3GPP TSG-RAN WG2 Meeting #112-e***R2-20xxxxx***

Electronic, November 2 – 13, 2020

**Agenda item:** 8.11.1

**Source:** Swift Navigation

**Title:** Email discussion [AT112-e][614][POS] Text proposals on GNSS integrity (Swift)

**Document for:**  Discussion and Decision

# 1. Introduction

This document addresses the following email discussion:

**[AT112-e][614][POS] Text proposals on GNSS integrity (Swift)**

Scope: Progress the text proposals related to the integrity topics (R2-2009129, R2-2008812, R2-2009331, R2-2010073, R2-2010061, R2-2009333, and the table in R2-2009003) and attempt to reach one or more endorsable TPs.  Documents to be split into separately agreeable topics (rapporteur’s judgement on the division).

Deadline:  Friday 2020-11-13 0000 UTC

The content from each submission has been divided into three topics corresponding to the overall study objectives, which are individually addressed in the sections below:

1. Integrity Concepts, KPIs and Use Cases
2. Integrity Error Sources
3. Integrity Methodologies

Please provide your comments prior to Wednesday 2020-11-11 (12.00 UTC) to allow sufficient time for consideration as part of the resulting text proposals.

# 2. Integrity Concepts, KPIs and Use Cases

Rapporteur’s Comments:

The following updates have been made to Sections 9.1 (Integrity Overview – Background Information) and 9.2 (Use Cases) of the draft TP [1] following initial feedback from the online discussions at RAN2#112-e [2].

1. Reference 6 [1] has been removed throughout the document (NOTE: the reference numbering has now been updated in the TP below as a result of this change).
2. The ‘Editor’s Note’ (‘Terminology and definitions relating to these concepts have been provided in Section 3.1’) has been removed from Section 9.1.1 (Integrity Concepts).
3. The Integrity definition provided in Section 9.1.1 has been added to Section 3.1 (Terms).

**Question 1: Do you agree with updated text proposal for Sections 9.1 and 9.2 (and their subsections)? If not, please provide your reasoning and any proposed changes to the text?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Generally OK but some modifications are needed | As we have commented online, the term “hazardous” in the AL definition does not seem to bring much value – instead it create some confusion. From 3GPP point of view, we only need to know that the positioning system would become unavailable when the PL exceeds AL; by saying that the operation becomes “hazardous” may raise some unnecessary concerns of stakeholders who planned to use this technology. So we propose the following change:**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, ~~operations are hazardous and~~ the positioning system should be declared unavailable for the intended application to prevent loss of integrity.On the other hand, for the integrity definition, the warning should be given to the LCS client (the application that is interested in such information) anyway, and LCS client could be in either UE or Network. Hence we do not need to explicitly mention “UE” in this case, as it is already covered by “LCS client”. We propose the following change:**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 UE and/or~~ the LCS client when the positioning system does not fulfil the condition for intended operation. |
| InterDigital | Yes |  |
| Fraunhofer | Yes |  |
| ESA | Yes | We agree with the TP for sections 9.1 and 9.2 with the following improvements:* Editorial: some of the terms under Abbreviations need indentation; Some sentences in the last paragraph of section 9.1.1.1 use a red Font color – please check it.
* Improve the explanation of the Road-User Charging use case by including the following paragraph:

*Another important 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 this kind 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 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.*Introduce a new KPI: as explained in **[R2-2010098](https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_112-e/Docs/R2-2010098.zip)**, we propose the inclusion of **PL availability** as an additional KPI. Current KPIs (TIR, AL and TTA), are providing requirements only on the capability of the PL to indicate when the Position Error is greater than the Alert Limit. When the system provides a PL (e.g., 15m) > AL (e.g. 10m), this PL value will always satisfy the TIR, AL, and TTA but it will make the system unavailable. Therefore, we think that we need to include a KPI to measure the availability of the computed PLs.* Please add these two references (see improvements proposed to section 9.3.1)

[17] European GNSS Agency, “GNSS User Technology Report issue 3”, 2020[18] Air Force Research Laboratory, “IS-AGT-100 Chips Message Robust Authentication (Chimera)”, 2019. |
| Convida | Yes, with changes | **2 References:** Update the reference to the most recent version of the approved SI; <https://www.3gpp.org/ftp/TSG_RAN/TSG_RAN/TSGR_89e/Docs/RP-202094.zip>**3.1 Definitions/Terms:** Include a definition for “feared events”. Generally, fix the styles consistent with the TR template.**9.1.1** Add reference to 22.872. Remove the statement about existing products: “Various GNSS service providers already support integrity monitoring [1] in their products”**9.2.2** Add editor’s note: “Editor’s note: Rail use cases are FFS”**9.2.3** Use same/similar wording for EN: “Editor’s note: Industrial IoT (IIoT) use cases are FFS”Also, consider incorporating TPs in R2-2010090 (Convida) and R2-2010074 (Ericsson) to address FFS for IIoT for the next revision.**9.2.4** Change Table 9.2.4 Note: **(NOTE: KPIs are defined by the ~~positioning system owner on~~ *service provider* implementation)** |
| ZTE | Almost Yes. | 1. For the integrity definition issue which is mentioned by Nokia, considering currently RAN2 does not have any consensus about the methodologies about the positioning integrity and how to transport&use the integrity related factors, the warnings may be given to UE, LCS clients, LMF or other potential network units.Hence, we prefer to modify the definition as below:

**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 UE and/or the LCS client~~ the target when the positioning system does not fulfil the condition for intended operation.1. We prefer to add the *PE positioning error* into clause 3.3.
2. As we discussed online, we prefer to introduce the definition of feared event before we use it in TR. How about add the definition in clause 9.1.1 integrity concepts?
 |
| Spreadtrum | Yes |  |
| Xiaomi | Yes |  |
| Hexagon | Yes |  |
| Swift Navigation | Yes | We agree with the proposal from ESA to include a KPI to measure the availability of the computed PLs. We suggest renaming this to Integrity Availability to clarify that we are indicating whether an integrity validated solution is available (not whether the PL is output or not). Adapted from R2-2010098:**Integrity Availability**The integrity availability is the percentage of time that the PL is below the required AL.Proposed definition of feared event from RP-2006541:**Feared Event:** Feared Events are considered to be all possible events (i.e. of natural, 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. |

================================= START TP ===========================================

# 2 References

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] RP-193237: "new SID on NR Positioning Enhancements".

