3GPP TSG-RAN WG2 Meeting #115-e***R2-21xxxxx***

Electronic, Aug 16 – 27, 2021

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

**Source:** Swift Navigation (Rapporteur)

**Title:** [Post114-e][601][POS] GNSS integrity assistance information, KPIs, and reporting of integrity results (Swift)

**Document for:**  Discussion, Agreement

# 1. Introduction

This document is to trigger the following email discussion:

* [Post114-e][601][POS] GNSS integrity assistance information, KPIs, and reporting of integrity results (Swift)

Scope: Discuss the contents of GNSS integrity assistance information, the signalled KPIs, and reporting of the integrity results.

Intended outcome: Report to next meeting

Deadline: Long

Companies are asked to provide their views on the stated topics and questions. It is anticipated that this email discussion will be undertaken in multiple phases in order to prepare the final report.

The topics are grouped into 3 categories corresponding to the email discussion scope:

1. Contents of the GNSS integrity assistance information
2. Contents of the signaled KPIs
3. Contents and reporting of the integrity results

First round feedback is due **Friday 25-Jun-2021 23:59 UTC** before the inactive period commences in July.

# 2. Contents of the GNSS integrity assistance information

At RAN2#114-e the following proposal was made [1]:

Proposal 8: RAN2 confirms that assistance information for positioning integrity may include:

- Feared events in the GNSS Assistance Data

- Feared events in transmitting the data to the UE

- GNSS feared events

- UE feared events

RAN2 continues to discuss details about assistance data parameters required for GNSS positioning integrity support. Possible liaison with RTCM may be taken into account.

Therefore, the focus of this section is to:

1. Discuss which of the feared events need to be addressed as part of the WI in order to support GNSS positioning integrity determination in 3GPP;
2. Discuss which assistance data parameters need to be specified as part of the WI in order to mitigate the impact of the feared events identified in (a).

## 2.1 Feared event considerations

First, we revisit the summary of the A-GNSS feared events and integrity assistance information considerations identified in Table 9.4.1.1 in the Study [2]:

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

Table 1: Summary of A-GNSS feared events and integrity assistance information considerations [2].

Five categories of feared events are identified in Table 1:

1. Feared events in the GNSS Assistance Data
2. Feared events during positioning data transmission
3. GNSS feared events
4. UE feared events
5. LMF feared events

Question 1: Please identify which of the feared event categories in Table 1 need to be addressed in the WI in order to support GNSS positioning integrity determination in 3GPP. Explain your reasoning.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Company | Feared Event Category  Yes / No / FFS | | | | | Comments |
| 1) | 2) | 3) | 4) | 5) |
| Swift Navigation | Y | FFS | Y | FFS | N | For 1) and 3), GNSS integrity assistance data parameters are used to mitigate the impact of the feared events (e.g. Table 1 in [R2-2106105](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_114-e/Docs/R2-2106105.zip) [13]) and these parameters are applicable to the UE-based and UE-assisted positioning modes.  For 2), we suggest that state-of-the-art security measures can be used to prevent deliberate attacks on the data communications (such as a digital signature to validate authenticity of the data, end-to-end), meaning these measures can be handled outside the specifications. For accidental corruption, it is FFS whether existing data integrity measures in LPP (e.g. CRC, parity check, checksum) are sufficient to meet the needs of integrity. We propose that the data integrity requirements for positioning integrity determination should be further examined in the WI.  4) For UE-based positioning, the UE feared events can be handled in the implementation and do not need to be considered in the specifications. For UE-assisted positioning, the GNSS measurements at the UE must be sent to the LMF. However, the additional information that is needed to indicate the integrity of the GNSS measurements, alongside the information that can be detected by the UE in order to characterize the local environment feared events, are both FFS (as discussed in [8]).  For 5), we think the LMF feared events are only relevant in the UE-assisted case (i.e. when the LMF is the entity that computes the integrity) and can be handled in the implementation. In the UE-based case the LMF is only passing the assistance data to the UE, which is covered by the data integrity scheme (i.e. Category 2 above) rather than the LMF feared events. |
| Qulalcomm | N | N | Y | N | N | (1) and (5): The usual assumption in 3GPP is that the network does not provide bad or incorrect assistance data to the UE. Therefore, (1) and (5) need to be addressed via implementation.  (2): We understand that errors may occur over the communication link that provides real-time corrections, causing erroneous data, data loss, or high latency. However, this topic seems out of scope of the current objectives and would need to involve multiple other 3GPP groups (e.g., RAN1, SA3).  (4): These are internal to the UE and need to be addressed via implementation. |
| Nokia | Y | FFS | Y | N | FFS | Items in 1) and 3) are commonly used in GNSS to meet the needs of integrity. We do not anticipate any need to develop anything specific in the WI  For 4) , it would be difficult to specify any requirements due to the heterogeneity of the devices population. This should remain part of implementation  2) and 5) can be FFS. |
|  |  |  |  |  |  |  |

