3GPP TSG-RAN WG2 Meeting #113-e***R2-2102092 [DRAFT]***

Electronic, Jan 25 – Feb 05, 2021

**Agenda item:** 8.11.3.1

**Source:** Swift Navigation

**Title:** [AT113-e][601][POS] – Integrity Text Proposal

**Document for:**  Discussion, Agreement

# 1. Introduction

This is the text proposal resulting from the following email discussion:

 **[AT113-e][601][POS] Integrity text proposal (Swift)**

Scope: Continue discussion of the remaining open issues on integrity, taking into account contributions to agenda items 8.11.3.1 and 8.11.3.2, and develop an agreeable text proposal

Intended outcome: Updated TP

Deadline:  Tuesday 2021-02-02 1200 UTC

This TP should be reviewed alongside the Moderator Summary in [1].

# 2. Conclusion

**Proposal 1: Agree to adopt the text proposal as baseline for TR 38.857.**

# 3. References

[1] Moderator Summary [AT113-e][601][POS] Integrity TP (Swift), [https://www.3gpp.org/ftp/tsg\_ran/WG2\_RL2/TSGR2\_113-e/Inbox/Drafts/%5BOffline-601%5D%5BPOS%5D%20Integrity%20TP%20(Swift)/Moderator%20Summary%20and%20TP](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_113-e/Inbox/Drafts/%5BOffline-601%5D%5BPOS%5D%20Integrity%20TP%20%28Swift%29/Moderator%20Summary%20and%20TP)

# 4. Text Proposal

*Start of Text Proposal*

# 2 References

[1] 3GPP TR 22.872: “Study on positioning use cases”.

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] RP-202094: "Study on NR Positioning Enhancements".

[4] 3GPP TR 38.855: "Study on NR Positioning (Release 16)".

[5] R2-2006541, TP for Study on Positioning Integrity and Reliability, Swift Navigation, Deutsche Telekom, u-blox, Ericsson, Mitsubishi Electric, Intel Corporation, CATT, UIC.

[6] Zhu, N., Marais, J., Betaille, D., Berbineau, M., “GNSS Position Integrity in Urban Environments: A Review of Literature”, IEEE Transactions on Intelligent Transportation Systems, Vol. 19, No. 9, Sep 2018.

[7] European Space Agency, “Integrity”, Navipedia, 2018, <https://gssc.esa.int/navipedia/index.php/Integrity>.

[8] Reid, T., Houts, S., Cammarata, R., Mills, G., Agarwal, S., Vora, A., Pandey, G., “Localization Requirements for Autonomous Vehicles,” SAE International Journal of Connected and Automated Vehicles, Vol. 2, No. 3, pp. 173–190, Sep 2019.

[9] GSA-MKD-RD-UREQ-250283, “Report on Road User Needs and Requirements: Outcome of the European GNSS’ User Consultation Platform”, Issue/Rev: 2.0, 2019.

[10] GSA-MKD-RL-UREQ-250286, “Report on Rail User Needs and Requirements: Outcome of the European GNSS’ User Consultation Platform”, Issue/Rev: 2.0, 2019.

[11] 5GAA, “White Paper – C-V2X Use Cases Methodology, Examples and Service Level Requirements, 2019.

[12] Global Positioning System Wide Area Augmentation System (WAAS) Performance Standard, Department of Transportation USA, Federal Aviation Authority, Edition 1, October 2008.

[13] International Civil Aviation Organization, “Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications: International Standards and Recommended Practices”, 2006.

[14] RTCA DO-178C, “Software Considerations in Airborne Systems and Equipment Certification,” 2011.

[15] DO-229D, RTCA, "RTCA DO-229D Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment," 2013.

[16] SAE J3016, “Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems”, SAE International, 2018.

[17] 3GPP TS 33.501, “Security architecture and procedures for 5G system”.

[18] European GNSS Agency, “GNSS User Technology Report issue 3”, 2020.

[19] Air Force Research Laboratory, “IS-AGT-100 Chips Message Robust Authentication (Chimera)”, 2019.

[20] 3GPP TR 22.804, “Study on Communication for Automation in Vertical Domains”.

[21] 3GPP TS 38.305, “Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN”.

[22] 5G ACIA White Paper, "5G for Automation in Industry: Primary use cases, functions and service requirements", July 2019.

[23] Working Group C (WG-C), “EU-U.S. Cooperation on Satellite Navigation”, ARAIM Technical Subgroup, Interim Report, Issue 1, December 2012.

[24] EGNOS Open Service (OS) Service Definition Document, European Commission, Version 2.3, 2017.

[25] Elliott D. Kaplan, Christopher J. Hegarty, “Understanding GPS/GNSS Principles and Applications” Third Edition, Artech House, 2017.

*Next Text proposal*

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

**Positioning Integrity:** A measure of the trust in the accuracy of the position-related data provided by the positioning system and the ability to provide timely and valid warnings to the LCS client when the positioning system does not fulfil the condition for intended operation.

**Integrity Availability:** The integrity availability is the percentage of time that the PL is below the required AL.

**Feared Event:** Feared Events are considered to be all possible events (e.g., of natural, man-made, systemic or operational nature) that can cause the computed position to deviate from the true position, regardless of whether a specific fault can be identified in one of the positioning systems or not.

**Target Integrity Risk (TIR):** The probability that the positioning error exceeds the Alert Limit (AL) without warning the user within the required Time-to-Alert (TTA).

NOTE: The TIR is usually defined as a probability rate per some time unit (e.g., per hour, per second or per independent sample).

**Alert Limit (AL):** The maximum allowable positioning error such that the positioning system is available for the intended application. If the positioning error is beyond the AL, the positioning system should be declared unavailable for the intended application to prevent loss of positioning integrity.

NOTE: When the AL bounds the positioning error in the horizontal plane or on the vertical axis then it is called Horizontal Alert Limit (HAL) or Vertical Alert Limit (VAL) respectively.

