3GPP TSG-RAN WG2 Meeting #113-e***R2-20xxxxx***

Electronic, January XXXXX, 2020

**Agenda item:** 8.XX.X

**Source:** Swift Navigation

**Title:** [Post112-e][618][POS] - Error Sources Text Proposal

**Document for:**  Discussion and Decision

# 1. Introduction

This document contains the updated Error Sources text proposal (originally submitted as R2-2010878 [1] to RAN2#112-e) based on feedback from the following email discussion [2], which also includes [3][4]:

[Post112-e][618][POS] Finalise integrity text proposals (Swift)

Scope: Refine the text proposals in R2-2010877/R2-2010878/R2-2010879.

Intended outcome: Agreeable TPs

Deadline: Long

The email discussion was undertaken in two phases which are recorded in Appendix A (Phase 2) and Appendix B (Phase 1) below. The appendices will be removed in the final Tdoc submission but are included here for review.

# 2. Moderator Summary

The following section reviews the comments on each individual proposal in Phase 2. The company responses were recorded as ‘Yes’ unless otherwise stated in the comments.

* **Proposal 1: Rename ‘External feared events’ to ‘GNSS feared events’ in the draft TP.**
  + Yes (8): Vivo, Swift, Huawei, Qualcomm, Apple, InterDigital, ZTE ESA
  + See comments (1): OPPO
* **Moderator:** Further to the comments from OPPO, the example in the table was updated to align with the updated text in 9.3.1.1.1b, i.e., “e.g. station outages, or other GNSS feared event (Category 3)” was updated to “e.g. satellite, atmospheric or local environment feared events (Category 3) impacting the GNSS reference stations in the provider’s network” – refer to Proposal 12 below.
* **Proposal 2: Add the following Editor’s Note: GNSS feared events are those which occur external to the UE.**
  + Yes (8): Vivo, Swift, Huawei, Qualcomm, Apple, InterDigital, ZTE, ESA (with comments)
  + See comments (1): OPPO
* **Moderator:** Editor’s note was updated as follows based on comments from ESA and OPPO: ‘GNSS feared events are those which occur external to the UE and potentially impact the quality and availability of the GNSS signals’.
* **Proposal 3: Add LMF feared events (9.3.1.1.5) for consideration in the study, noting the specification impacts, if any, are FFS.**
  + Yes (6): Swift, OPPO, Qualcomm, InterDigital, ZTE, ESA
  + See Comments (2): Huawei, Apple,
  + No (1): Vivo
* **Moderator:** Further to the comments from Vivo, Apple and Huawei, hardware/software faults in the LMF can be handled outside of the specification, which is also captured as a ‘\*NOTE’ in table 9.4.1.1.6 (Methodologies). Given the general level of support from companies on this proposal, and the fact that in UE-assisted scenarios the LMF is responsible for computing the Protection Level, we still think it is useful to enumerate a full list of potential feared event categories as a basis for then identifying (as indicated by the NOTE above) which are in scope or out of scope of the specifications through this study. Refer to Proposal 12 for further detail.
* **Proposal 4: Rename ‘Feared events in transmitting data to the UE’ to ‘Feared events during positioning data transmission’.**
  + Yes (9): All
* **Moderator:** Captured in the text proposal.
* **Proposal 5: Rename ‘error sources’ to ‘feared events’.**
  + Yes (9): All
* **Moderator:** Captured in the text proposal.
* **Proposal 6: Retain the ‘incorrect computation by provider’ feared event, noting the specification impacts, if any, are FFS.**
  + Yes (7): Vivo, Swift, Huawei, Apple, InterDigital, ZTE, ESA (with comments)
  + See Comments (1): OPPO
  + No (1): Qualcomm
* **Moderator:** Regarding the comments from OPPO, it was described in Section 9.4.1.1 of R2-2010879 that the corrections from the GNSS network may still be of sufficient quality to improve positioning accuracy but not valid to use for positioning integrity, which is why they need to be flagged. Regarding Qualcomm’s and ESA’s comments, to avoid further confusion we propose an amended version of the ESA suggestion (also captured in the text proposal in Section 3):
  + **9.3.1.1:** Feared events in the GNSS Assistance Data
  + **9.3.1.1.1a:** Incorrect computation of the GNSS Assistance Data
  + **9.3.1.1.1b:** External feared event impacting the GNSS Assistance Data
* **Proposal 7: Retain the hardware and software faults for UE feared events, noting specification impacts, if any, are FFS.**
  + Yes (8): Swift, OPPO, Huawei, Qualcomm, Apple, InterDigital, ZTE, ESA
  + See Comments (1): Vivo
  + No (0):
* **Moderator:** Regarding the comments from Vivo, Editor’s Notes are already included in Section 9.3.1.1.4.
* **Proposal 8: Rename ‘Provider’ to ‘Positioning Service Provider’ with an associated Editor’s Note: the Positioning Service Provider is the external source (non-3GPP) of positioning integrity assistance data.**
  + Yes (7): Vivo, Swift, OPPO, Huawei, Apple, ZTE
  + See Comments (1): InterDigital
  + No (2): Qualcomm, ESA
* **Moderator:** Refer to moderator comments and changes in Proposal 6. The term ‘provider’ has also been clarified as ‘GNSS corrections provider’ in the associated text descriptions to avoid confusion – refer to track changes. There is no proposal to alter the meaning of ‘provider’ in the 3GPP specifications.
* **Proposal 9: Rename Correction Data to Assistance Data.**
  + Yes (5): Vivo, Swift, Qualcomm, Apple, ESA
  + See Comments (4): OPPO, Huawei, InterDigital, ZTE
  + No (0):
* **Moderator:** Further to Proposals 6 and 8, Category 1 is renamed ‘Feared events in the GNSS Assistance Data’, recognizing GNSS Assistance Data is the 3GPP terminology for the GNSS corrections supplied by the external GNSS corrections provider. The GNSS Assistance Data IEs and procedures for positioning integrity are not yet defined – they are FFS in the WI.
* **Proposal 10: Rename Section 9.3.1.1 to ‘A-GNSS Feared Events’**
  + Yes (9): All
* **Moderator:** Captured in the text proposal.
* **Proposal 11: Add a new Section (9.3.1.1.6) titled ‘Summary of A-GNSS Feared Event Considerations’.**
  + Yes (7): Swift, OPPO, Huawei, Qualcomm, Apple, InterDigital, ESA
  + See Comments (0):
  + No (2): Vivo, ZTE
* **Moderator:** Refer to proposal 12 below.
* **Proposal 12: Add the proposed Table (9.3.1.1.6):**
  + Yes (5): Swift, OPPO, InterDigital, ZTE, ESA (with clarifications)
  + See Comments (1): Apple
  + No (2): Huawei, Qualcomm
* **Moderator:** Regarding Qualcomm’s comments, refer to Proposals 6 and 8 above. Further to comments in Phases 1 and 2, rather than adding a new section and duplicating parts of the table, we can instead use table 9.4.1.1.6 which already summarizes this content. NOTE: Table 9.4.1.1.6 is renumbered to 9.4.1.1 in [4].
* **Proposal 13: The integrity models/algorithms for mitigating feared events for GNSS positioning integrity are defined by the service implementation and therefore out of scope of this study.**
  + Yes (8): Swift, OPPO, Huawei, Qualcomm, Apple, InterDigital, ZTE, ESA.
  + See Comments (1): Vivo
  + No (0):
* **Moderator:** Regarding Vivo’s comment, we think the updates above clarify that it is the assistance data which is used to mitigate the feared events, as per table 9.4.1.1.6.
* **Proposal 14: Agree to adopt the ‘Error Sources’ TP as the baseline text for the TR.**
  + Yes (6): Swift, OPPO, Huawei, InterDigital, ZTE, ESA (with comments)
  + See Comments (3): Vivo, Qualcomm, Apple
  + No (0):
* **Moderator:** Refer to moderator comments and updates to the text proposal in Section 4.