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

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

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 5GAA, “White Paper – C-V2X Use Cases Methodology, Examples and Service Level Requirements, 2019.

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

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

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

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

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

[16] 3GPP TS 33.501, “Security architecture and procedures for 5G system”.

# 3 Definitions of terms, symbols and abbreviations

3.1 Terms

**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 UE and/or the LCS client when the positioning system does not fulfil the condition for intended operation.

**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, operations are hazardous and the positioning system should be declared unavailable for the intended application to prevent loss of 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 position integrity annunciates a corresponding alert.

3.2 Symbols

3.3 Abbreviations

**AL Alert Limit**

**HAL Horizontal Alert Limit**

**HMI Hazardously Misleading Information**

**HPL Horizontal Protection Level**

**MI Misleading Information**

**PL Protection Level**

**TIR Target Integrity Risk**

**TTA Time-to-Alert**

**VAL Vertical Alert Limit**

**VPL Vertical Protection Level**

================================== END TP ===========================================

================================= START TP ===========================================

9 Positioning integrity and reliability

9.1 Integrity Overview – Background Information

9.1.1 Integrity Concepts

As positioning demands continue to increase, the scale and connectivity of emergent applications such as self-driving vehicles have necessitated a standards-based approach. More devices connecting to the 3GPP network means more users rely on the network being trustworthy and interoperable. The ability to navigate safely means users must trust their estimated position with a high degree of confidence. Trustworthiness of position is the study of positioning integrity, which is adapted from TR 22.872 as follows:

**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 UE and/or the LCS client when the positioning system does not fulfil the condition for intended operation.

Various GNSS service providers already support integrity monitoring[[1]](#footnote-1) in their products, but there is no common 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 integrity, it is important to understand how it differs from the more familiar concept of Accuracy.

Accuracy and 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 centimeters, 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, integrity can be used to quantify the trust on the provided position. 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 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, operations are hazardous and the positioning system should be declared unavailable for the intended application to prevent loss of 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 position integrity annunciates a corresponding alert.

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 [4], 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).

Integrity system failures are known as Integrity Events. An integrity event occurs when the positioning system outputs Misleading Information (MI) or Hazardous Misleading Information (HMI). MI occurs when, the positioning system being declared available, the actual positioning error exceeds the PL but not the AL. Typically, positioning systems are designed to tolerate some level of MI, provided the system can continue to operate safely within the AL. HMI occurs when, the positioning being declared available, the actual positioning error exceeds the AL without annunciating an alert within the required TTA. 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 integrity events (MI, 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)
and the MI and HMI integrity events [5].

A useful representation for interpreting the relationship between the Integrity KPIs and PL is the so-called Stanford Diagram [6] 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 [6][7].

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 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, 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, 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 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 integrity monitoring has a long operational history in the field of civil aviation [11][12][13][14]. The 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.

Automotive and Rail have been highlighted as two industries which implement the most demanding safety-standards for positioning integrity. The following use case descriptions outline key integrity concepts and implications for users that require positioning integrity within their positioning system. An extended list of application examples is provided in the Use Cases Summary.

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 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 an integrity service provider via the mobile network to request UE-Based 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 integrity assistance data, resulting in a larger PL computed by the UE.

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 [15] which are illustrated in the 5GAA use case requirements [10], 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 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

9.2.3 Industrial IoT

Editor’s note: Industrial IoT (IIoT) use cases are FFS and can be included later.

9.2.4 Use Case Summary

Table 9.2.4 is adapted from [8][9] and supplemented by [7][10]. 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 owner on implementation (e.g. a vehicle OEM), taking into consideration the 3GPP and non-3GPP components of the system.

|  |
| --- |
| **AUTOMOTIVE EXAMPLES** |
| **APPLICATION CATEGORIES** | **TIR** | **AL** | **TTA** |
| **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 |
| **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 |
| **Regulatory Critical Applications*** Hazardous Material Tracking
* E-Call
* Geofencing (e.g. low emission zone)
 |
| **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** |
| **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 |
| **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 |

**Table 9.2.4: KPI examples for the Automotive and Rail use cases [7][8][9][10].**

**(NOTE: KPIs are defined by the positioning system owner on implementation)**

================================== END TP ===========================================

# 3. Integrity Error Sources

The following agreements were made at RAN2#112-e as an input to this email discussion:

Agreements:

1 RAN2 to agree following additional sub-feared events:

3. External feared events, e.g.

- Spoofing

- Jamming/interference

4. UE faults

- GNSS receiver measurement error

- Hardware faults

2 RAN2 to confirm the need to capture the table on feared events and corresponding assistance data in the TR; the actual handling of these events is FFS.

* Text proposals in R2-2008812/R2-2009331/R2-2010073/R2-2010061 to be taken into account in discussion [614], and aligned with the agreements above.

Rapporteur’s Comments:

To address the Agreements and corresponding text proposals above, the following updates have been made to the text proposal below, corresponding to Section 9.3 of the TR.