## 2.2 GNSS integrity assistance data parameters

GNSS integrity messages can be sent as assistance data between the LMF and the UE. At RAN2#114-e there were several integrity messages / indicators proposed in the contributions, including the proposals in [8][11][12][13]. Before the messages can be defined, the rapporteur suggests that RAN2 first agree on the A-GNSS positioning techniques (e.g. RTK/PPP/PPP-RTK [17]) that should be supported in the WI, and therefore which of these techniques require integrity information to be sent in the assistance data. Then we can begin defining the contents of these messages in future discussions.

Question 2: Please indicate (Yes/No) which of the A-GNSS positioning techniques (RTK / PPP / PPP-RTK) in LPP should support integrity?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Company** | **RTK** | **PPP** | **PPP-RTK** | **Comments** |
| Swift Navigation | Yes | Yes | Yes | GNSS positioning integrity determination should be supported for all the GNSS positioning techniques supported by LPP, as per the WI objectives. |
| Qualcomm | Yes | Yes | Yes | …but the objective is to support GNSS positioning integrity determination, and not only for HA-GNSS. |
| Nokia | Yes | Yes | Yes | All these techniques need to be supported for RAT-independent positioning integrity |
|  |  |  |  |  |

Question 3: Which of the A-GNSS positioning techniques (RTK / PPP / PPP-RTK) in LPP require additional assistance data to be defined to support integrity? Please explain your reasoning.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Company** | **RTK** | **PPP** | **PPP-RTK** | **Comments** |
| Swift Navigation | Yes | Yes | Yes | All. New IEs for quantifying integrity need to be defined in the assistance data.  The existing GNSS-RealTimeIntegrity IE in LPP contains basic information to improve system robustness but is not sufficient for integrity as discussed in this WI where the PL, AL and TIR are quantified.  Some integrity messages may also be common to the different positioning techniques (e.g. orbit and clock parameters for PPP and PPP-RTK etc). |
| Qualcomm | Yes | Yes | Yes | All are affected by "GNSS feared events". |
| Nokia | Yes | Yes | Yes | Some earlier papers provided a comprehensive gaps analysis (R2-2007647 and [11]). For example, individual quality indicators for satellite error clocks and satellite bias are currently not supported in LPP. 5GS support for navigation message authentication as well as ranging authentication are desirable.  Commonalties between the integrity messages for each method should be identified, and the benefit of supporting additional IE should be assessed before including them |
|  |  |  |  |  |

The topic of interoperability has also been raised in [11][13] given traditional integrity systems such as SBAS are typically specified end-to-end, including using a prescribed set of algorithms, whereas 3GPP typically requires interoperability at the interface level between different vendors (of the UE and LMF) whose implementations may differ.

