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

Electronic, January XXXXX, 2020

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

**Source:** Swift Navigation

**Title:** [Post112-e][618][POS] Draft TP – Methodologies (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] Error Sources – PHASE 1 Draft TP [5]

# 2. Methodologies (PHASE 1)

Objective C of the study is to:

* **Study methodologies for network-assisted and UE-assisted integrity.**

As reflected in the latest submissions to RAN2#112-e and the comments online by **ESA,** the methodologies have received least discussion and treatment to date, and therefore require further examination. The ‘Summary of 8.11.3.3 Methodologies for network-assisted and UE-assisted integrity’ prepared by InterDigital [6] provides a comprehensive review of the methodologies topics raised in the submissions to RAN2#112-e. Many of these considerations are not yet reflected in the draft TP below [2]. Therefore, the questions below are intended to identify and prioritize the open issues for addressing Objective C.

# 2.1 Scope of Study Objective

**Question 1: What key topics should be addressed for the integrity methodologies objective?**

|  |  |
| --- | --- |
| Company | Comments |
|  |  |
|  |  |
|  |  |

**Question 2: From the existing Tdoc submissions, what content should be considered for inclusion?**

|  |  |
| --- | --- |
| Company | Comments |
|  |  |
|  |  |
|  |  |

# 2.2 GNSS Positioning Integrity Methods

**Question 3. What GNSS positioning integrity methods should be addressed within the scope of the study?**

|  |  |
| --- | --- |
| Company | Comments |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 2.3 Methodologies Summary table

**Question 4. Do you agree with Table 9.4.1.3 as a summary of the methodologies?**

|  |  |
| --- | --- |
| Company | Comments |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 2.4 Other Open Issues

**Question 5: Are there any open issues which have not been addressed by Questions 1 to 4? If so, please identify the issue(s), your reasoning and your proposed resolution.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 2.5 Draft Text Proposal

The baseline text from R2-2010879 [2] unless otherwise indicated by track changes or comments.

*Start of Text Proposal*

9.4 Positioning Integrity Methods

9.4.1 RAT-Independent

Detection of GNSS error sources is necessary to support positioning integrity by ensuring the TIR can be met. This section describes how the feared events occurring in different parts of the positioning system can be detected to support the implementation of UE-based and UE-assisted methodologies.

9.4.1.1 UE-Based A-GNSS Integrity Methods

9.4.1.1.1 Detection of Feared Events in the Correction Data

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

9.4.1.1.2 Detection of Feared Events in Transmitting Data to the UE

Data integrity ensures that the end-to-end data transmission link needed to signal integrity assistance data across the network is secure and free from the possibility of data corruption, including the data link to the corrections service provider. Data integrity algorithms and related security architectures for the 5G system are individual work areas in 3GPP [17].

A related observation in the context of this SI (further addressed in Section ‘9.4.1.1.5 - Data Validation’ below) is that industry-specific functional safety standards (e.g. ISO-26262 for Automotive, IEC 62278 for Rail) are also required to validate integrity compliance for a given implementation. These standards include requirements that may be outside of the current RAN architecture. For example, consider the typical service interface between a corrections service provider sending GNSS assistance data to the UE via the NG-RAN. Both the correction service provider and UE can be designed and qualified with integrity compliance. However, the NG-RAN architecture, although rigorously specified with data security and integrity features in [17], may not comply with industry-specific functional safety standards by default. This implies that the integrity of the data transmission from the correction provider to the UE needs to be trusted and assured without any alterations via the NG-RAN.

One method for achieving this is by providing for the data to be signed by the correction provider and verified by the UE in accordance with the relevant functional standards[[1]](#footnote-1). Once the data has left the correction provider, any changes to the data would invalidate the certificate. This in turn means that, irrespective of whether the 3GPP architecture is compliant to the functional safety standards, appropriate procedures can be implemented to sign and verify the network integrity assistance data with minimal impacts to the NG-RAN – i.e. the NG-RAN can still be leveraged as an efficient data link. Further investigation is required through the SI/WI to determine whether new data integrity IEs are needed for positioning integrity or whether existing data integrity IEs are sufficient (e.g. to carry a data signature from the corrections service provider to the UE).