* The feared event naming in the table and descriptions has been updated in line with the current agreements.
* The feared event descriptions from [7] have been proposed as an initial baseline.
* Generally speaking, those in favor of including a complete table of feared events in the TR suggested it is necessary to enumerate the potential error sources in order to satisfactorily address objective 2 (noting that if and how each error sources is handled in scope of the specification is FFS). The alternative view from the online discussion was to only address the error sources that will be handled in the specification, meaning an enumerated table of feared events is not needed. Therefore:
	+ Taking into consideration the updated feared event categories above and the text proposals from [4][5][6][7], an updated table of feared events has been proposed for further discussion and consideration by RAN2 as an outcome of this email discussion. The table combines proposed fields from both [5] and [6] to identify the existing IEs which already support improved accuracy in LPP, alongside the new indicators to be considered for determining integrity. An introduction to the table has also been added, alongside the diagram from [5] to illustrate which parts of the 3GPP positioning system that each event category corresponds to. The ‘Group Names’ from [4] have not been adopted as they differ from the naming and allocation of the feared event categories already agreed. Also, it is anticipated that the assistance data definition will not occur until the WI phase.

**Question 2: Do you agree with the text descriptions for the feared event error sources? If not, please provide your reasoning and any proposed changes to the text.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Yes |  |
| InterDigital | Yes (with comments) | We are generally fine with the text descriptions (with a comment in the TP). In Section 9.3.1.1, we understand that Table 9.3.1.1 is oriented towards UE-based integrity and as such, lists the possible new IEs in the assistance data. However, since the feared event error sources are applicable for both UE-based and LMF-based integrity, they should be described before focusing on UE-based integrity. In light of this, we think a modified Table 9.3.1.1 (see answer to Q3-b) should be moved after the descriptions of error sources (after section 9.3.1.1.4). |
| ESA | Yes with simplifications | Some editorial suggestions are included as Comments directly in the TP. Following online discussions and suggestion from InterDigital we think error sources description text can benefit from text simplification: Jamming, now proposed to be replaced by Intentional and Unintentional Interference, Spoofing.1. *~~“Jamming~~ Intentional and unintentional 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):** *Unintentional RFI is due to a nearby radio device broadcasting at a frequency that lies within the passband of one of the GNSS frequencies.*
* *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. ~~For example, low-cost GNSS jammers have caused more than 50,000 disruptions between 2016 and 2018 in Europe alone.~~**Simple jamming is a very easy attack to launch but is also very easily detected, readily localized, and often relatively easily mitigated. GNSS systems providers offer protection against jamming by stronger signals, broadcast on more frequencies, and using more constellations simultaneously.”*Regarding spoofing, ESA´s initial text is too complicated and long. In line with discussions during online session, we propose several amendments to fix these shortcomings: 1. Spoofing

*“In this type of threat the attacker threatens integrity and ~~confidentiality~~ authenticity 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 systems ~~service providers~~ e.g., GPS, Galileo, etc. ~~have come to the help of users and~~ 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 [17][18] ~~proving attestation to the integrity targeted by the navigation system~~. 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 ~~reconstruct and use the solutions for~~ verify the signal/ranging authentication;*
* *Data Channel Authentication data: the navigation data and their ~~authentication tags (digital~~ signatures ~~in the data stream of the GNSS broadcast).~~*

*~~The drawback to data authentication and ranging signal authentication is that they both endure an authentication delay. In other words, the user must wait for a period of time before they can despread the stored cryptographic precorrleation samples or evaluate the digital signature sent by the GNSS satellite. This delay is further increased by the fact that GNSS services are broadcast systems with very low data rates (50-150 bps) i.e., small data amounts need lots of time to be broadcast in full. Therefore, the time to retrieve such data directly from the GNSS signal can be high impacting the battery consumption.~~* *The introduction of A-GNSS has partly solved the need for GNSS Data Authentication for UEs which can retrieve GNSS Navigation Message from 5GS through an LPP transaction instead from GNSS signals, which is slow and affects the batter consumption. 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. ~~In response to this emerging hazard, several spoofing mitigation strategies are under development by the GNSS service providers: cryptographic authentication of GNSS ranging signals and data channels by the core GNSS constellations (Galileo OS-Authentication, GPS-CHIMERA, BeiDou, and QZSS) although at this moment there is no operational service.~~**RAT-dependent positioning techniques could be used as independent means to cross-check the authenticity of 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 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.”* |
| Convida | Yes, with comments | Prefer that we completely separate the concept of “feared events” versus UE faults. UE faults are not “feared events” and mitigation of this should be outside the scope of the integrity indicators/IEs as it is implementation dependent.  |
| ZTE | Yes with comments | 1. Add definition of the feared event before use(same as Q1.)
2. Change the title of clause 9.3.1.1 to A-GNSS

3GPP is only responsible for network assisted GNSS(A-GNSS). Currently, all error source discussions are limited in the A-GNSS, RAT-independent positioning methods. As it shown in figure 9.3.1.1, we should also discuss the error sources between 1,2 and 4 which are not fully covered by GNSS.Diagram  Description automatically generated**Figure 9.3.1.1: Simplified relationship between the GNSS Integrity feared events and the 3GPP UE positioning architecture (GNSS).** |
| Spreadtrum | Yes |  |
| Xiaomi | Yes |  |
| Hexagon | Yes, with comments | The terminology used for ‘event’ in the text above needs to be better defined and made consistent and aligned to section 9.3. For example, the following terms are currently used: ‘fault feared events’, ‘fault-free feared events’, ‘external events’ and ‘sub-feared events’, without these being well defined.We agree in general terms with the text descriptions in sections 9.3.1.1 – 9.3.1.4, though with these comments:1. We agree with the categories listed in the 1st column of Table 9.3.1.1.
2. More details from the text descriptions in [7] can be adopted, particularly on satellite and signal errors
3. Descriptions on UE faults are currently limited. It should be noted that the UE is not only responsible for mitigating feared events. As a system component it can also itself be a cause of a fault causing the TIR to be exceeded.