# 3. Conclusion

## 3.1 Easily agreeable

**Proposal 1: Rename ‘External feared events’ to ‘GNSS feared events’ in the draft TP and include the following 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.**

**Proposal 2: Rename ‘Feared events in transmitting data to the UE’ to ‘Feared events during positioning data transmission’.**

**Proposal 3: Rename ‘error sources’ to ‘feared events’.**

**Proposal 4: Retain the hardware and software faults for UE feared events, noting specification impacts, if any, are FFS.**

**Proposal 5: Rename Section 9.3.1.1 to ‘A-GNSS Feared Events’**

**Proposal 6: The integrity models/algorithms for mitigating feared events for GNSS positioning integrity are defined by the service implementation and therefore out of scope of this study.**

## 3.2 May require further discussion

**Proposal 7: Add LMF feared events (9.3.1.1.5) for consideration in the study, noting the specification impacts, if any, are FFS.**

**Proposal 8: Rename ‘Feared events in the assistance data’ to ‘feared events in the GNSS Assistance Data’.**

**Proposal 9: Rename ‘Incorrection computation by the provider’ to ‘incorrect computation of the GNSS Assistance Data’.**

**Proposal 10: Rename ‘External feared event impacting the provider’ to ‘External feared event impacting the GNSS Assistance Data’.**

**Proposal 11: Agree to adopt the ‘Error Sources’ TP as the baseline text for the TR.**

**Are there any remaining questions or comments to be addressed in this email discussion for the Error Sources text proposal?**

|  |  |
| --- | --- |
| **Company** | **Comment** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 4. Text Proposal

*Start of Text Proposal*

## 9.3 Positioning Integrity Error Categories

### 9.3.1 RAT-Independent

#### 9.3.1.1 A-GNSS Feared Events

This section describes 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 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 handle 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 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*. 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. 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 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 systems providers offer protection against jamming by 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 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.

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 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 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.

###### 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

*End of Text proposal*

# References

[1] R2-2010878 TP on Integrity Error Sources, Swift Navigation.

[2] R2-xxxxxx [RAN2-112-e-Positioning-Relay-2020-11-13-1745\_eom.docx](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_112-e/Inbox/Chairmans_Notes/RAN2-112-e-Positioning-Relay-2020-11-13-1745_eom.docx),

<https://www.3gpp.org/ftp/tsg\_ran/WG2\_RL2/TSGR2\_112-e/Inbox/Chairmans\_Notes>.

[3] R2-20xxxxx Email Discussion [618] TP on Integrity KPIs and Use Cases\_Draft

[4] R2-20xxxxx Email Discussion [618] TP on Integrity Methodologies\_Draft

1. PHASE 2

# 1. PHASE 2 - Introduction

This document is Phase 2 of the following email discussion [1][2][3]:

[Post112-e][618][POS] Finalise integrity text proposals (Swift)

Scope: Refine the text proposals in R2-2010877/R2-2010878/R2-2010879.