**Time-to-Alert (TTA):** The maximum allowable elapsed time from when the positioning error exceeds the Alert Limit (AL) until the function providing positioning integrity annunciates a corresponding alert.

**Misleading Information (MI):** An MI event occurs when, the positioning system being declared available, the positioning error exceeds the PL.

**Hazardous Misleading Information (HMI):** An HMI event occurs when, the positioning system being declared available, the positioning error exceeds the AL without annunciating an alert within the TTA.

**Integrity Event:** An Integrity Event occurs when the positioning system outputs HMI.

## 3.2 Symbols

## 3.3 Abbreviations

**AL Alert Limit**

**HAL Horizontal Alert Limit**

**HMI Hazardously Misleading Information**

**HPL Horizontal Protection Level**

**MI Misleading Information**

**PE Positioning Error**

**PL Protection Level**

**TIR Target Integrity Risk**

**TTA Time-to-Alert**

**VAL Vertical Alert Limit**

**VPL Vertical Protection Level**

*Next Text proposal*

9 Positioning integrity and reliability

9.1 Integrity Overview – Background Information

### 9.1.1 Integrity Concepts

The ability to navigate safely means users must trust their estimated position with a high degree of confidence. The trustworthiness of position estimates is the study of positioning integrity, which is adapted from TR 22.872 [1] as follows:

**Positioning Integrity:** A measure of the trust in the accuracy of the position-related data provided by the positioning system and the ability to provide timely and valid warnings to the LCS client when the positioning system does not fulfil the condition for intended operation.

Positioning integrity monitoring[[1]](#footnote-1) is already supported by GNSS service providers, but there is no standard for expanding the ecosystem of connected devices which can benefit from positioning integrity. This study investigates new integrity assistance data and procedures to be considered in LPP and associated specifications, to assist in quantifying positioning integrity for the positioning system.

#### 9.1.1.1 Accuracy and Integrity

To understand the necessity of introducing the concept of positioning integrity, it is important to understand how it differs from the more familiar concept of Accuracy.

Positioning accuracy and positioning integrity are related but separate concepts, and for many use cases, accuracy alone is insufficient to meet the requirements. Positioning devices and services are typically designed to report the distribution of errors that characterize the overall system performance, which is often specified as an error percentile representing the accuracy. For example, a road vehicle with an embedded UE positioning client may report a lane-level accuracy of <50cm 95th percentile. In this case, the UE is indicating that, based on all the computed positions, its estimated accuracy is better than 50 cm, 95% of the time. For the remaining 5%, the position error is unknown. In fact, these errors might reach 10s or 100s of meters due to multiple different error sources. The 5% of errors are essentially unbounded without any way to reliably validate their distribution. In the case of GNSS, these errors could include constellation geometry (i.e., Dilution of Precision), sharp atmospheric gradients or irregularities, and local receiver effects such as high measurement noise or multipath.

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 confidence. For example, a Target Integrity Risk (TIR) of 10-7/hr translates to a 99.99999% probability that no hazardously misleading outputs occurred in a given hour of operation. The TIR sets the target for determining which feared events need to be monitored in order to meet the specified Alert Limit (AL) at this level of probability. A lower TIR introduces a wider range of threats (i.e., feared events) that need to be monitored to improve confidence in the estimated position. Erroneous position estimates which do not meet the positioning integrity criteria can then be omitted in the final positioning solution, allowing only the valid position estimates to be utilized, which also leads to higher accuracy.

#### 9.1.1.2 Integrity Key Performance Indicators (KPIs)

The following KPIs for positioning integrity are defined for the study:

**Target Integrity Risk (TIR):** The probability that the positioning error exceeds the Alert Limit (AL) without warning the user within the required Time-to-Alert (TTA).

NOTE: The TIR is usually defined as a probability rate per some time unit (e.g., per hour, per second or per independent sample).

**Alert Limit (AL):** The maximum allowable positioning error such that the positioning system is available for the intended application. If the positioning error is beyond the AL, the positioning system should be declared unavailable for the intended application to prevent loss of positioning integrity.

NOTE: When the AL bounds the positioning error in the horizontal plane or on the vertical axis then it is called Horizontal Alert Limit (HAL) or Vertical Alert Limit (VAL), respectively.

**Time-to-Alert (TTA):** The maximum allowable elapsed time from when the positioning error exceeds the Alert Limit (AL) until the function providing positioning integrity annunciates a corresponding alert.

**Integrity Availability:** The integrity availability is the percentage of time that the PL is below the required AL.

The relationship between the KPIs and the Protection Level (PL), and their impacts on the positioning solution are further examined below.

#### 9.1.1.3 Integrity Protection Level (PL)

The Protection Level (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 PL is defined as follows:

**Protection Level:** The PL is a statistical upper-bound of the Positioning Error (PE) that ensures that, the probability per unit of time of the true error being greater than the 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)) for longer than TTA] < required TIR**

NOTE: 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: A specific equation for the PL is not specified as this is implementation-defined. For the PL to be considered valid, it must simply satisfy the inequality above.

The PL is used to indicate the positioning system availability, as when the PL is greater than the AL, the system is considered unavailable (see Stanford Diagram below). The PL establishes a more rigorous upper bound on the positioning error by taking into consideration the additional feared events which have a lower occurrence (i.e., lower TIR) compared to the nominal events considered in the standard accuracy estimate alone. The lower the TIR, the more feared events that need to be considered.

Fault feared events are those which are intrinsic to the positioning system and typically caused by the malfunction of an element of the positioning system (e.g., constellation or ground network failures). Fault-free feared events occur when the positioning system inputs are erroneous, but the event is not caused by a malfunction of the positioning system. In the GNSS context for example, fault-free feared events include nominal effects experienced every day such as poor satellite geometry, larger atmospheric gradients, and signal interruption, all of which can degrade positioning performance without causing the system to fail. A common limitation of existing industry functional safety standards, as summarized in [5], is that only the fault conditions are considered. In practice, however, the fault-free conditions also have a material contribution to the total integrity risk budget and must therefore be monitored.