It should be indicated that the UE will ultimately be the system component that collates all integrity IE’s to produce the PL information provided to the downstream application and/or user |
| Swift Navigation | Yes (subject to editorial review) | We are ok to move the table after the generic error source descriptions. |

**Question 3-a: Do you agree with including a table which summarises the feared event categories and examples of integrity indicators as part of the TR? If not, please provide your reasoning.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Yes |  |
| InterDigital | Yes  |  |
| Fraunhofer | Yes |  |
| ESA | Yes |  |
| Convida | Yes, with comments | It is helpful to provide what is in scope of the integrity indicators.However, per the comments for Q2, Feared Event Category Feared & Event Sub-Category should be renamed as “Error source category” or something similar. In the column for “New Integrity IEs required?” consistently use FFS, rather than “Maybe” and remove “Maybe” from the Note in the table. |
| ZTE | Yes |  |
| Spreadtrum | Yes |  |
| Xiaomi | Yes |  |
| Hexagon | Yes | We agree. Such table is essential for mapping IE’s to specific integrity event categories and to indicate which system component is responsible for providing the required integrity information (IE). |
| Swift Navigation | Yes | Swift Navigation |

**Question 3-b: If you answered Yes to Question 3-a, do you agree with the table presented in the text proposal? If not, please provide your reasoning and any proposed changes.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Partly (with quesions) | By essence, faults in the correction data due to e.g. SW bugs are unknown. The reliability and usefulness of a quality indicator would therefore be questionable. A statistical indicator providing the a-priori probability that such feared event happens would be enough.Faults in transmitting the data to the UE: Not sure if we understand this correctly so more clarification is appreciated. The 5GS already provides an efficient data integrity support for the LMF to UE segment. Is the proposal to consider an end to end integrity support between the correction service provider and the UE. What would be in that case the additional contribution of LPP ? Regarding the atmospheric feared events, the text proposal should describe in more details the gaps with what LPP currently supports. A description of the content, role, expected improvements and originator of the ‘individual quality indicator’ is missing.The rest of the section is OK. In particular, we support the principle proposed for 5GS aided ranging/data authentication. |
| InterDigital | Yes (with comments) | We think the summary table should be modified to be agnostic to UE-based or LMF-based integrity. Specifically, the columns in the summary table can include feared event categories, feared event subcategories and integrity indicator examples. The existing IEs related to accuracy can be described separately in the text but not in the summary table. We are also of the opinion that the protocol aspects, including the use of LPP for delivery of error source indications and the introduction of new IEs, should be discussed under the methodologies section. |
| Fraunhofer | Yes (with comments) | For jamming/interference, the integrity indicator examples could be flags indicating interference/jamming/spoofing on certain frequency bands. Further parameters that could characterize such events could be left FFS. Furthermore, measurements from UE or classification from UE indicating issues with jamming/interference/spoofing are examples of integrity indicators signaled from the UE. Since integrity issues around spoofing and jamming are not yet specified in LPP messages, it is clear new integrity IEs are needed. Exact details on what needs to be signaled is FFS, but it is also the case for other Sub-categories too. |
| ESA | Yes (with some modifications) | “Relevant LPP Message” is not a correct name, we would suggest to replace it by “Existing IEs in LPP”. Second, the last two columns should be merged into a new one, maybe something like “Possible Solution”, in an attempt to keep the solutions study open to options other than quality indicators – new IEs pair. In reality, we may not need entirely new IEs but extend existing ones or relay on a solution that does not necessarily requires definition of new IEs. Lastly, agreements reached until now do not support filling in the current last two columns of the table. Before doing this, discussions, either online or in a dedicated email discussion where these new IEs are presented, should take place. An alternative is to keep current text but mark everything with FFS as all solutions, except the *RealTime-Integrity* IE, are only tentative for now and not the only possibilities. |
| Convida | Yes, with comments | See comments in 3a. |
| ZTE | Partly yes | We are fine to add the examples of integrity indicators. Meanwhile, in New Integrity IE’s required column, we do not think YES should be used. From our point of view, RAN2 has not made consensus about whether new IEs are needed or how to modify existed IEs. We prefer to change all YES to FFS. |
| Spreadtrum | Partly yes | Replace “Relevant LPP Message” with “relevant IE” and change all YES to FFS for New Integrity IE column. |
| Xiaomi | Yes with comments | We prefer to delete the “relevant LPP message” and “New Integrity IEs required” columns, since we think it is too early to discuss it in SI phase. |
| Hexagon | Yes | We like to state that it cannot be assumed that the list of ‘External Feared Events’ is finite if very specific events are listed in the table, as further specific events may be identified. A better categorisation would be ‘Satellite’, ‘Atmospheric’ and ‘User environment signal events’.Additionally, the category ‘UE faults’ appears to be missing a sub-category ‘Software Faults’ category. |
| Swift Navigation | Yes | Some general comments on the above:As per Sections 9.3.1.1.1 and 9.4.1.1.1, for a complete integrity solution (safety-critical use cases in particular) the correction provider requires the ability to monitor the validity of the correction data (e.g. corrupt or invalid observations), for example using redundant processing chains, which enables the detection of these events at the network for indication to the UE.We anticipate the interface from the correction provider to the LMF will be implementation-defined. However, as per Section 9.4.1.1.2, integrity validation requires the integrity of the correction data to be validated end-to-end between the correction provider, LMF and/or UE. Therefore, it remains FFS whether existing protections in the 5GS are sufficient to ensure data integrity to the level required by a given TIR (e.g. CRCs have sufficient size). In addition we believe an end-to-end data integrity concept would have the advantage of avoiding the possibility of undetected data corruption while the data is being reformatted into LPP by the LMF (from the correction provider interface). To meet automotive “ASIL” standards (ISO-26262), any systems that handle (i.e. process or reformat) data that are not covered by end-to-end integrity protections additionally need to be ASIL certified; we believe that avoiding the need to ASIL certify the LMF will be advantageous to system implementation.We think Section 9.3.1.1.3 gives a useful introduction to the atmospheric feared events and the following text can be added to highlight why additional atmospheric indicators are necessary to ensure a given TIR can be met: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 alert limit 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. |