*Note: The Rapporteur believes that although this may seem like a trivial point, it is important to have clear consensus on the scope of interoperability. It may have impacts on the normative work as additional considerations may need to be given to ensure a broader degree of interoperability than has been demonstrated in existing systems where implementation details and user algorithms are prescribed in the standard.*

Question 4: How should the topic of interoperability with respect to integrity be handled in the specifications?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Different vendors (of UE and LMF) should be capable of exchanging assistance data to support integrity determination without requiring additional coordination between these vendors to agree on underlying assumptions not specified within the standard. This is a central principle of standards-based interoperability.  For example, existing integrity systems such as SBAS require a fully standardized end-to-end architecture, including algorithm and implementation choices. This in turn means that certain assumptions and parameters are “hard coded” into the SBAS standard and implicit in the assistance information that is sent from the SBAS network. For example, the probability of missed detection of a given feared event is specified in the SBAS specifications and all vendors must adopt this value. This does not allow for the possibility of different vendors innovating or differentiating on performance based on their unique implementations, e.g. if a vendor develops a new technique to reduce the probability of missed detection.  However, in 3GPP the aim is to provide a standard that allows for different vendors to interoperate whilst ideally maintaining the possibility for innovation and differentiation within the ecosystem. Therefore, our view is that this WI should adopt the same goal for interoperability.  Swift’s view is that it is possible to achieve this level of interoperability by minimizing the number of “hard coded” parameters or assumptions in the standard and rather include the needed parameters within the assistance data itself, such that an integrity assistance data vendor can communicate to the position determining entity what parameters it is able to achieve. An example of this was provided in [13] as part of the Worked Example (Section 3.1) and Section 3.1.1.4. |
| Qualcomm | We think one of the motivations for specifying integrity assistance data is based on avoiding "hard coded" parameters. The GNSS ARAIM Integrity Support Messages (ISM) would be an example.  Interoperability and testing can only be on "message level"; i.e., correct encoding/decoding of assistance data (aka protocol conformance tests). |
| Nokia | Dynamic parameters communication between the entities seems to be the best option, and we believe this can be supported by extending some of the existing messages. |
|  |  |

Question 5: Any other comments?

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

# 3. Contents of the signalled KPIs

During the SI phase, RAN2 has defined a set of positioning integrity KPIs (including AL, TIR and TTA) that can be provided to the entity that computes the integrity. The following proposals were presented for discussion at RAN2#114-e [1]:

Proposal 5: RAN2 confirms positioning integrity requirements are associated to QoS, and send LS to SA1, SA2, CT1, and CT4 for relevant specification work. FFS whether the concept of “integrity level classification” should be supported in Rel-17.

Proposal 6: RAN2 confirms that positioning integrity requirement information (a.k.a. KPIs) including AL, TIR, and TTA can be provided to the integrity computing entity (either UE or LMF) over LPP. FFS the need of TIR set.

It has been discussed in the contributions [1][4][5][7][9][13][15] that the *RequestLocationInformation* and *ProvideLocationInformation* procedures in LPP can be reused to transfer the KPIs between the LMF and the UE. It has been further discussed in [1][4][10][12] whether the KPIs can be associated to the QoS, and if so, whether the required signaling should be discussed with CT4.

The rapporteur suggests that we first discuss and agree on the preferred procedures for transferring the KPIs before determining what (if any) LSs are required for defining the signalling.

Question 6: Do you agree that the RequestLocationInformation and ProvideLocationInformation procedures in LPP should be used transfer the KPIs (TIR, AL and TTA)? Explain your reasoning.

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Yes, to transfer the KPIs for the UE-based MT-LR and UE-assisted MO-LR modes. For UE-based MO-LR and UE-assisted MT-LR, the KPIs are already known internally to the integrity computing entity and do not need to be transferred. |
| Qualcomm | Yes for *RequestLocationInformation* and TIR; No for *ProvideLocationInformation.*  For "Mode 1 of Integrity Result Reporting" (PL reporting) we cannot see why AL and TTA should be provided in *RequestLocationInformation* (see also our response to Question 9)*.* However, the question is which Location Information IE is going to be used: Common Positioning (*CommonIEsRequestLocationInformation*) or A-GNSS Positioning (*A‑GNSS‑RequestLocationInformation* (*GNSS-PositioningInstructions*)). Also, the KPIs in *RequestLocationInformation* would only be required for UE-based mode. |
| Nokia | Yes, this is the most straightforward approach. There is no need to introduce new information fields for such purposes. |
|  |  |

Question 7: Do you agree that the KPIs can be associated to the QoS signalling? Explain your reasoning.