The PL is necessary to ensure all potential faults and fault-free events down to the required TIR are considered. It bounds the tails of the distribution with higher certainty (per unit of time) and provides a measure for ensuring only those positions whose positioning integrity has been validated within the TIR are included in the final positioning solution. By contrast, the standard accuracy estimate only considers a subset of feared events up to a nominal percentile (e.g., 2-sigma, 95%), based on the entire distribution of estimated position errors.

#### 9.1.1.4 Relationship between the PL and KPIs

The TIR is a design constraint for a positioning system and represents the probability that a positioning error exceeds the AL, but the positioning system fails to alert the user within the required period of time (i.e., TTA). In practice, the TIR is very small. For example, <10-7/hr TIR translates to one failure permitted every 10 million hours (equivalent to 1142 years approximately).

Positioning integrity system failures are known as Integrity Events and integrity events occur when the positioning system outputs Hazardous Misleading Information (HMI). HMI occurs when, the positioning being declared available, the actual positioning error exceeds the AL without annunciating an alert within the required TTA. Misleading Information occurs when, the positioning system being declared available, the actual positioning error exceeds the PL. Typically, positioning systems are designed to tolerate some level of MI, provided the system can continue to operate safely within the AL. To properly monitor for integrity in the positioning system, both the fault and fault-free conditions which potentially lead to MI or HMI need to be characterized for the network and the UE.

Figure 9.1.1.4-A illustrates the concept of MI and HMI with respect to the KPIs, PL and PE.

 

**Figure 9.1.1.4-A:** Relationship between Positioning Error (PE), Protection Level (PL), Alert Limit (AL), MI and HMI [6].

A useful representation for interpreting the relationship between the positioning integrity KPIs and PL is the so-called Stanford Diagram [7] in Figure 9.1.1.4-B. It should be noted that the Positioning Error (PE) in this diagram is the difference between the true position and the estimated position, computed by the positioning device. In practice, the true position is not known.



**Figure 9.1.1.4-B:** Stanford Diagram for integrity events, adapted from [7][8].

Important observations can be made from Figure 9.1.1.4-B in the context of this study:

1. The conditions represented above the diagonal line (Nominal Operations, System Unavailable) mean the positioning system is operating as intended by correctly detecting when the system should or should not be available.
2. The conditions represented below the diagonal line mean the system is not operating as intended. These conditions are what the positioning integrity system is designed to protect against, i.e., by monitoring the necessary fault and fault-free events to protect against MI or HMI for a given TIR. This concept is further described:
	* The TIR is equivalent to the probability per unit time of HMI, corresponding to the red block in the Stanford Diagram. The rate of MI (corresponding to the orange region), while undesirable, does not contribute towards the TIR.

In practice, positioning integrity systems are designed to tolerate some level of MI or HMI for a period of time within the TTA, without exceeding the TIR. This framework underpins the PL definition in this study (Section 9.1.1.3) and is particularly important for systems with communication latency, such as 3GPP NR, given assistance data can be monitored and sent by the network (i.e., the basis of this study). Sufficient time is therefore needed to signal that a fault is present. There is nothing prohibiting the TTA being set to zero for instantaneous detection, however a grace period must be accommodated to allow some level of functionality to be offloaded to the network when the network is utilized. Hence, the TTA depends on the overall positioning integrity system design (including 3GPP and non-3GPP elements) and is specified by the positioning system owner (e.g., a vehicle manufacturer) alongside the TIR and AL.

1. Interpretations when the system is **available** (PL<AL):
* **Nominal Operations (PE<PL):** the solution is available and operating safely without an integrity event.
* **Misleading Information (PE>PL & PE<AL):** the solution is available but contains an MI integrity event due to PE>PL. It is still operating safely given PE does not exceed the AL.
* **Hazardous Misleading Information (PE>PL & PE>AL):** the solution is available but contains an HMI integrity event due to PE>AL. It is still declared safe (PL<AL) when it should not have been.
1. Interpretations when the system is **unavailable** (PL>AL):
* **System Unavailable, False Alert (PE<PL & PE<AL):** the solution is unavailable but is a false alert integrity event, given PE<AL.
* **System Unavailable (PE<PL & PE>AL):** the solution is unavailable and operating as intended without an integrity event given PE>AL was properly detected.
* **System Unavailable and Misleading (PE>PL & PE>AL):** the solution is unavailable and contains a MI (PE>PL) integrity event.

## 9.2 Use Cases

RAT-Independent GNSS positioning integrity monitoring has a long operational history in the field of civil aviation [12][13][14][15]. The positioning integrity framework examined in this study extends beyond aviation, to address a broader suite of use case and architectural considerations for the 3GPP system. These concepts are further illustrated by the use case descriptions and KPIs provided below, including a particular focus on safety-critical and liability-critical applications, requiring the capability to validate the estimated position with greater trust.

### 9.2.1 Automotive

#### 9.2.1.1 Road-Level Identification and Road-User Charging

Positioning integrity is a key input to determining whether a road vehicle is traveling on a highway or a neighbouring access road (e.g., a collector-distributor lane). For example, consider a manufacturer wanting to ensure their Advanced Driver-Assistance Systems (ADAS) only activates when the vehicle is on a highway. This requires the UE to determine with a high degree of positioning integrity which road the vehicle is traveling on, in order to avoid the potential for unintended ADAS functionality on the access road (or conversely to ensure the appropriate functionality has been activated on the highway). The road vehicle may also be subject to road-user charging with fees that vary depending which road is used, also requiring positioning integrity validation.