Intended outcome: Agreeable TPs

Deadline: Long

It should be reviewed alongside the other email discussion documents:

* Email Guideline - [Post112-e][618][POS] Integrity TPs [3]
* [618] KPIs and Use Cases – PHASE 2 Draft TP [4]
* [618] Methodologies – PHASE 2 Draft TP [5]

# 2. PHASE 2 – Moderator Summary

A summary of key topics from Phase 1 (Appendix B) is provided below. The summary is grouped based on the common themes raised in Questions 1 to 3 rather than individual summaries for each question.

## 2.1 External feared events

Vivo, ZTE and ESA suggested further clarification is needed to distinguish ‘External feared events impacting the provider’ (9.3.1.1.1b) vs ‘External feared events’ (9.3.1.1.3). ESA suggested renaming 9.3.1.1.3 to ‘GNSS feared events’ since the described effects relate to the GNSS systems and signals.

**Proposal 1: Rename ‘External feared events’ to ‘GNSS feared events’ in the draft TP.**

**Proposal 2: Add the following Editor’s Note: GNSS feared events are those which occur external to the UE.**

## 2.2 LMF feared events

Swift Navigation and ESA proposed to include LMF faults/feared events to address the case for UE-assisted. InterDigital and OPPO agreed that feared events for both the UE-based and UE-assisted methods should be classified. CATT disagreed that LMF faults need to be considered for UE/LMF or LMF/AMF interactions. ESA thinks that the LMF faults are relevant to both UE-based and UE-assisted.

**Proposal 3: Add LMF feared events (9.3.1.1.5) for consideration in the study, noting the specification impacts, if any, are FFS.**

This topic also related to the comments raised by ZTE, ESA and Swift Navigation on generalizing the list of error sources/feared events to accommodate both the UE-based and UE-assisted cases. Specifically, two options were proposed for updating the name of category 2 (‘feared events in transmitting data to the UE’):

1. ‘Feared events in transmitting data within the 3GPP system’ (Swift Navigation).
2. ‘Feared events during positioning data transmission’ (ZTE, supported by ESA).

**Proposal 4: Rename ‘Feared events in transmitting data to the UE’ to ‘Feared events during positioning data transmission’.**

## 2.3 Error Sources or Feared Events?

Hexagon, ESA and u-blox proposed to rename error sources to be ‘feared events’ given error sources are handled separately through GNSS augmentation (i.e. to correct for positioning accuracy).

**Proposal 5: Rename ‘error sources’ to ‘feared events’.**

Huawei proposed to regroup the four categories of error sources/feared events under two categories: ‘Internal’ and ‘External’ feared events. Moderator notes there is already broad support on the current grouping (with clarifications on naming herein). Moderator also notes that External feared events are those which are external to the UE (including satellite feared events).

## 2.4 Incorrect computation by provider

Nokia and OPPO noted that ‘incorrect computation by the provider’ (9.3.1.1.1a) may not be relevant to 3GPP and should be removed. CATT suggested clarification is needed on who checks the validity and which data applies the CRC.

Moderator notes that there has been previous support to include a full list of feared events for consideration in the SI, such that the relevant feared events with specification impacts can be identified.

**Proposal 6: Retain the ‘incorrect computation by provider’ feared event, noting the specification impacts, if any, are FFS.**

## 2.5 UE feared events

CATT and Xiaomi proposed to remove hardware and software UE faults given these are part of the UE implementation. U-blox also had reservations on including these faults but noted in Question 2 that they may be needed for UE-assisted. The remaining comments from other companies generally supported the error sources/feared events currently listed.

Moderator notes that the UE hardware and software faults in the case of UE-based were already labelled in Table 9.4.1.1.6 as *‘\*\*not possible to mitigate with assistance data from the network, the UE is responsible for mitigating these feared events locally’*. Further to Proposals 3 and 6, Moderator suggests that a complete list of positioning integrity feared events should first be identified in order to determine what is in and out of scope of the specifications, to be finalized in the WI

**Proposal 7: Retain the hardware and software faults for UE feared events, noting specification impacts, if any, are FFS.**

## 2.6 Who is the Provider?

ESA sought clarification on whether ‘Provider’ refers to the MNO or the owner of the GNSS CORS network? Qualcomm also raised this topic in Question 2 of the Methodologies TP [5], noting ‘From a UE point of view, the "service provider" is the network operator from which a UE obtains service (i.e., subscription). How (if at all) a network operator or deployment obtains assistance data from external sources is beyond the scope of 3GPP’.

With reference to Figure 9.4.1.1.6, Moderator notes that the intended meaning is the external source, as proposed by Qualcomm, i.e. the GNSS positioning service provider supplying the integrity assistance information to the LMF. Moderator also notes the not all CORS network operators provide GNSS positioning and integrity services. Therefore,

**Proposal 8: Rename ‘Provider’ to ‘Positioning Service Provider’ with an associated Editor’s Note: the Positioning Service Provider is the external source (non-3GPP) of positioning integrity assistance data.**

## 2.7 Correction Data or Assistance Data?

ESA proposed to rename Correction Data to Assistance Data.

**Proposal 9: Rename Correction Data to Assistance Data.**

## 2.8 Summary of error sources/feared events

There was a general consensus in the responses to include a table which summarizes the error sources/feared events described in Section 9.3.1.1. Swift Navigation proposed to include a modified version of Table 9.4.1.1.6 containing only columns 1 and 2 and the updated naming from the Phase 2 proposals herein. The Moderator also proposes that the headings for columns 1 and 2 also need switching, i.e. the four categories of feared events are column 1, and the feared events corresponding to these categories are column 2. ESA suggested adopting only one table rather than a second modified version in the Methodologies TP (which also includes examples of integrity assistance information, FFS).