================================== START TP ==========================================

9.3 Positioning Integrity Error Categories

9.3.1 RAT-Independent

9.3.1.1 GNSS

Table 9.3.1.1 summarises the feared event categories which need to be considered in order to determine positioning integrity. Each of the feared event categories are further described in the following sections, and their relationship to the 3GPP positioning architecture is illustrated in Figure 9.3.1.1. Note that some relevant existing LPP messages have also been included, however these existing IEs are in support of positioning accuracy. New IEs to support integrity will in many cases be required as identified by the SI/WI.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feared Event Category** | **Feared Event Sub-Category** | **Relevant LPP Messages** | **Integrity Indicator Examples** | **New Integrity IEs required?** |
| 1. Faults in the correction data  | Incorrect computation by provider, e.g. software bug, corrupt or lost data |  | Validity or quality flags for existing assistance data IEs | Yes |
| External feared event impacting provider, e.g. station outages, or other external feared event, per (3) |
| 2. Faults in transmitting the data to the UE | Data integrity faults | FFS | Data corruption check, e.g. CRC | Maybe\* |
| Data Authentication / Signature | Maybe\* |
| 3. External Feared Events | Satellite feared events | *GNSS-RealTimeIntegrity* IE*GNSS-SSR-OrbitCorrections* IE*GNSS-SSR-ClockCorrections* IE*GNSS-SSR-CodeBias* IE*GNSS-SSR-PhaseBias* IE | Bad Signal in Space | Maybe\*, possible to re-use G*NSS- RealTimeIntegrity* |
| Bad Broadcast Navigation Data | Yes |
| Atmospheric feared events | *GNSS-SSR-STEC-Correction* IE*GNSS-SSR-GriddedCorrection* IE | Ionosphere disturbance | Yes |
| *GNSS-SSR-GriddedCorrection* IE | Troposphere disturbance | Yes |
| Multipath |  | N/A | No\*\* |
| Spoofing |  | FFS | FFS |
| Jamming/interference |  | FFS | FFS |
| 4. UE Faults | GNSS receiver measurement error |  | N/A | No\*\* |
| Hardware faults |  | N/A | No\*\* |

**Table 9.3.1.1: GNSS feared event categories for UE-based GNSS positioning integrity.**

**\*Maybe** means the parameters require further study to determine whether existing IEs can be utilized or extended.

**\*\*No** means it is not possible to mitigate with assistance data from the network, the UE is responsible for mitigating these feared events locally on implementation)



**Figure 9.3.1.1: Simplified relationship between the GNSS Integrity feared events and the 3GPP UE positioning architecture (GNSS).**

9.3.1.1.1 Faults in the correction data

1. Incorrect computation by the provider

GNSS correction networks collect and process GNSS measurements in order to be able to obtain estimations of various GNSS corrections (e.g., the satellite orbits, clocks, etc.). All impacted GNSS corrections are described in section 8.1 of TS 38.305.

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

1. External feared event impacting the provider

The correction service provider generates/computes the correction data employed to estimate the location of the UE. Any event affecting the quality of the generated data i.e., poor accuracy, will be considered as feared events impacting the provider.

This is different than the incorrect computation of the corrections, which are mainly due to wrong implementation of algorithms or corrupted data. These events comprise situations affecting the estimation process that happens at the correction provider, like not having enough data to compute the corrections (e.g. limited number of GNSS sensor stations recording measurements from GNSS satellites) or not having recent data (e.g. due to outages in the communications between the processing center and the GNSS sensor stations providing satellite measurements). The quality of the corrections will degrade with time and besides, even if the corrections are considered accurate enough, the satellite would not be recently monitored so any event happening at the satellite during the outage would go undetected.

A first approach to handle this type of events is to monitor these situations at the 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 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 Faults in transmitting the data to the UE

1. Data integrity faults

Data tampering i.e., 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 External feared events

1. Satellite feared events

Satellites can suffer HW failures and therefore enter into a mode in which they cannot broadcast a signal altogether 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.

1. 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. The effect is lower when the satellite is at the zenith than when it is near the horizon and it is frequency dependent. 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° [3]. 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 difficulty 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*. An individual quality indicator is missing and it can be easily added as a field to each of these IEs.

1. 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 the receiver is located within, 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 [3].

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

The effects of multipath are commonly assessed when the direct path signal is received unattenuated, 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.

1. Jamming

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.

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. For example, low-cost GNSS jammers have caused more than 50,000 disruptions between 2016 and 2018 in Europe alone.

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

1. 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 service providers have come to the help of users and 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, proving attestation to the integrity targeted by the navigation system. 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 reconstruct and use the solutions for signal/ranging authentication;
* Data Channel Authentication data: the navigation data and their authentication tags (digital signatures in the data stream of the GNSS broadcast).

The drawback to data authentication and ranging signal authentication is that they both endure an authentication delay. In other words, the user must wait for a period of time before they can despread the stored cryptographic precorrleation samples or evaluate the digital signature sent by the GNSS satellite. This delay is further increased by the fact that GNSS services are broadcast systems with very low data rates (50-150 bps) i.e., small data amounts need lots of time to be broadcast in full. Therefore, the time to retrieve such data directly from the GNSS signal can be high impacting the battery consumption.