Consider an access road that is within 3 metres of a freeway, with a corresponding AL of 3 metres and TIR of 1 x10-7/hr specified by the vehicle manufacturer. The road vehicle connects to a positioning integrity service provider via the mobile network to request UE-Based positioning integrity assistance data. The assistance data is applied by the UE alongside its local positioning measurements in order to compute the real-time PL. So long as the PL remains below the AL, the positioning system is available and functioning as intended, and the road-level identification can be made safely. If the PL exceeds the AL, the impacted positioning system should be declared unavailable on the vehicle and a road-level determination is not possible. For example, a network-detected fault can be flagged in the positioning integrity assistance data, resulting in a larger PL computed by the UE.

Another important positioning integrity aspect to take into account in road-user charging and other applications (like pay how you drive insurances) is that, because of their intrinsic nature, they have to be robust against attempts to deceive the positioning system. In these types of applications, the driver of the vehicle may be motivated to alter the position of its own vehicle in order to avoid being charged. Hence, the positioning integrity of the vehicle position needs to be ensured by being able to detect these deception attempts, for example by employing anti-tamper equipment and by cross-checking different positioning sources.

#### 9.2.1.2 Lane-Level Identification

The same concepts and methods from 9.2.1.1 also apply to validating the lane in which the vehicle is traveling. Lane change warnings and manoeuvres are a crucial input to enabling various Levels of autonomy [16] which are illustrated in the 5GAA use case requirements [11], such as an AL of 1.5m and TIR of 1x10-7/hr or lower.

The ability to handle faults almost instantaneously on a road vehicle is absolutely critical in order to recover the situation and avoid a potential collision between lanes. The UE is responsible for monitoring localized events which need to be detected in the shortest time possible, i.e., ‘highly dynamic’ feared events (e.g., multipath, cycle slips and satellite feared events in the case of GNSS). The network is therefore used to monitor the low dynamic threats, which are less time-critical but still depend on a reliable communication channel with the UE. In the automotive and other 5G positioning use cases, the TTA is also far more stringent (e.g., 100ms in some cases) compared with an aviation TTA of 6 seconds (or slower) for precision approaches. Hence, the low latency of the 3GPP communications presents a strong synergy for supplying positioning integrity assistance data that is secure and assured.

Once again, the positioning system should remain available unless the PL exceeds the AL, in which case the system should be unavailable and the corresponding ADAS functionality on the vehicle disengaged. To avoid an integrity event, any feared event with an occurrence probability higher than the TIR (i.e., >1x10-7/hr) needs to be detected and mitigated within the TTA[[2]](#footnote-2). The UE application is typically responsible for issuing alerts to inform the preventative or remedial actions required by the positioning system.

If a feared event occurs at the network or UE, the positioning system should be capable of determining its effect on the PL relative to the AL, within the required TTA, such that the position reported by the UE remains fault-free (i.e., even if the fault-free position leads to the system being unavailable). The TTA therefore represents the ability of the system to recover before being impacted by a potential integrity event. For some use cases, the TTA may simply be set to zero depending on the implementation requirements.

### 9.2.2 Rail

#### 9.2.2.1 Safety-Critical Applications

**Automatic Train Protection** (ATP) applications are used to ensure that trains run safely and efficiently on the right tracks with appropriate speed. Automatic Train Protection aims to prevent a train proceeding beyond the point of danger and to prevent the speed of the train exceeding the permissible limit in the event of a driver error. It consists of the safe determination of position, speed and direction of train movement in order to supervise the safe movement of the train up to its stopping point. This application requires the combination of several functions (or lower level applications) which in turn are strongly dependent of the accurate and safe determination of position and speed of the trains. There are many ATP applications where positioning integrity could be employed, among them one can include Enhanced Odometry, Absolute Positioning, Cold Movement Detection, Train integrity and train length monitoring, Track Identification, Odometer Calibration, and Level Crossing Protection.

**Emergency Management** applications, like the trackside personnel protection (to protect personnel working on or close to the track from the trains using the network) and the door control supervision (to enable the opening of specific doors at particular stations), are also safety-critical applications where positioning integrity will improve the performances and reduce risks.

#### 9.2.2.1 Liability-Critical Applications

**Asset Management**. The accuracy and confidence on the position needed for the location of the assets in some cases can be demanding and require high precision and reliable surveying. Fixed asset management applications are linked with the railway environment, from the infrastructure surveying and structural monitoring to the trackside equipment. Rolling stock asset management applications are in charge of the vehicles that move on a railway including both powered and unpowered vehicles, for example locomotives, railroad cars, coaches, and wagons. Rolling stock applications include: fleet management, cargo monitoring, infrastructure charging, energy charging and hazardous cargo monitoring.

**Protection and Emergency Management Systems**. This group includes applications such as trackside personnel protection, management of emergencies and train warning systems. Management of emergencies can be greatly improved if an accurate, reliable and continuous location of the train is available, allowing the emergency teams to optimise their operations. Train warning systems are employed when some railways require a special warning to passengers on a platform when a train is approaching and is expected to pass the platform at a speed greater than a defined level. This application requires reliable details of train location, speed and other infrastructure data, and may result in an automatic station announcement via a public service broadcast.

**Traffic Management and Information Systems**. This group of applications includes traffic management systems (dispatching), but also on-board train monitoring and recording units, hazardous cargo monitoring and infrastructure charging.

### 9.2.3 Industrial IoT

In contrast to consumer-oriented Internet of Things (IoT), Industrial IoT (IIoT) use cases predominantly focus on operational, safety, and financially beneficial applications of the IoT ecosystem for businesses, infrastructure, and various industries. IIoT positioning integrity/reliability requirements are essential given various safety, payment, and regulatory critical applications. There are many outdoor IIoT devices/UEs employing GNSS-based positioning in various industries that include, but not limited to: Construction, Agriculture/forestry/fishing (smart farming), Oil/Gas industries, and Smart cities (traffic, electric and water systems, waste management, public safety, schools) derived from [1][20]. The ACIA white paper [22] provides some use cases and requirements on 5G positioning in general. An illustrative example relating to Automated Guided Vehicles (AGV) is provided below.