The following proposals are subsequently made:

**Proposal 10: Rename Section 9.3.1.1 to ‘A-GNSS Feared Events’**

**Proposal 11: Add a new Section (9.3.1.1.6) titled ‘Summary of A-GNSS Feared Event Considerations’.**

**Proposal 12: Add the proposed Table (9.3.1.1.6):**

**Table 9.3.1.1.6: Summary of A-GNSS feared event for considerations (FFS).**

|  |  |
| --- | --- |
| **Feared Event Category** | **Feared Events (specification impacts are FFS)** |
| 1. Feared events in the assistance data | Incorrect computation by positioning service provider,  e.g. software bug, corrupt or lost data |
| External feared event impacting positioning service provider,  e.g. station outages, or other GNSS feared event (Category 3) |
| 2. Feared events during positioning data transmission | Data integrity faults |
|
| 3. GNSS feared events | Satellite feared events  e.g. bad signal-in-space or bad broadcast navigation data |
|
| Atmospheric feared events |
|
| Local Environment feared events,  e.g. Multipath, Spoofing, Interference |
| 4. UE feared events | GNSS receiver measurement error |
| Hardware faults |
| Software faults |
| 5. LMF feared events | Hardware faults |
| Software faults |

## 2.9 Other

Vivo, ESA, CATT and u-blox all provided additional comments within the draft TP itself. Each of these comments have received an initial response from the Moderator in Appendix B under the author name of ‘Swift Navigation’. If the issues require further discussion, companies are encouraged to use the comments table to provide their feedback.

Huawei also proposed to include additional descriptions on how each error source influences positioning integrity. Moderator suggests new descriptions can be contribution-led in Phase 2.

Huawei also proposed to study positioning integrity models/algorithms for mitigating the feared events. It is understood from the other company comments below (along with those provided in the Methodologies TP [5]) that this study focuses on methods for signaling the assistance information rather than studying the integrity models/algorithms for mitigating the feared events, which are defined by the service implementation.

**Proposal 13: The integrity models/algorithms for mitigating feared events for GNSS positioning integrity are defined by the service implementation and therefore out of scope of this study.**

## 2.10 Summary of Phase 2 Proposals

**Proposal 1: Rename ‘External feared events’ to ‘GNSS feared events’ in the draft TP.**

**Proposal 2: Add the following Editor’s Note: GNSS feared events are those which occur external to the UE.**

**Proposal 3: Add LMF feared events (9.3.1.1.5) for consideration in the study, noting the specification impacts, if any, are FFS.**

**Proposal 4: Rename ‘Feared events in transmitting data to the UE’ to ‘Feared events during positioning data transmission’.**

**Proposal 5: Rename ‘error sources’ to ‘feared events’.**

**Proposal 6: Retain the ‘incorrect computation by provider’ feared event, noting the specification impacts, if any, are FFS.**

**Proposal 7: Retain the hardware and software faults for UE feared events, noting specification impacts, if any, are FFS.**

**Proposal 8: Rename ‘Provider’ to ‘Positioning Service Provider’ with an associated Editor’s Note: the Positioning Service Provider is the external source (non-3GPP) of positioning integrity assistance data.**

**Proposal 9: Rename Correction Data to Assistance Data.**

**Proposal 10: Rename Section 9.3.1.1 to ‘A-GNSS Feared Events’**

**Proposal 11: Add a new Section (9.3.1.1.6) titled ‘Summary of A-GNSS Feared Event Considerations’.**

**Proposal 12: Add the proposed Table (9.3.1.1.6):**

**Proposal 13: The integrity models/algorithms for mitigating feared events for GNSS positioning integrity are defined by the service implementation and therefore out of scope of this study.**

