink positioning is still ongoing.

Bluetooth is also referenced in 3GPP 37.355 as an additional technology that can be used to establish location. Bluetooth can provide accuracy <10m. The 3GPP specification provides an interface to Bluetooth devices and beacons to provide positioning measurements.

Ultra-wide band [27] is another technology that can be used in the automotive industry to measure the distance between two objects. The technology can provide ranging accuracy at the decimetre level. Different topologies exist, however in all the cases a peer-to-peer communication needs to be established in order to compute the distance between two points. With double-sided two-way ranging (DS-TWR), UWB can specifically provide distance measurements between two points. In addition, there are cryptographic techniques used to ensure the distance measurement is highly secure to avoid any chance of being spoofed. A key factor in proving a high level of security, as outlined in [27], is a scrambled time stamp (STS). The STS provides a randomised key to make the PHY transmission less predictable, and reduces the chances of an external spoofer being able to manipulate distance readings. The receiver needs a copy of the sequence locally before the start of the reception.

In order to establish a connection between two UWB devices a new interface could be introduced to provide UWB management services via V2V link. V2V systems have a protocol for creating a group of vehicles and then starting communications among the group. Once the group is set up, then the UWB session could be started. The V2V system would identify the nodes on each vehicle that need to be involved in the point-to-point distance measurement, set up the session parameters/keys and start the ranging exchange. Once the UWB session is started, the ranging information could be provided to improve the performance of the localisation function or to correlate it with the information received via V2X message.

More information would be needed to determine orientation as well as the location of the four corners of the vehicle. One way to explore this in the next steps is to provide two sensors on each surface. This allows a crossbar operation enabling not only precise positioning but also relative orientation. See [31] for more details.

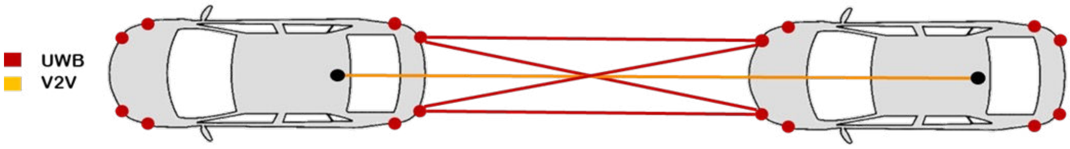


Figure 30. Sensors location.

There are many other use cases where more complex interactions are needed. Also, UWB anchors can be located at various points along the infrastructure allowing a vehicle to periodically validate its precise location. UWB systems are fast enough, capable enough and future-proof enough to meet even complex interaction scenarios.

As cooperative driving accelerates, the UWB sensor can improve the system capabilities with precise distance measurements. These measurements are bidirectional in that both ends know the position and orientation of each other. This, in turn, establishes the trust needed in a V2V information exchange. While the value of such a UWB + V2X system goes beyond establishing trust, the simple benefit of establishing it is enough to justify such a system.

7. Conclusions

Establishing trust is a critical component of any transaction and when decisions should be made based on the information exchanged. In particular, when we consider the V2X technology, status information or information about a danger or objects in the surroundings of the vehicle is exchanged via the use of specific messages (CAM/DENM/CPM/BSM). This data is used to warn the driver (for example via a display, HMI) or to suggest to drivers specific manoeuvres or apply them directly in the case of an autonomous vehicle. If the information exchanged is not trustworthy this could have potentially serious consequences, ranging from irritating the driver to dangerous accidents. Of particular importance is the information related to the position of the transmitting vehicle as well as the detected danger, surrounding objects, etc.).

This work focuses on the positioning information exchange. In particular, we have focused on initial Day 1 use cases and basic messages such as CAM, DENM or BSM, and we have analysed the current specification from different regions with the scope to highlight whether a certain level of trust can be achieved at the receiver end upon reception of the position information via theV2X message transmitted by a remote vehicle.

The following was identified:

- The definition of trustworthiness considered in this TR, as offered in [26]: “Ability to meet stakeholders’ expectations in a verifiable way.” This requires clear definition of the requirements and the definition of a methodology to verify that the received information meets the requirements.
- The definition of integrity issued in this TR is also a relevant metric for trustworthiness, however it is not supported in the current version of the standard, thus requiring some modifications in the definition of the messages. Currently, confidence information is the most important metric to ensure a certain level of trust in the received information.
- The definition of the confidence metric has been explained in detail in the TR, and covers issues such as:
  - Requirements to handle false alarms, errors, and confidence information relevant to stakeholder expectations, and not only in terms of accuracy.
  - The SLRs in the master-list [27] provide requirements at the application input level and they are defined independently of the technology; moreover, they do not correspond to the requirements at the output level (the V2X facility layer).
  - Additional work is required to match the application-level requirements with requirements that should be satisfied by the V2X technology.
  - The position requirement in the master-list [27] should be interpreted as an approximation of the ellipse size this use case would require to work in typical conditions.

    - This TR proposes
        - 5GAA introduces clear requirements in terms of the maximum size of the confidence ellipse at a certain confidence level needed to be achieved for the use case to work properly (minimum requirement)
        - Derive requirements that the V2X technology should satisfy
        - Clarify the definition of accuracy requirements in the use cases list [27]
        - For advanced use cases (Day 2 use cases) a reference usage of the position information should be considered for the definition of the requirements

- As to metrics:
    - In the current version of the standard the 'confidence ellipse' information is the fundamental metric that can be used to measure the trustworthiness of the information.
    - Other metrics such as 'PathHistory' and 'LaneIdentification' can also help to improve the level of trust in the received information.
    - This TR proposes that:
        - 'SemiMinorConfidence/SemiMajorConfidence' axis should always be present in the V2X message (it could be 'unavailable' or 'out of range')
        - 'LaneIdentification' information as well as 'PathHistory' can be easily used in the receiver to verify if consistent information is sent. The 'LaneIdentification' field could be considered as redundant information because the 'PathHistory' provides a set of point that can be used in the receiver to identify whether the new position is consistent. Nevertheless, a best practice is to always include 'LaneIdentification' and 'PathHistory'
        - The definition of confidence ellipse should be harmonised following [22]
        - It is proposed to follow specific principle in order to complete the methodology and verify the definition of confidence, as defined in Section 6.5.1.
- Feedback from OEMS has clarified that confidence information is fundamental, and that in the longer term a conformance assessment scheme could be considered.

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

5GAA
Automotive Association

in