#### 9.2.3.1 Path and Zone Identification for AGV

Positioning integrity is a key input to determining whether an AGV such as a forklift, in a factory or an open space such as ports or construction buildings, is traveling on the narrow halls within lots of different machinery. Aside from the demanding positioning accuracy, the trust needs to be assigned for the path and the zone of its movements. AGV not running into anything unexpectedly is something that needs to be assured. This requires that the AGV, which is the UE in this use-case, to determine with a high degree of positioning integrity which path it can travel within its defined work task. One can also consider that an industrial scenario can have several different zones in which different levels of positioning integrity can be defined, and hence depending on demand of the works in each zone the positioning methods and positioning integrity KPIs can be defined in respect to those. Once again, the positioning system should remain available unless the PL exceeds the AL, in which case the system should be unavailable and the corresponding AGV functionality on the vehicle is disengaged. The set AL for such use-case depends on how large and how densely equipped the factory is, and hence it is reasonable to assume that it can be set to some value between 0.5m to 3m depending on the controlled area use-case and demands. Further illustration of AGV, which requires support for positioning for tracking, routing and guiding is provided in [22].

### 9.2.4 Use Case Summary

Table 9.2.4 is adapted from [9][10] and supplemented by [8][11]. It summarises the typical KPI ranges to be expected on implementation for the Automotive and Rail categories. Importantly, the KPIs are illustrative only; KPIs are typically specified by the positioning system provider on implementation (e.g., a vehicle OEM), taking into consideration the 3GPP and non-3GPP components of the system.

**Table 9.2.4: KPI examples for the Automotive, Rail and IIoT use cases [8][9][10][11].**

NOTE: KPIs are defined by the service provider implementation.

|  |
| --- |
| **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: ≥10-8/hr to ≤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: ≥10-6/hr to ≤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
 |
| **RAIL EXAMPLES** |
| **APPLICATION CATEGORIES** | **TIR** | **AL** | **TTA** | **Integrity Availability** |
| **Safety-Critical Applications** * Absolute Positioning
* Train Awakening
* Cold Movement Detector
* Track Identification
* Level Crossing Protection
* Train Integrity and Train Length Monitoring
 | Typical range: ≥10-9/hr to ≤10-8/hr | Typical range: ≥2.5m to <25m | Typically <7s | Typically ranges from 95% to 99.9% or greater |
| **Liability-Critical Applications** * Trackside Personal Protection
* Management of Emergencies
* Train Warning Systems
* Infrastructure Charging
* Hazardous Cargo Monitoring
* On-Board Train Monitoring and Recording Unit
* Traffic Management Systems
 | TBD | Typical range: ≥25m to <62.5m | Typically ranges from seconds to <30s | Typically ranges from 95% to 99.9% or greater |
| **IIOT EXAMPLES** |
| **APPLICATION CATEGORIES** | **TIR** | **AL** | **TTA** | **Integrity Availability** |
| **AGV Applications** * Mobile device tracking
* Asset tracking
* Process automation
* Inbound logistics
 | Typical range: ≥10-8/hr to ≤10-1/hr | Typical range: ≥0.5m to <30m (vertical/horizontal) | Typically ranges from 100s of milliseconds to <10 seconds | Typically ranges from 95% to 99.9% or greater |

## 9.3 Positioning Integrity Error Categories

### 9.3.1 RAT-Independent

#### 9.3.1.1 A-GNSS Feared Events

This section describes the types of feared events to be considered for implementing positioning integrity using A-GNSS. The feared events are further addressed as part of the UE-based and UE-assisted positioning integrity mode considerations in Section 9.4, including the summary of feared events in Table 9.4.1.1.

##### 9.3.1.1.1 Feared events in the GNSS Assistance Data

###### a) Incorrect computation of the GNSS Assistance Data

GNSS correction networks collect and process GNSS measurements in order to estimate various GNSS corrections (e.g., the satellite orbits, clocks, etc.). If the corrections contain incorrect data, this can lead to incorrect computation of the PL and a potential integrity event. All impacted GNSS assistance data are described in section 8.1 of TS 38.305.

Different types of events can lead to the incorrect computation of corrections: there can be errors on the implementation of the algorithms employed by the GNSS corrections provider to compute the GNSS assistance data; equipment malfunction may corrupt the measurements employed by the GNSS corrections provider; or the correction data computed by the corrections provider may be corrupted before being sent. In any case these events are handled by the GNSS corrections provider by performing consistency checks on the input data, checking the validity of the corrections before sending them and applying CRCs.

###### b) External feared event impacting the GNSS Assistance Data

The GNSS corrections provider generates the correction data employed to estimate the location of the UE. Any event affecting the quality of the generated data will be considered a feared event impacting the GNSS corrections provider.

This is different than the incorrect computation of the GNSS assistance data, which is mainly due to wrong implementation of algorithms or corrupted data. These external events comprise situations affecting the estimation process that happens at the GNSS correction provider, such as erroneous data inputs used to compute the corrections (e.g. satellite, atmospheric or local environment feared events impacting the GNSS reference stations in the GNSS correction provider’s network).

A first approach to handling these events is to monitor these types of situations at the GNSS corrections provider and, for those satellites not achieving some required threshold conditions, flag them or not send their corrections. This ON/OFF approach can work when there is only one level of target accuracy that needs to be achieved but, when there can be several levels of target accuracy and, moreover, when these levels are not predefined, then a more flexible and powerful approach is for the GNSS corrections provider to indicate the quality of each correction, thus allowing the location function to decide whether it uses the satellite or not and to have a better estimation of the location errors.