**Proposal 14: Agree to adopt the ‘Error Sources’ TP as the baseline text for the TR.**

**Question 1: Do you agree with Proposals 1 to 14? If not, please identify the specific proposal(s) you want to discuss and why.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| vivo |  | Yes: 1,2,4,5,6,8,9,10  No: 3(no need to include LMF feared event. It should be part of assistance data),  11(we need this summary, but don’t need separately add a new section, it can be included at 9.3.1.1)  FFS: 7(we can include UE feared event, but for category or context FFS)  13(agree study of these are out of scope, but need clarify assistant data of models and algorithms are specified, if any FFS)  14(As we indicated the category is not applicable, LMF feared event should be removed) |
| Swift Navigation | Yes |  |
| OPPO | See comment | For P1/2, now still the difference between 9.3.1.1.1b and 9.3.1.1.3 is not clear, i.e., as stated in the updated table 9.3.1.1.6, “e.g. station outages, or other GNSS feared event (Category 3)”  For P6, by reading the description in 9.3.1.1.1a, “In any case these events are handled by the provider by performing consistency checks on the input data, checking the validity of the corrections before sending them and applying CRCs”, the puzzling point for us is this seems to be a checking step, performed by service provider before sending the correction data out. In that case, this would not lead further information sent out to 3GPP and forwarded to UE. On the other hand, this category (9.3.1.1.1 as a whole) is listed in the discussion of “Methodology” as a part of assistance data to be specified, so seems a bit contradictory to us.  For P9, this renaming seems misleading: on the one hand, “Assistance Data” is used in 3GPP to associate with specific information / messages in LPP, while our understanding here the original definition is for “Correction Data” which is from service provider (we have not fully understood the definition as commented for P6). |
| Huawei/HiSilicon |  | * Not support: P9/12   For P9: Agree with OPPO. The difference between assistance data and correction data should be clarified.  For P12: We don’t see any need to add this table since P11 already mentioned to add a new section for the summary for the feared events.   * FFS: P3   No need to add another section for LMF feared events, which can be included in 9.3.1.1.1. Also, Table 9.4.1.1.6 does a similar summary. |
| Qualcomm | Partly | "No" for:  P6: ‘incorrect computation by provider’ does not need to be an event. The "provider" is an LMF in an operator's network; i.e., can be the same as P3.  P8: There is no need to introduce a "Positioning Service Provider" in the specifications. We also do not have such Provider for basic A-GNSS assistance data, or RTK, assistance data etc. The "Positioning Service Provider" is the network operator for which a target has a subscription.  P12: Based on comments for P6/8 above.  P14: Based on comments for P6/8/12 above. |
| Apple | See comment | We do not agree with the following proposal:  P3: LMF does not generate correction data, so the data are provided by external service providers. Basically, the erros in those data are not LMF faults. In general, we have concerns to characterize the LMF faults, a faulty LMF will affect all the UEs in the network and can cause very severe problems for millions of UEs using either A-GNSS or RAT-dependent methods. The proposed 3GPP integrity work is not the right remedy for such a failure. Although the intention is to capture all potential faults, we still need to focus on the events which can be tackled with the proposed 3GPP work.  P12/P14: Pending on the comments on P4 above |
| InterDigital |  | In general, we are ok with the proposals. Regarding P8, we think further descriptions may be included in 9.3.1.1.1b on how handling of the external feared events by the Positioning Service Provider can impact the positioning/integrity procedures in 3GPP network. It may be beneficial to describe the information that can be provided to LCS client, LMF or UE when external feared events are encountered by the positioning service provider.  For P9, we also share similar concern expressed by Oppo as “assistance data” appears to have broader connotation (e.g. in LPP), whereas correction data is more specific to the type of feared events described in Section 9.3.1.1.1. For clarity, perhaps “Feared events related to GNSS corrections in the LPP assistance data” may be considered in the title of 9.3.1.1.1. and in Table 9.3.1.1.6. |
| ZTE |  | No: 9, 11.  P9: We prefer to combine the ideas from both OPPO and ESA. We also think Assistance Data may not clearly enough to describe all involved data we used for positioning integrity. But from other side, some of the current discussed “correction data” have already been used as Assistance Data in LPP& positioning SIBs in Rel-16(e.g tropospheric indicator in *GNSS-SSR-GriddedCorrection*).  Hence, in this TR, we may use Integrity Assistance Data to instead of either Assistance Data or Correction Data.  P11: If we can insert the table 9.3.1.1.6 at the head of clause 9.3.1.1, we do not need to add a new section(9.3.1.1.6). |
| ESA |  | Yes:  P1,  P2 (GNSS feared events are those which occur external to the UE **and impact the quality and availability of the GNSS ranging signals**),  P3  P4  P5  P6 (if renamed “incorrect computation of assistance data”)  P7  P9 – in 3GPP language, GNSS corrections are formally referred to as GNSS Assistance Data. The LPP works with Assistance Data (procedures and IEs) and we should keep the language consistent. We noticed that several companies are already confused and think that corrections and assistance data have different definitions.  P10  P11  P12 – with clarifications P6 and P8  P13  P14 – we think this TP is very mature and a solid basis for this objective of the SID. Having said that, we need to sort out the 9.3.1.1.1 taking into account feedback from companies.  No:  P8 – provider is an MNO. We would suggest to limit our analysis to what is generally part of the NG-RAN positioning architecture. |

# 3. PHASE 2 – Text Proposal

The following text proposal includes the changes presented in Proposals 1 to 14 above.

*Start of Text Proposal*

## 9.3 Positioning Integrity Error Categories

### 9.3.1 RAT-Independent

#### 9.3.1.1 A-GNSS Feared Events

This section describes feared events to be considered for implementing positioning integrity using A-GNSS. The feared events are further considered as part of the UE-based and UE-assisted integrity methodologies in Section 9.4.

##### 9.3.1.1.1 Feared events in the assistance data

###### a) Incorrect computation by the positioning service provider

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 corrections 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 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 by the 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 positioning service provider

**Editor’s Note:** the Positioning Service Provider is the external source (non-3GPP) of positioning integrity assistance data.

The positioning service 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 provider.

This is different than the incorrect computation of the corrections, 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 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 provider’s network).

A first approach to handle these events is to monitor these types of 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 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.

###### 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 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*. 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. 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 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 systems providers offer protection against jamming by 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 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.

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 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 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.

###### b) Hardware faults

Editor’s Note: FFS

###### c) Software faults

Editor’s Note: FFS

##### 9.3.1.1.5 LMF Feared Events

###### a) Hardware Faults

Editor’s Note: FFS

###### b) Software Faults

Editor’s Note: FFS

##### 9.3.1.1.6 Summary of A-GNSS Feared Event Considerations

Table 9.3.1.1.6 summarizes the feared event categories and examples described in Sections 9.3.1.1.1 to 9.3.1.1.5

**Table 9.3.1.1.6: Summary of A-GNSS feared events for consideration in the WI (FFS).**

|  |  |
| --- | --- |
| **Feared Event Category** | **Feared Events (specification impacts are FFS)** |
| 1. Feared events in the assistance data | Incorrect computation by positioning service provider,  e.g. software bug, corrupt or lost data |
| External feared event impacting positioning service provider,  e.g. station outages, or other GNSS feared event (Category 3) |
| 2. Feared events during positioning data transmission | Data integrity faults |
|
| 3. GNSS feared events | Satellite feared events  e.g. bad signal-in-space or bad broadcast navigation data |
|
| Atmospheric feared events |
|
| Local Environment feared events,  e.g. Multipath, Spoofing, Interference |
| 4. UE feared events | GNSS receiver measurement error |
| Hardware faults |
| Software faults |
| 5. LMF feared events | Hardware faults |
| Software faults |

Editor’s Note: Additional UE-assisted errors may be included in this list, FFS.