9.4.1.1.3 Detection of External Feared Events

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

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

In addition to the network providing integrity assistance data corresponding to the detection of feared events, the network may also provide to the UE certain threat model parameters, allowing them to be updated based on the evolving operational history of the GNSS constellations. An example of this is found in the ARAIM Integrity Support Message (ISM) which contains parameters such as the assumed probability of satellite failure [23]. The scope of this SI is not intended to standardize the integrity algorithms implemented by the corrections service provider to detect the feared events. The study identifies the common set of feared events that can be indicated to the UE by specifying network-assistance data IEs.

9.4.1.1.4 Detection of UE Feared Events

UE-detected feared events depend on the hardware and software capabilities of the equipment and its internal integrity algorithms. This SI does not attempt to standardize the GNSS integrity algorithms at the network or the UE, but rather the network-assistance data needed to transport the integrity indicators derived from the algorithms. The assistance data can then be applied by the UE’s GNSS positioning function (i.e. independent of 3GPP).

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

9.4.1.1.5 Positioning Integrity Validation

Positioning integrity can only be validated end-to-end, per-implementation. Validation requires a comprehensive Fault-Tree Analysis (as described in [24]) and a complete qualification dossier (e.g. documentation, methodologies, tests and traceability through the entire integrity qualification process).

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

9.4.1.1.6 Summary of UE-Based A-GNSS Integrity Assistance Information Considerations

Further to the general error sources described in Section 9.3.1.1 and the integrity methods described above, Table 9.4.1.1.6 summarises the potential error sources and assistance information to be considered for UE-Based A-GNSS positioning integrity, noting the assistance information and transport procedures remain FFS in the WI.

**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 | \*\* |

Figure 9.4.1.1.6 illustrates where each of the four error sources from Table 9.4.1.1.6 originates in the end-to-end positioning system.

**Figure 9.4.1.1.6: Relationship between the UE-Based GNSS Integrity feared events and the 3GPP UE positioning architecture (GNSS). Refer to [21] for a detailed description of the UE positioning architecture.**

Diagram

Description automatically generated

9.4.1.2 UE-Assisted A-GNSS Integrity Methods

Editor’s Note: UE-assisted methods are FFS.

9.4.1.3 Summary of A-GNSS Integrity Methods

Table 9.4.1.3 summarizes the network-assisted (UE-Based) and UE-assisted (LMF-Based) considerations for determining integrity.

**Table 9.4.1.3: Summary of network assisted (UE-Based) and UE-assisted (LMF-Based) considerations for determining Integrity.**

NOTE: the details are FFS and to be discussed in WI phase, including the LPP messages and transfer procedures.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Integrity method** | **Location service type** | **Source of KPIs** (e.g. TIR, AL, TTA etc) | **Source of Integrity results**  (e.g. PL, Integrity Availability etc) | **Integrity assistance information (FFS)** | **Spec impact (FFS)** |
| Network assisted (for UE-based positioning) | MO-LR | Obtained via UE internal implementation; | Keep inside the UE | From LMF to UE:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events | Procedure to transfer Integrity assistance information from LMF to UE |
| MT-LR | From LMF | From UE | From LMF to UE:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events | Procedure to transfer Integrity assistance information and KPIs from LMF to UE  Procedure to transfer Integrity results from UE to LMF |
| UE assisted (for LMF-based positioning) | MO-LR | From UE | From LMF | From Service Provider to LMF:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events  From UE to LMF:  - UE feared events | Procedure to transfer Integrity assistance information and KPIs from UE to LMF  Procedure to transfer Integrity results from LMF to UE |
| MT-LR | Obtained via LMF implementation | LMF internal implementaiton | From Service Provider to LMF:  - Feared events in the correction data  - Feared events in transmitting the data to the UE  - External feared events  From UE to LMF:  - UE feared events | Procedure to transfer Integrity assistance information from UE to LMF |

*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] R2-2010879 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(Swift)/)

[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(Swift)/PHASE%201/KPIs%20and%20Use%20Cases)

[5] [[618] Error Sources – 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(Swift)/PHASE%201/Error%20Sources)

[6] R2-2010675 Summary of 8.11.3.3 Methodologies for network-assisted and UE-assisted integrity, InterDigital.

1. Note that the requirements called out by integrity standards such as ISO-26262 can be extremely onerous for any entity that “processes” (i.e. modifies in any way) the data. This possibly includes use of qualified tools such as special compilers, as well as using ISO-26262 certified hardware and CPUs to perform the processing. [↑](#footnote-ref-1)