##### 9.3.1.1.2 Feared events during positioning data transmission

###### a) Data integrity faults

Data tampering e.g., spoofing can also affect the quality and integrity of the positioning services provided by 5GS. For instance, the interface between 5GS and a GNSS Corrections Network (need for RTK, PPP-RTK, etc.) may be vulnerable to malicious attacks. The situation here is similar to the GNSS Data Channel tampering described in section 9.3.1.1.3 but applicable to another type of data transmission channel.

##### 9.3.1.1.3 GNSS feared events

Editor’s Note:GNSS feared events are those which occur external to the UE and potentially impact the quality and availability of the GNSS signals.

###### a) Satellite feared events

Satellites can suffer HW failures and potentially output an incorrect signal for a period of time or permanently, depending on the magnitude of the issue. In situations like this the health of the GNSS satellite(s) and the signal(s) must be communicated to the UE in real-time. This is achieved by using flags in the message broadcast by SBAS systems or directly by the affected GNSS constellation. Alternatively, the *GNSS-RealTimeIntegrity* IE can be used in UE-based mode. This is the most basic form of integrity capability included in LPP protocol.

###### b) Atmospheric feared events

The Ionosphere is the region of the atmosphere between around 80km – 600km above the Earth. The GNSS signals are delayed in the region above an altitude of 80km by an amount proportional to the number of free electrons given off by the sun. Since the ionospheric delay is frequency dependent, it can virtually be eliminated by making and differencing ranging measurements on two GNSS frequency bands e.g., B1-C/E1/L1 (1,575.42 MHz) and B2a/E5a/L5 (1,176.45 MHz). Although ionospheric delay errors are removed, this approach has the drawback that measurement errors are significantly magnified through the combination. When not removed, ionosphere represents the largest error source.

The troposphere is the lower part of the atmosphere that is nondispersive for frequencies up to 15 GHz. Within this medium, the phase and group velocities associated with the GNSS carrier and signal information (ranging code and navigation data) on the GNSS L-band frequencies are equally delayed with respect to free-space propagation. This delay is a function of the tropospheric refractive index, which is dependent on the local temperature, pressure, and relative humidity. Left uncompensated, the range equivalent of this delay can vary from about 2.4m for a satellite at the zenith and the user at sea level to about 25m for a satellite at an elevation angle of approximately 5° [25]. Basic models can correct up to 90%, linked to the dry component, while the remaining errors are linked to the wet component which is more difficult to predict due to uncertainties in the atmospheric distribution.

LPP already includes an IE for these correction data, namely *GNSS-SSR-STEC-Correction, GNSS-SSR-GriddedCorrection*. The existing atmospheric messages in LPP remove a large portion of the atmospheric errors impacting the positioning accuracy. However, the residual errors after the atmospheric corrections have been applied may still have a magnitude sufficient to cause the position error to exceed the AL with a probability of occurrence greater than the TIR. In addition, if the temporal or spatial rate of change of these errors is unusually large, this may also lead to larger than anticipated residual errors. Additional integrity indicators are therefore necessary to detect these feared events. A key benefit of network-assisted integrity is to leverage the additional number of measurements, redundancy and cross-checks made available from a network of GNSS reference stations, potentially leading to lower TIRs and less overhead at the UE. Individual ionospheric and tropospheric quality indicators are missing and can be easily added as a field to each of these IEs.

###### c) Local Environment feared events

Multipath

Multipath is one of the most significant errors incurred in the GNSS receiver measurement process. The magnitude of multipath errors varies rapidly and significantly depending on the environment in which the receiver is located, satellite elevation angle, receiver signal processing, antenna gain pattern, and signal characteristics. Unlike the other error sources considered thus far, multipath errors are uncorrelated even in short-baselines and cannot be removed by differential techniques (e.g., RTK).

There are two multipath scenarios:

* Multipath without blockage (Line-of-Sight, LOS)

In addition to the direct satellite-to-receiver path, the signals are also reflected from the ground and other objects. These cause multiple copies of the signal or a broadening of the signal arrival time, both of which reduce precision. Since the path travelled by a multipath is always longer than the direct path, multipath arrivals are delayed relative to the direct path. Multipath reflections distort the correlation function between the received composite (direct path plus multipaths) signal and the locally generated reference in the GNSS receiver, and also distort the phase of the composite received signal, introducing errors in pseudorange and carrier phase measurements that are different among the signals from different satellites, and thus produce errors in position, velocity, and time [25].

* Multipath with blockage or shadowing (Non-Line of sight, NLoS)

The effects of multipath are commonly assessed when the direct path signal is received without attenuation, so that multipath power is lower than direct path power. When blockage or shadowing of the direct path occurs along with multipath, the direct path is attenuated and received power of the multipath may be even greater than the received power of the shadowed direct path. Such a phenomenon can occur in outdoor situations and also in indoor situations, when the direct path is significantly attenuated while passing through walls or ceiling and roof, while the multipath is reflected from another building and arrives with little attenuation through a window or other opening. Consequently, shadowing of the direct path and multipath has combined effects on the relative amplitudes of direct path and multipaths. In some cases, shadowing of the direct path may be so severe that the receiver only tracks the Non Line-of-Sight (NLoS) multipath(s) and errors of several tens of meters can appear in the pseudorange measurements.

NLoS is more likely to happen in urban environments and is an important issue for integrity. This is a local error, specific to each receiver and its mitigation takes place at the UE without assistance data from LMF.

Interference

The theoretical principle behind this threat is the jamming of data transmission in general between a transmitter and a receiver. The practical principle defines however the exclusive jamming of the GNSS receiver where the transmitted signal is weakest and most open to attack.

There are two forms of GNSS Radio Frequency Interference (RFI), Intentional and Unintentional:

* Unintentional RFI is due to a nearby radio device broadcasting at a frequency which impacts the GNSS signals.
* Intentional RFI is the deliberate action of blocking the reception of GNSS signals by broadcasting a strong signal on GNSS frequencies.