The introduction of A-GNSS has partly solved the need for GNSS Data Authentication for UEs which can retrieve GNSS Navigation Message from 5GS through an LPP transaction instead from 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. In response to this emerging hazard, several spoofing mitigation strategies are under development by the GNSS service providers: cryptographic authentication of GNSS ranging signals and data channels by the core GNSS constellations (Galileo OS-Authentication, GPS-CHIMERA, BeiDou, and QZSS) although at this moment there is no operational service.

RAT-dependent positioning techniques could be used as independent means to cross-check the authenticity of 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 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 faults

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.

1. 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 GNSS modern 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.

1. Hardware faults

================================== END TP ===========================================

# 4. Integrity Methodologies

The following was noted at RAN2#112-e as an input to this email discussion:

* Text proposals from R2-2009333 and R2-2009003 (the table) to be taken into account in discussion [614].

Rapporteur’s Comments:

R2-2009333 [8] introduces UE-Based GNSS Integrity Methodologies, including proposed text corresponding to the feared event categories discussed in Section 3 above. R2-2009003 [9] presents an associated table describing how to support the network-assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining integrity. The detailed procedures and assistance data for these methods are intended to be defined WI phase. Both proposals (the text from [8] and the table from [9]) are adopted as a baseline for comment in this email discussion.

**Question 4: Do you agree with the table describing the network-assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining integrity? If not, please provide your reasoning and any suggested updates.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Yes but | We are generally fine with the table, but we think it would be more clear if we can provide some examples relating to “KPI” and “Integrity Results”, for instance:* KPIs (e.g. Alert Limit)
* Integrity results (e.g. Integrity event indication or PL)

By the way, we do have sympathy to Qualcomm’s concerns (in online session) regarding the term “UE faults”, perhaps we can change to something such as “impairment” ? No strong view about what terminology should be used in this regard. |
| InterDigital | Yes (with comments) | Table 9.4 provides a good overview of UE-based and LMF-based integrity methodologies, both of which are well described for MO-LR and MT-LR service types. However, some modification may be needed for clarification. In the case of LMF-based integrity MO-LR service, it is indicated in Table 9.4 that the KPIs and UE faults are sent by UE as assistance data in LPP. At this stage, it is not clear if this uses the existing assistance data transfer procedure (with enhancements) or the location transfer procedure in LPP. Also, it is not clear if the KPIs for UE-based MT-LR and LMF-based MO-LR are delivered via LPP since some/all KPIs (i.e. assuming AL, TTA and TIR) can be application specific. In light of this, the details in Table 9.4 may be slightly revised by indicating only the source of KPIs and including a Note stating that LPP may be used for delivering certain KPIs. |
| Fraunhofer | Yes |  |
| ESA | Partly | We agree with many items listed in the table but this is not complete work. It should be made clear that this is FFS. We haven´t had even one single online discussion on these items and we think there is no rush on the methodology side. |
| Convida | Yes, but with comments | We have doubts as far as specification impacts of “UE faults” and appropriate standardized mitigation. Perhaps some specific examples/scenarios would be helpful as well as a relationship to A-GNSS errors already defined, e.g. *GNSS-TargetDeviceErrorCauses*. |
| ZTE | Partly Yes | The note at the bottom of the table is not clearly enough. RAN2 has not made consensus about which part in the system is responsible for the error source factors. Though there is a note at the end of the table and mentioned that “**NOTE: the details are to be discussed in WI phase.**”, the content in the table e.g.LPP (from UE), LPP (from LMF) in KPI&Error source columns, may misunderstanding that the UE&LMF are responsible for all integrity related parameters. We prefer to add one more note as below:**NOTE: the details are to be discussed in WI phase.** **NOTE: Whether LMF or UE has capability for the responsibility of the integrity related parameters is FFS.** |
| Spreadtrum | Yes with comments | For the spec impacts, we would like to add capability to support integrity as FFS. |
| Xiaomi | Yes with comments | Regarding the MO-LR, UE may be better to report the integrity result to network when the positioning system is unavailable (PL>AL).  |
| Swift Navigation | Yes | Further to the comments, we agree with adding examples of the KPIs and Integrity results and agree with noting the procedures are FFS.We reiterate from Sections 9.3.1.1.4 and 9.4.1.1.4 that the UE faults are implementation-dependent and outside the scope of the study. We have added general comments to the table for consideration as part of the WI phase, in light of online discussions and related submissions to date. |