*End of Text proposal*

1. PHASE 1

# 1. Introduction (PHASE 1)

This document contains the questions and baseline TP for the following email discussion [1][2][3]:

[Post112-e][618][POS] Finalise integrity text proposals (Swift)

Scope: Refine the text proposals in R2-2010877/R2-2010878/R2-2010879.

Intended outcome: Agreeable TPs

Deadline: Long

The following documents should also be reviewed as part of this email discussion:

* Email Guideline - [Post112-e][618][POS] Integrity TPs [3]
* [618] KPIs and Use Cases – PHASE 1 Draft TP [4]
* [618] Methodologies – PHASE 1 Draft TP [5]

# 2. Error Sources (PHASE 1)

# 2.1 Positioning Error Categories

The following agreements were made in the online discussion [1]:

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.

Taking into consideration, R2-2008812/R2-2009331/R2-2010073/R2-2010061 and the online comments [1], additional updates to these agreements were also captured in the draft TP (R2-2010878 [2]):

* Changed the ‘UE faults’ category to ‘UE feared events’ and added ‘Software faults’ as another example (**Swift Navigation**) in response to questions from **Qualcomm and ESA** on what is defined as a UE fault?
* Grouped the ‘Spoofing’ and ‘Jamming/interference’ examples under a new heading titled ‘Local Environment feared events’ (adapted from the **Hexagon** feedback), which now includes examples of ‘Multipath’, ‘Interference’ and ‘Spoofing’.

The resulting headings are summarized below, noting the term ‘feared event’ is FFS subject to outcomes from the ‘[618] KPIs and Use Cases – PHASE 1 Draft TP’ [4] discussion paper:

* Feared events in the correction data

1. Incorrect computation by the provider
2. External feared event impacting the provider

* Feared events in transmitting the data to the UE

1. Data integrity faults

* External feared events

1. Satellite feared events
2. Atmospheric feared events
3. Local Environment feared events

Multipath

Interference

Spoofing

* UE feared events

1. GNSS receiver measurement error
2. Hardware faults
3. Software faults

**Question 1: Do you agree with the updated list of error source categories? If not, please provide your reasoning and your proposed alternatives.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| vivo |  | The words in red, what is the difference with external feared events in blue?Take satellite feared events for example, doesn’t the satellites feared event also gain from correction system like EGNOS or GLONAS? |
| Swift Navigation | Partly | We believe this is a complete list for UE-based.  If UE-assisted is also supported, then the list must be generalized to be complete and correct, including an additional category for **LMF-faults** (hardware and software). In this case, the ‘Feared events in transmitting the data to the UE’ category should also be generalized as “**Feared events in transmitting data within the 3GPP system**”, including:   * Integrity assistance data from the service provider to the UE/LMF * Measurement data from the UE to the LMF * Integrity results to the LCS client |
| Hexagon A&P | Yes | One comment: rather than referring to the list of ‘error sources categories’ it would be more appropriate to refer to the list of ‘feared events categories’.  Within GNSS augmentation / assisted-GNSS it is inherent to have error sources, which are then mitigated or removed by augmentation (usually a form of differencing).  What we are concerned about are ‘feared events’ |
| Nokia | No | For the ‘*incorrect computation by the provider’*, it depends on the implementation and this is difficult to characterize how likely this would happen. We don’t think 3GPP has to be over-specified and implies deficiency of the system. Therefore, we suggest removing “incorrect computation by the provider” from the list. |
| InterDigital |  | We agree with Swift that the list of feared events should be identified and categorized according to UE-based and LMF-based integrity |
| CATT | Partly | For UE-based mode:   * Integrity assistance data from the service provider LMF and then from LMF to UE, * Measurement data from the UE to the LMF, if needed, * Integrity results to the LCS client from UE to LMF   So it seems that “Hardware faults” and “Software faults” in UE feared events are not required to report from UE to LMF.  For UE-assisted mode:   * Integrity assistance data from the service provider LMF and then from LMF to UE, * Measurement data from the UE to the LMF * Integrity results to the LCS client from LMF to AMF   It also seems that “Hardware faults” and “Software faults” in UE feared events are not required to report to LMF. BTW, the LMF-faults is not required either in the interaction between UE and LMF or between LMF and AMF.  So we prefer to delete “Hardware faults” and “Software faults” in UE feared events which are not required in the interaction between UE and LMF. |
| ZTE | Nearly Yes | We also share the same concern with vivo. External feared events and external feared event impacting the provider need more explanation.  The second category “Feared events in transmitting the data to the UE” seems not clearly enough. From our mind, this should be modified as “Feared events during positioning data transmission”. And this kind of feared event(like data integrity fault) may happen in the data transmisison in correction data provider&LMF, LMF&UE and satellite&UE. The current name may not cover all involved scenarios. |
| OPPO |  | We agreed the comments above that UE-assisted method should be taken into account, and the “Feared events in the correction data” may not be of high interest from 3GPP perspective. |
| ESA | Yes(with clarifications) | We do tend to agree with the latest categorization of error sources. We are also intrigued by ZTE´s proposal which seems to have some merits – as an example, it could cover also transmission of e.g. measurements from UE to LMF for the UE-assisted mode. We are also supporting Hexagon´s proposal to rename ‘’error sources categories’’ as ‘’feared events categories’’. To address vivo´s concerns, maybe category 3 can be renamed as “GNSS feared events” since all those effects are about GNSS systems which are also external to 3GPP.  Other clarification are required:  0. Add LMF-feared events to the list of items that can have an impact on positioning integrity (we think this is equally applicable to UE-based and UE-assisted as LMF is one of the LPP terminating nodes)  1. We have the feeling that what “provider” means is anything but clear. Currently, there are two possible meanings, depending on who we ask: providers as in MNO (as per 3GPP positioning architecture) vs provider as in a 3rd party owner of GNSS CORS networks. Once definition of provider is clarified, we can discuss whether to capture anything additional or not.  2. Correction data should be replaced by Assistance Data as per LPP terminology. |
| Xiaomi |  | We think it is not feasible to standardize ‘Hardware faults’ and ‘Software faults’ in the spec. Moreover, we share the same view with CATT that ‘Hardware faults’ and ‘Software faults’ are not required in the interaction between UE and LMF. So we think the ‘Hardware faults’ and ‘Software faults’ is UE implementation and suggest to delete it. |
| u-blox | Partly | We generally agree with the categorization of the error sources. We agree with Hexagon about calling it “feared event categories” rather than “error source categories”.  We also share reservations about including hardware and software faults in the UE category. This tends to be managed as part of the implementation though FTA and FMEA processes. There may need to be some acknowledgement that HW and SW implementation need to also meet the TIR profile. |
| Huawei/HiSilicon | No | We are generally ok with the error source categories, but suggest to change the title as follows:   * Internal feared events * Feared events in the correction data from the provider  1. Incorrect computation by the provider 2. External feared event impacting the provider  * Feared events in transmitting the data to the UE  1. Data integrity faults  * Satellite feared events * UE feared events  1. GNSS receiver measurement error 2. Hardware faults 3. Software faults  * External feared events  1. Atmospheric feared events 2. Local Environment feared events   Multipath  Interference  Spoofing  1. We suggest to group the feared events as “internal” and “external” ones to improve the readability. We think the error sources except Atmospheric feared events and Local Environment feared events belong to the internal ones.  2. We suggest to category “Satellite feared events” as the “Internal feared events” instead of “External feared events”, since these feared events are related to the health of the GNSS satellite(s) and the real-time of signal(s).  3. We suggest to also include other measurement error such as GDOP in addition to “GNSS receiver measurement error”. |

In response to Agreement 2 above, there was unilateral consensus in the email discussion [6] to include a table of feared events as part of the TR (**Nokia, InterDigital, Fraunhofer, ESA, Convida, ZTE, Spreadtrum, Xiaomi, Hexagon, Swift Navigation, Intel, Ericsson, CATT**). The table proposed in [7] includes updated naming to match the error categories above plus additional modifications described in the Moderator Comments in the Email Summary [6]. The resulting table was shifted to Section 9.4.1.1.6 as part of the Integrity Methods section to summarize the UE-based A-GNSS assistance information considerations. The table is presented below:

**Table** **9.4.1.1.6: Summary of UE-based A-GNSS integrity assistance information considerations.**

\*FFS whether new integrity assistance information needs to be specified in LPP.

**\*\***not possible to mitigate with assistance data from the network, the UE is responsible for mitigating these feared events locally.

|  |  |  |
| --- | --- | --- |
| **Error source** | **Error source category** | **Examples of integrity assistance information (FFS)\*** |
| 1. Feared events in the correction data | Incorrect computation by provider, e.g. software bug, corrupt or lost data | Validity or quality flags for existing assistance information |
| External feared event impacting provider, e.g. station outages, or other external feared event, per (3) |
| 2. Feared events in transmitting the data to the UE | Data integrity faults | Data corruption check, e.g. CRC |
| Data Authentication / Signature |
| 3. External feared events | Satellite feared events | Bad Signal in Space |
| Bad Broadcast Navigation Data |
| Atmospheric feared events | Ionospheric indicator |
| Tropospheric indicator |
| Local Environment feared events, e.g. Multipath, Spoofing, Interference | FFS |
| 4. UE feared events | GNSS receiver measurement error | \*\* |
| Hardware faults | \*\* |
| Software faults | \*\* |
|  | out of sync , out of coverage, fail to receive assistant data, fail to support TIR(TIR not available for calculation) |  |

