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] Draft TP – Error Sources (PHASE 1)

**Document for:**  Discussion and Decision

# 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
 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

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)\***’. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 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*

# 3. Conclusions

# References

[1] 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>.

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

[3] [Email Guideline - [Post112-e][618][POS] Integrity TPs](https://www.3gpp.org/ftp/Email_Discussions/RAN2/%5BRAN2%23112-e%5D/%5BPost112-e%5D%5B618%5D%5BPOS%5D%20Integrity%20text%20proposals%20%28Swift%29/)

[4] [[618] KPIs and Use Cases – PHASE 1 Draft TP](https://www.3gpp.org/ftp/Email_Discussions/RAN2/%5BRAN2%23112-e%5D/%5BPost112-e%5D%5B618%5D%5BPOS%5D%20Integrity%20text%20proposals%20%28Swift%29/PHASE%201/KPIs%20and%20Use%20Cases)

[5] [[618] Methodologies – PHASE 1 Draft TP](https://www.3gpp.org/ftp/Email_Discussions/RAN2/%5BRAN2%23112-e%5D/%5BPost112-e%5D%5B618%5D%5BPOS%5D%20Integrity%20text%20proposals%20%28Swift%29/PHASE%201/Methodologies)

[6] R2-2010880 Email Summary [AT112-e][614][POS] GNSS Integrity, Swift Navigation.

[7] R2-2010879 TP on Integrity Methodologies, Swift Navigation.