A typical jammer relies on power and spectral occupation to deny the GNSS signals. Studies of simple jamming attacks have demonstrated that it is relatively easy, given sufficient broadcast power, to deny the use of GNSS to many receivers in a given geographic area. Jamming represents complete disruption of GNSS signals by another radio frequency source, be it the sun, privacy seeking citizens, or belligerent nations. Jamming can heave very serious impacts, depending upon the number and type of affected users, duration of the disruption, etc.

Simple jamming is a very easy attack to launch but is also very easily detected, readily localized, and often relatively easily mitigated. GNSS system providers offer protection against jamming by using stronger signals, broadcast on more frequencies, and using more constellations simultaneously.

Spoofing

In this type of threat the attacker threatens integrity and confidentiality of a GNSS transmission by broadcasting false signals with the intent that the victim receiver will misinterpret them as authentic signals. Spoofing aims at making the receiver compute a false position and time. Spoofing attacks are difficult to detect and can also be deployed in a coherent manner, as such bypassing any integrity detection and recovery measures (i.e. RAIM). Therefore, when such events occur, the measurements from the receiver can pass the integrity check, even if the error of the computed position far exceeds the expected accuracy.

GNSS system (e.g. GPS, Galileo etc) are working on securing their publicly broadcast signals. In order to overcome these threats, signal and message/data channel authentication solutions are being deployed by GNSS systems providers to ensure authenticity to the ranging measurements and data channels [18][19]. Such authentication solutions are especially useful for road users, UAVs, rail users, and timing users. These UEs will then need to retrieve the following information:

* Ranging Authentication Data: primarily the cryptographic data needed to verify the signal/ranging authentication;
* Data Channel Authentication data: the navigation data and their signatures.

The introduction of A-GNSS has partly solved the need for GNSS Data Authentication for UEs which can retrieve the GNSS Navigation Message from 5GS through an LPP transaction instead of the GNSS signals. On the other hand, ranging authentication continues to be a serious challenge. The idea is to protect the GNSS pseudorange, performed by the UE, from intentional acts, ensuring the trustworthiness of location and time.

RAT-dependent positioning techniques could be used as independent means to cross-check the authenticity of the position reported by the GNSS receiver, while *GNSS-ReferenceTime, GNSS-SystemTime,* and *NetworkTime IEs* could be used as redundant information to cross-check the authenticity of the GNSS time reported by the receiver. Besides these capabilities, useful in detecting a spoofing event, 5GS could also enable GNSS ranging and navigation authentication by acting as an alternative data channel to the GNSS signal in space for the dissemination of cryptographic assistance data. In this scenario the UE could instantaneously verify that the received signal and data came from the correct source i.e., a GNSS constellation and avoid spending energy to retrieve the data from the GNSS signal.

##### 9.3.1.1.4 UE feared events

UE specific errors are not possible to mitigate with assistance data from the network, the UE is responsible for mitigating these feared events locally, based on implementation.

###### a) GNSS receiver measurement error

Measurement errors are also induced by the receiver tracking loops, so this is an inherent noise within the receiver which causes jitter in the signal. Typical values for the noise and resolution error in the case of modern GNSS receivers are on the order of a decimetre or less in nominal conditions (i.e., without external interference) and negligible compared to errors induced by multipath.

###### b) Hardware faults

Editor’s Note: FFS

###### c) Software faults

Editor’s Note: FFS

##### 9.3.1.1.5 LMF Feared Events

Editor’s Note: FFS

###### a) Hardware Faults

###### b) Software Faults

## 9.4 Positioning Integrity Methods

### 9.4.1 RAT-Independent

The scope of this study is limited to examining positioning integrity considerations for A-GNSS positioning.

#### 9.4.1.1 A-GNSS Positioning Integrity Methods

The 3GPP specifications can be extended to support the determination of positioning integrity, by defining information elements and signalling procedures to transport assistance information to mitigate feared events. A summary of the feared events studied in Section 9.3 is provided in Table 9.4.1.1 below, including examples of the types of assistance information to be considered for inclusion in LPP

Editor’s Note: The LPP IEs and procedures for positioning integrity will be defined in the WI.

**Table 9.4.1.1: Summary of A-GNSS feared events and integrity assistance information considerations (FFS).**

NOTE: The positioning integrity assistance information IEs are FFS as part of the WI.

**\***NOTE: The UE or LMF are responsible for mitigating these feared events locally, outside the scope of the specifications.

|  |  |  |
| --- | --- | --- |
| **Feared Event Category**  | **Feared Event**  | **Examples of positioning integrity assistance information (FFS)**  |
| 1. Feared events in the GNSS Assistance Data  | Incorrect computation of the GNSS Assistance Data, e.g. software bug, corrupt or lost data | Validity or quality flags for existing assistance information |
| External feared event impacting the GNSS Assistance Data, e.g. satellite, atmospheric or local environment feared events (Category 3) impacting the GNSS reference stations in the GNSS correction provider’s network. |
| 2. Feared events during positioning data transmission  | Data integrity faults | Data corruption check, e.g. CRC |
| Data Authentication / Signature |
| 3. GNSS feared events | Satellite feared eventse.g. bad signal-in-space or bad broadcast navigation data | Satellite health or quality flags |
| Atmospheric feared events | Ionospheric indicator |
| Tropospheric indicator |
| Local Environment feared events, e.g. Multipath, Spoofing, Interference | Assistance information: Trustable time reference, Data Authentication / Signature, Regionalized indicator of multipath, interference, jamming, spoofing, etc |
| 4. UE feared events | GNSS receiver measurement error | *e.g., GNSS-MeasurementList* |
| Hardware faults | \* |
| Software faults | \* |
| 5. LMF feared events | Hardware faults | \* |
| Software faults | \* |

**Figure 9.4.1.1: Simplified relationship between the positioning integrity feared event categories and the 3GPP positioning architecture. Refer to [21] for a detailed description of the UE positioning architecture.**



##### 9.4.1.1.1 Signalling considerations

The following LPP signalling was identified in the study, for consideration in the WI:

1. Signalling to determine the positioning integrity capability
2. Signalling to deliver the KPIs and integrity results
3. Signalling to deliver the integrity assistance information to the UE
4. Signalling to deliver the integrity information related to the GNSS positioning measurements from the UE to the LMF

Table 9.4.1.1.1 summarizes the UE-based and UE-assisted considerations for supporting positioning integrity in the 3GPP specifications, with respect to the feared events identified in Table 9.4.1.1 and the signalling considerations above.