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Yes, we believe the KPI fields (TIR, AL, TTA) can be included in the QoS IE. Also, similar to the way the LCS QoS (e.g. for accuracy) can be characterized into two Classes (Best Effort Class and Assured Class) [TS 23.273], the integrity KPI request can also be characterized using a similar scheme (see Question 9 below). |
| Qualcomm | Up to SA1 and SA2 to decide. This may also have impacts to protocols outside of 3GPP (e.g., OMA MLP). |
| Nokia | Yes, the integrity KPIs can be considered as additional attributes of the QoS. This should be approved by SA. |
|  |  |

Question 8: Any other comments?

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

# 4. Contents and reporting of the integrity results

At RAN2#114-e the following proposal was made [1]:

Proposal 7: RAN2 confirms that at least integrity result reporting mode 1 (PL reporting) is supported in Rel-17. The messages RequestLocationInformation and ProvideLocationInformation in LPP are used for signalling relating to integrity result reporting. FFS if other types of reporting (including Mode 2) and/or optimization mechanisms are needed.

Modes 1 and 2 (described below) have being considered in many of the contributions [1][4][5][6][9][10][11][13]. Other types of reporting have also been suggested, including adding more categories of availability to Mode 2 [4] and sending the Achieved KPIs [13] (e.g. the degree of accomplishment of the KPIs [11]). It has also been discussed in [1][4][5][7][9][15] that the *RequestLocationInformation* and *ProvideLocationInformation* procedures in LPP can be used to report the integrity results.

|  |
| --- |
| **Mode 1 of Integrity Result Reporting : PL Reporting**   * The in*tegrity* computing entity calculates the PL, based on the measurement, assistance information and TIR. Then, the calculated PL is directly reported to where the LCS client resides (Network or UE). Hence, the integrity computing entity does not judge whether the positioning system is still available, it simply provides whatever PL value it has obtained. It is left to the LCS client itself to determine if the positioning system is still available based on the reported PL.   **Mode 2 of Integrity Result Reporting : Integrity Event Flagging**   * The integrity computing entity calculates the PL, based on the measurement, assistance information and TIR. Then, the integrity computing entity further compares the calculated PL with the given AL to determine if the positioning system is still available to offer trustable position estimation. Thus, the integrity computing entity may only have to report a binary flag (0 and 1) to indicate whether the positioning system is available or not. Thus, in this case the LCS client can be directly informed about the system availability, without conducting further evaluation by itself. |

The rapporteur suggests that RAN2 should first discuss what information may be included in the integrity results in order to satisfy the GNSS positioning integrity objectives of the WI. Then we can determine if / how the integrity results can be differentiated into different modes as part of the specifications.