**Question 5: Do you agree with the text descriptions for UE-Based GNSS Integrity Methodologies provided in the text proposal below? If not, please provide your reasoning and any suggested updates.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Nokia | Partly  | Correction Data Quality Indication : in most situations, “lost, corrupt or invalid observations, software bugs” are unknown by both the correction service providers and the mobile service providers. The reliability and usefulness of such an indicator would therefore be questionable. Data Transmission Fault Detection : Adding such security layer on top of the 5G security layer seems redundantRest of the section : OK |
| InterDigital | Yes (with comments) | We are generally fine with the TP. We have a comment on Section 9.4.1.1.4. This section appears to be referring feared events at UE. Is this the same as UE faults? There also appears to be a contradiction with Table 9.3.1.1 (on error sources) where it is indicated that assistance data related to UE faults is not needed. As such, further clarification may be needed to describe what are the integrity indicators (related to UE feared events) that are provided in assistance data to the UE, which the UE can then use in its internal function. If some of the aspects in this section also covers faults in the network, then perhaps the text should be modified and covered under different feared event category (e.g. transmission system in 9.4.1.1.2). |
| Fraunhofer | Yes (with comments) | Even for UE-based positioning, if the integrity fault detected by the UE is also relevant to other UEs, then it might be advantageous if such events are reported to the NW. |
| ESA | Partly | Are these the only possible solutions allowed? Can additional items be considered? Again, I think we need to discuss this online before advancing further.Lastly, we would also add a section for UE-assisted as FFS. |
| Convida | Yes, but with comments | Clarity on what is in scope or out of scope for specification enhancements and methodologies would be beneficial. Change text, e.g. “independent of 3GPP” and “implementation-defined” wording to, e.g. “outside the scope of this TR”. |
| ZTE | Almost Yes | Wording issue. Considering we are discussing the error sources in RAT-independent positioning methods, the title of 9.4.1.1 should be changed as below:9.4.1.1 UE-Based A-GNSS Integrity Methods |
| Spreadtrum | Yes with comments | We think that UE-assisted should be added as FFS. |
| Xiaomi | Yes with comments | For UE Feared Event Detection, we think we could only describe that the network can provide assistance information to UE and UE can report detection results to network.  |
| Hexagon | Yes | We would like to comment that section 9.4.1.1 refers to detection of ‘GNSS feared events’, whilst it would be more appropriate the talk about detection of feared events at system level, i.e. more widely. GNSS is a significant part of the overall end-2-end system, however it is not the only component that can be a cause of fault, as table 9.3.1.1 has already indicated. |
| Swift Navigation | Yes | In order to provide a rigorous treatment of integrity, we believe that this SI should aim to enumerate a complete list of feared events. This is necessary before deciding which feared events will have specification impacts. Our view is that UE faults are UE feared events which should be included in the table, but ultimately are out of scope of 3GPP to monitor and mitigate in the UE-based case. Whether and which UE faults should be reported to the LMF for LMF-based positioning is FFS. |

================================== START TP ==========================================

9.4 Positioning Integrity Methods

Table 9.4 provides an overview of the network-assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining integrity, which are further described in the following sections.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Integrity method** | **Location service type** | **KPIs** | **Integrity results** | **Error sources** | **Spec impact** |
| Network assisted (for UE based positioning) | MO-LR | Obtained via UE internal implementation; | Keep inside the UE | LPP (from LMF): Faults in the correction data, Faults in transmitting the data to the UE, External feared eventsUE internal implementation: UE faults | Assistance data in LPP (from LMF) to include:Faults in the correction data, Faults in transmitting the data to the UE, External feared events; |
| MT-LR | LPP (from LMF): KPIs  | LPP (from UE): integrity results; | LPP (from LMF): Faults in the correction data, Faults in transmitting the data to the UE, External feared eventsUE internal implementation: UE faults | Assistance data in LPP (from LMF) to include:* KPIs;
* Faults in the correction data, Faults in transmitting the data to the UE, External feared events;

LPP (from UE): integrity results; |
| UE assisted (for UE assisted positioning) | MO-LR | LPP (from UE): Obtained via UE internal implementation; | LPP (from LMF): integrity results; | LMF implementation: Faults in the correction data, Faults in transmitting the data to the UE, External feared eventsLPP (from UE): UE faults | Assistance data in LPP (from UE) to include:* KPIs;
* UE faults;

LPP (from LMF): integrity results; |
| MT-LR | LMF implementation: KPIs  | Keep inside the LMF | LMF implementation: Faults in the correction data, Faults in transmitting the data to the UE, External feared eventsLPP (from UE): UE faults | Assistance data in LPP (from UE) to include:* UE faults;
 |

**Table 9.4: Summary of network assisted (UE-Based) and UE-assisted (LMF-Based) methods for determining Integrity. NOTE: the details are to be discussed in WI phase.**

9.4.1 RAT-Independent

9.4.1.1 UE-Based GNSS Integrity Methods

Detection of GNSS feared events is necessary to support positioning integrity by ensuring the TIR can be met. This section lists the GNSS feared event categories and identifies from which entities of the system they may originate, as well as how the assistance data can be indicated.

9.4.1.1.1 Correction Data Quality Indication

The 3GPP network-assistance data can be used to indicate potential faults in the correction data processing itself, as determined by the corrections service provider systems. If the GNSS correction data processing encounters an error that degrades or impacts the validity of the correction data (e.g. lost, corrupt or invalid observations, software bugs; or external feared events such as satellite failures), and the service provider is capable of monitoring and detecting these feared events, the quality of the correction data can be indicated to the UE. As noted in Table 2, there are no existing IEs corresponding to correction data quality, meaning new assistance data is needed. Signaling the Correction Data quality allows the UE to determine the impact of these events on its computed PL. Note that often the correction data may still be sent even if not indicated as high enough quality for integrity purposes, as it is still of sufficient quality to improve accuracy even though integrity cannot be ensured.

9.4.1.1.2 Data Transmission Fault Detection

Data integrity ensures that the end-to-end data transmission link needed to signal integrity assistance data across the network is secure and free from the possibility of data corruption, including the data link to the corrections service provider. Data integrity algorithms and related security architectures for the 5G system are individual work areas in 3GPP [16].

A related observation in the context of this SI (further addressed in Section ‘9.4.1.1.5 - Data Validation’ below) is that industry-specific functional safety standards (e.g. ISO-26262 for Automotive, IEC 62278 for Rail) are also required to validate integrity compliance for a given implementation. These standards include requirements that may be outside of the current RAN architecture. For example, consider the typical service interface between a corrections service provider sending GNSS assistance data to the UE via the NG-RAN. Both the correction service provider and UE can be designed and qualified with integrity compliance. However, the NG-RAN architecture, although rigorously specified with data security and integrity features in [6], may not comply with industry-specific functional safety standards by default. This implies that the integrity of the data transmission from the correction provider to the UE needs to be trusted and assured without any alterations via the NG-RAN.