Two modes of integrity result reporting are also identified below for consideration in the WI:

* **Mode 1 of Integrity Result Reporting : PL Reporting**

The integrity computing entity calculates the PL, based on the measurement, assistance information and TIR. Then, the calculated PL is directly reported to where the LCS client resides (Network or UE). Hence, the integrity computing entity does not judge whether the positioning system is still available, it simply provides whatever PL value it has obtained. It is left to the LCS client itself to determine if the positioning system is still available based on the reported PL.

* **Mode 2 of Integrity Result Reporting : Integrity Event Flagging**

The integrity computing entity calculates the PL, based on the measurement, assistance information and TIR. Then, the integrity computing entity further compares the calculated PL with the given AL to determine if the positioning system is still available to offer trustable position estimation. Thus, the integrity computing entity may only have to report a binary flag (0 and 1) to indicate whether the positioning system is available or not. Thus, in this case the LCS client can be directly informed about the system availability, without conducting further evaluation by itself.

**Table 9.4.1.1.1: Summary of network-assisted (UE-Based) and UE-assisted (LMF-Based) positioning integrity mode considerations.**

NOTE: The table provides a summary of considerations and the final details and specification impacts are FFS in the WI.

\*NOTE: Examples of KPIs are the TIR, AL, TTA. Examples of Integrity results are the PL and Integrity Availability.

\*\*NOTE: From LMF to UE does not mean the integrity assistance information is generated by the LMF.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Positioning Integrity Mode** | **Location service type** | **Source of KPIs\***  | **Source of Integrity results\*** |  **Positioning Integrity assistance information\*\***  | **Specification impact**  |
| Network assisted (UE-based): Positioning integrity result is derived by the UE | MO-LR | UE internal implementation | UE internal implementation  | From LMF to UE: - Feared events in the GNSS Assistance Data- Feared events in transmitting the data to the UE- GNSS feared events | Procedure to transfer Integrity assistance information from LMF to UE |
| MT-LR | From LMF  | From UE | From LMF to UE: - Feared events in the GNSS Assistance Data- Feared events in transmitting the data to the UE- GNSS feared events | Procedure to transfer Integrity assistance information and KPIs from LMF to UEProcedure to transfer Integrity results from UE to LMF  |
| UE assisted (LMF-based): Positioning integrity result is derived by the LMF | MO-LR | From UE | From LMF | From GNSS corrections provider (external source) to LMF: - Feared events in the GNSS Assistance Data- Feared events in transmitting the data to the UE- GNSS feared eventsFrom UE to LMF:- UE feared events | Procedure to transfer Integrity assistance information and KPIs from UE to LMFProcedure to transfer Integrity results from LMF to UE  |
| MT-LR | LMF implementation | LMF internal implementation | From GNSS corrections provider (external source) to LMF: - Feared events in the GNSS Assistance Data- Feared events in transmitting the data to the UE- GNSS feared eventsFrom UE to LMF:- UE feared events | Procedure to transfer Integrity assistance information from UE to LMF  |

##### 9.4.1.1.2 Summary of A-GNSS Positioning Integrity Methods

The detection of feared events is necessary to support the implementation of positioning integrity. Assistance information and associated IEs can be optionally sent between the LMF and the UE to mitigate the feared events. LPP signalling considerations for UE-based and UE-assisted positioning integrity have been examined in this section to support the use cases in Section 9.2. To ensure that the system meets the integrity goals and requirements, it must be systematically validated, possibly including compliance to relevant industry functional safety specifications such as ISO-26262 for automotive. Integrity validation is considered outside the scope of the 3GPP specifications as it concerns a specific integrity system implementation.

*Next Text proposal*

## 10.10 Enhancements of signalling and procedures for positioning integrity

The following enhancements of signalling and procedures to support positioning integrity determination are recommended, including the following aspects:

* + Define the specific list of A-GNSS positioning integrity feared events to be addressed in the 3GPP specifications.
	+ Signalling and procedures to support positioning integrity determination:
		- The assistance information IEs that will be used to mitigate the feared events;
		- The details of the LPP signalling to transport the positioning integrity assistance information.
		- The details of the LPP signalling to transport the positioning integrity KPIs and integrity results.
	+ Support of integrity for UE-Based and UE-Assisted A-GNSS positioning.

*End of Text proposal*

1. A monitor is used to detect the feared events that occur more frequently than is acceptable to meet the TIR, i.e., the monitor’s purpose is to reduce the likelihood that feared events go undetected. [↑](#footnote-ref-1)
2. NOTE: If the lane-level requirement was simply specified by the accuracy estimate (e.g., <1.5m at the 95th percentile), 5% of the estimated positions may still be impacted by feared events which far exceeds the required AL, potentially leading to an integrity event. Positioning integrity KPIs are instead used to define probabilities of failure over a given period of time rather than relying on the combined statistical distribution of the estimated positions (which are potentially contaminated by fault and fault-free events that go undetected). The positioning integrity methodologies allow an positioning integrity risk to be allocated based on the probability of occurrence for each feared event, and then quantified as a contribution to the total TIR. This ensures only the integrity-validated positions are included in the positioning estimate, meaning the nominal accuracy should be easily achieved. [↑](#footnote-ref-2)