**Question 2: Do you agree with Table 9.4.1.1.6 as a summary of the error source categories? If not, what changes do you propose, and why?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Partly | 1. We think columns 1 and 2 could be used as part of a new section titled ‘**9.3.1.1.5 Summary of A-GNSS Error Source Categories**’ under Section 9.3 of the TR. The table name will also need updating.  2. This updated table described above could then be reused in the Methodologies Section (9.4) of the TR with the 3rd column added again. Individual versions of this would be needed for UE-based and UE-assisted methods, given some feared events are specific to only one method, while others are common to both. The third column could be renamed accordingly for each method, i.e. ‘**Examples of UE-based integrity assistance information (FFS)\***’ and ‘**Examples of UE-assisted integrity assistance information (FFS)\***’. |
| Hexagon A&P | Partly | Columns 1 & 2 contain firm information, but column 3 contains provision information that remains under discussion.  And to repeat the earlier comment: rather than calling these ‘error sources categories’ it would be more appropriate to refer to them as ‘feared events’ categories. |
| Nokia | No | As commented in Q1, we think “Incorrect computation by provider, e.g. software bug, corrupt or lost data” can be removed. |
| InterDigital |  | Similar to our answer to Q1 and in agreement with Swift, we think the error sources and the associated events and examples impacting UE-based and LMF-based integrity should be clearly identified in the summary table(s). |
| CATT | Partly | For UE-based A-GNSS, UE still can report GNSS receiver measurement error to LMF. So “\*\*” can be deleted following GNSS receiver measurement error. |
| ZTE |  | We wonder whether the “*out of sync , out of coverage, fail to receive assistant data*” can be covered by the second kind of feared event. These three errors can be summarized by data transmitting error(detail can be checked in Q1).  In addition, “*fail to support TIR”* can be covered by the “*UE feared events*”.  Besides, considering almost everything in the third conlumn is FFS, we think more detail should be discussed before we add this column. |
| OPPO |  | As replied to Q1 above.  And we share the view with ZTE on the added row of “out of sync,…” |
| ESA | Yes | We agree in principle with the table. We just want to point out that solutions other than provision of assistance data may be considered in some situations and therefore column 3 should not constrain discussions to solutions based on dissemination of AD only.  Also, it seems that this useful table is repeating too many times throughout chapter 9. Maybe it can be kept only once?! – see our answers to last TP |
| Xiaomi |  | As replied in Q1, for UE feared events, we suggest to delete ‘Hardware faults’ and ‘Software faults’. |
| u-blox | Partly | Since UE faults can’t be mitigated via assistance data they are implementation dependent. However they may be important for UE-assisted modes. Therefore we propose only retaining them for UE-assisted and not UE-based. |
| Huawei/HiSilicon | No | 1. Please find the comments about the categories of error sources in Question 1.  2. We suggest to specify the attributes of each error, such as the error type (e.g. STEP, RAMP, NOISE, etc.), the occurrence rate (typical value), the magnitude (typical value), to provide a full picture. |

# 2.2 Other Open Issues

**Question 3: Are there any open issues which have not been addressed by Questions 1 and 2? If so, please identify the issue(s), your reasoning and your proposed resolution.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Huawei/HiSilicon | Yes | 1. We suggest to specify how each error source may influence the positioning integrity, which may be helpful for the methodology part.  2. The possible error models (e.g. Gaussian Mixed Model, CDF/PDF overbounding) can be provided to measure the positioning error caused by the listed error sources. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 2.3 Draft Text Proposal

The baseline text from R2-2010878 [2] unless otherwise indicated in the track changes and comments.

*Start of Text Proposal*

9.3 Positioning Integrity Error Categories

9.3.1 RAT-Independent

9.3.1.1 A-GNSS

This section describes error sources to be considered for implementing positioning integrity using A-GNSS. These error sources are further considered as part of the UE-based and UE-assisted integrity methodologies in Section 9.4.

9.3.1.1.1 Feared events in the correction data(degrade of header)

1. Incorrect computation by the provider

GNSS correction networks collect and process GNSS measurements in order to estimate various GNSS corrections (e.g., the satellite orbits, clocks, etc.). This information are used by UE to calculate PL. (explain why incorrect data is a feared event) All impacted GNSS corrections 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 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 by the provider by performing consistency checks on the input data, checking the validity of the corrections before sending them and applying CRCs.

1. External feared event impacting the provider

The positioning correction service 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 provider.

This is different than the incorrect computation of the corrections, 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 correction provider, such as insufficient data to compute the corrections (e.g. limited number of GNSS sensor stations recording measurements from GNSS satellites,per my understanding this is Satellite feared events) 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.in case of outage, can we simply set it true or false for validation? If we only need measurement location one time per hour, then out of outage is tolerable

A first approach to handle these events is to monitor these types of 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.for outage, better time than flag, leave UE to judge

9.3.1.1.2 Feared events in transmitting the data to the 5GS

1. 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.

I think we need distinguish and clarify 1) spoofing between 5GS and GNSS Network with 2) data transmission inside 5GS from LMF to UE.

9.3.1.1.3 External feared events

1. Satellite feared events(degrade of header)

Satellites can suffer HW failures and therefore enter into a mode in which they cannot broadcast a signal altogether (so less number of satellites is a external feared event or feared event impacting the provider?)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* (in my understanding this IE is used as correction data)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. 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 difficulty to predict due to uncertainties in the atmospheric distribution.

LPP already includes an IE for these correction data(so if it is correction data, why not in 9.3.1.1.1), 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 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. Individual ionospheric and tropospheric quality indicators are missing and can be easily added as a field to each of these IEs.

1. 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 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.(why not belong to 9.3.1.1.2? it is feared event in transmission.)

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 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.(this is jamming in 9.3.1.1.2)

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 systems providers offer protection against jamming by stronger signals, broadcast on more frequencies, and using more constellations simultaneously.

**Spoofing**

Same comments with above, first why these environment not 9.3.1.1.2, second what are the differences among jamming/spoofing/interference?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 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.

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 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.

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
2. Software faults
3. out of sync , out of coverage, fail to receive assistant data, fail to support TIR(TIR not available for calculation)

Editor’s Note: Additional UE-assisted errors may be included in this list, FFS.

*End of Text proposal*