One method for achieving this is by providing for the data to be signed by the correction provider and verified by the UE in accordance with the relevant functional standards[[3]](#footnote-3). Once the data has left the correction provider, any changes to the data would invalidate the certificate. This in turn means that, irrespective of whether the 3GPP architecture is compliant to the functional safety standards, appropriate procedures can be implemented to sign and verify the network integrity assistance data with minimal impacts to the NG-RAN – i.e. the NG-RAN can still be leveraged as an efficient data link. Further investigation is required through the SI/WI to determine whether new data integrity IEs are needed for positioning integrity or whether existing data integrity IEs are sufficient (e.g. to carry a data signature from the corrections service provider to the UE).

9.4.1.1.3 External Feared Event Detection

The correction service provider systems can be used to detect the feared events which occur external to the correction networks and the UE equipment (e.g. GNSS feared events and atmospheric gradients). New assistance data can be defined in LPP to indicate these events to the UE via the NG-RAN, which in turn reduces overhead on the UE by offloading integrity monitoring to the network. It also enables the potential to achieve lower TIRs given the added monitoring and detection capabilities of the network. These methods are further described below.

In practice, feared events detected by the corrections service provider mean that, even outside the probability of a fault occurring (e.g. recognizing these probabilities can be estimated using threat models [5][7]), the correction network itself can be used to detect if the actual event occurs. For example, the correction provider network typically has the benefit of many GNSS reference stations distributed over a wide area. This additional observability can result in more effective detection of these events, removing the burden on the UE to detect them unassisted, and potentially increasing the probability with which these events can be detected (i.e. given the UE alone does not have the benefit of cross-checking data from surrounding GNSS reference stations). Examples of GNSS external feared events include satellite feared events, such as loss of signal, clock errors and constellation failures, and atmospheric feared events, such as large ionospheric and tropospheric gradients.

In addition to the network providing integrity assistance data corresponding to the detection of feared events, the network may also provide to the UE certain threat model parameters, allowing them to be updated based on the evolving operational history of the GNSS constellations. An example of this is found in the ARAIM Integrity Support Message (ISM) which contains parameters such as the assumed probability of satellite failure [7]. The scope of this SI is not intended to standardize the integrity algorithms implemented by the corrections service provider to detect the feared events. The study identifies the common set of feared events that can be indicated to the UE by specifying network-assistance data IEs.

9.4.1.1.4 UEeared Event Detection

UE-detected feared events depend on the hardware and software capabilities of the equipment and its internal integrity algorithms. This SI does not attempt to standardize the GNSS integrity algorithms at the network or the UE, but rather the network-assistance data needed to transport the integrity indicators derived from the algorithms. A UE may simply report the measurements or detected integrity event and its characteristics (such as interference or spoofing) subject to its capabilities to the LMF, which may make use of the available information to compute the UE position or use it to determine integrity assistance to the UE. The assistance data can then be applied by the UE’s GNSS positioning function (i.e. independent of 3GPP).

This same logic applies to how the RTK and SSR GNSS assistance data has been standardized in previous 3GPP releases – i.e. the RTK and SSR algorithms used to derive GNSS corrections are implementation-defined. The assistance data used to transport the derived corrections are specified in LPP.

9.4.1.1.5 Positioning Integrity Validation

Positioning integrity can only be validated end-to-end, per-implementation. Validation requires a comprehensive Fault-Tree Analysis (as described in [5]) and a complete qualification dossier (e.g. documentation, methodologies, tests and traceability through the entire integrity qualification process).

Integrity validation is particularly crucial for safety-critical applications such as Automotive and Rail. Integrity validation takes into consideration a much wider suite of requirements than the assistance data used to supply the GNSS integrity parameters. For example, this includes the hardware components (e.g. ISO-26262 certified hardware and CPUs), tooling (e.g. ASIL-qualified compilers), software architecture design, safety manuals, test procedures etc, all of which vary for each integrity implementation. While 3GPP integrity assistance data is just one of multiple inputs for integrity validation, defining a standardized set of GNSS integrity assistance data ensures a wider ecosystem of connected devices can readily benefit from knowing what inputs are available from the network to support integrity validation.

================================== END TP ==========================================

# 5. Summary

# References

[1] R2-2010577 TP for TR 38.857 Study on NR Positioning Ericsson, Swift Navigation report Rel-17 38.857

[2] R2-xxxxxx RAN2-112-e-Positioning-Relay-2020-11-05-1615,

<https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_112-e/Inbox/Chairmans_Notes>

[3] R2-2009129 Summary of [Post111-e][626][POS] Email Discussion on integrity use cases and specification

impacts Swift Navigation

[4] R2-2008812 Discussion on error sources, threat models, occurrence rates and failure modes CATT

[5] R2-2009331 Discussion on GNSS Integrity Errors Swift Navigation, Ericsson, Intel Corporation, u-blox

[6] R2-2010073 GNSS position integrity error sources Ericsson

[7] R2-2010061 Text Proposal on GNSS position integrity error sources ESA

[8] R2-2009333 TP for GNSS Integrity Methodologies Swift Navigation, Ericsson, Intel Corporation, u-blox

[9] R2-2009003 Methodologies for network-assisted and UE-assisted integrity Intel Corporation, Swift Navigation

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 exceed the required AL, potentially leading to an integrity event. 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 integrity methodologies allow an 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)
3. Note that the requirements called out by integrity standards such as ISO-26262 can be extremely onerous for any entity that “processes” (i.e. modifies in any way) the data. This possibly includes use of qualified tools such as special compilers, as well as using ISO-26262 certified hardware and CPUs to perform the processing. [↑](#footnote-ref-3)