Question 9: Please indicate what information should be included in the integrity results? Describe your reasoning.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Company** | **Protection Level** | **Integrity Flag(s)** | **Other** | **Comments** |
| Swift Navigation | Yes | No | Achieved KPIs | The PL should always be reported in the integrity results as part of any integrity implementation. It allows the application / LCS client to evaluate the PL relative to its KPIs (e.g. to determine system availability) but is also a very important measure in itself which if often used by the integrity application.  Also, the actual or ‘Achieved KPIs’ for which the PL was computed may sometimes differ from the KPIs that were requested (see example in Section 3.2 of [13]). This means the Achieved KPIs should also be sent as part of the Integrity Results, which is analogous to the ‘Best Effort Class’ described in Question 7 for the LCS QoS, i.e. even if the location estimate (including the Integrity Results in this case) does not fulfil the QoS requirements, it should still be returned. In other words, you still want to know what KPIs were achieved even if they are not what you requested. Likewise, the ‘Assured Class’ [TS 23.273] represents the case where the KPIs requested in the QoS *must* be fulfilled, otherwise an appropriate error flag should be sent in the response.  Swift does not see the utility in an additional Integrity Flag, however if it is determined by RAN2 that an optional Integrity Flag is useful for reporting system availability (e.g. 0: PL<AL, 1: PL>AL), it is also necessary that the PL and Achieved KPIs can be optionally reported alongside this Flag, to ensure all properties of the Integrity Results can be enumerated if required by the integrity system. |
| Qualcomm | Yes | No |  | It seems reporting of PL is indeed sufficient (e.g., in addition to the currently reported position uncertainty). The LMF can assess the integrity by comparing the PL with the required AL and decide on the system availability. The AL and TTA would then not be required in the *RequestLocationInformation* (see our response to Question 6).  The PL should be computed according to the requested TIR and according to the application requirements. It is not clear why the UE should compute a PL for a different TIR than requested. An LMF can still evaluate different AL's to determine system availability conditions. However, if beneficial, a location request could also include several TIRs for which a computed PL is requested.  As commented above, any QoS requirements or impacts to LCS QoS Class defintions would need to be investigated by SA1 and SA2. |
| Nokia | Yes | Yes | FFS | First of all, we should prioritize what have been identified in the SI. The “achievable KPI” is not captured in TR 38.857, whether it should be supported can be considered later. In any case we are not against this option.  From our point of view both Mode 1 (PL reporting) and Mode 2 (Integrity Event Flagging) should be supported, as they can be useful in different scenarios, and LMF may make a request to indicate which of these modes should be applied.  In particular, Mode 2 is suitable for cases where e.g. the LMF may (by implementation) take immediate actions to improve positioning quality, straight after receiving the integrity event flag without waiting for instructions from the LCS client. Mode 1, on the other hand, leaves some room for the LCS client to first judge whether there is a need of positioning quality improvement, by checking the absolute value of the PL. |
|  |  |  |  |  |

Question 10: Do you agree that the RequestLocationInformation and ProvideLocationInformation procedures in LPP should be used to report the integrity results?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Yes. |
| Qualcomm | Yes for *ProvideLocationInformation* and PL. No for *RequestLocationInformation*.  However, the question is in which IE: Common Positioning (*CommonIEsProvideLocationInformation*) and applicable to all positioning methods, or A-GNSS Positioning (*A-GNSS-ProvideLocationInformation*). |
| Nokia | Yes |
|  |  |
|  |  |
|  |  |

Question 11: Any other comments?

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

# 5. References

1. R2-2106453, [Pre114-e][609][POS] Summary on agenda item 8.11.5 on GNSS integrity (Nokia), Nokia.
2. TR 38.857, 3GPP TSG RAN Study on NR Positioning Enhancements; (Release 17), V2.0.0.
3. R2-2104843, Discussion on methodologies for network-assisted and UE-assisted integrity, vivo.
4. R2-2105218, Discussion on network-assisted and UE-assisted integrity, Huawei, HiSilicon .
5. R2-2105308, Discussion on procedures and signalling for GNSS positioning integrity, InterDigital, Inc.
6. R2-2105524, Discussion on supporting positioning integrity in RAN, OPPO.
7. R2-2105563, Discussion on signalling and procedures for GNSS positioning integrity, Xiaomi.
8. R2-2105735, UE-aided detection of threat to GNSS systems and assistance data signaling, Fraunhofer IIS; Fraunhofer HHI; Ericsson.
9. R2-2105874, Positioning Integrity Support in LPP, Nokia, Nokia Shanghai Bell.
10. R2-2105970, On GNSS Integrity, Ericsson.
11. R2-2105985, Guiding framework on integrity concepts for A-GNSS positioning, ESA.
12. R2-2106085, Considerations on GNSS positioning integrity support, Qualcomm Incorporated.
13. R2-2106105, Proposals on GNSS integrity assistance information, Swift Navigation.
14. R2-2106371, Consideration on the signalling design for Positioning Integrity, Samsung Electronics.
15. R2-2106427, Discussion on positioning integrity transportation, ZTE Corporation, Sanechips.
16. R2-2106428, Discussion on positioning integrity data calculation and LS to RTCM, ZTE Corporation, Sanechips.
17. TR 38.305, Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN, Release 16.