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. |
| MELCO | Y | Y | Y | Y | FFS | 1) Satellite and atmospheric anomalies should be separated and considered in “GNSS feared event”  4) Standard deviation of measurement error of UE is required to compute PL in LMF. Additionally TIR of receiver’s faults (H/W and S/W) may be required so that LMF can allocate total TIR (in KPIs) to other feared events based on fault tree.  5) What needs to be considered as LMF feared events is FFS. |
| u-blox AG | Y | Y | Y | N | N | 1) and 3) are important for integrity but it is not necessary to signal the events within each category individually  2) requires a mechanism to ensure correct delivery of corrections. Further study may be required in order to establish whether the transport of LPP is sufficiently error free.  4) and 5) do not need to be signalled for UE-based positioning, |
| InterDigital | Y | FFS | Y | Y/N | N | 1) and 3) Feared events in assistance data and GNSS feared events can be addressed by providing certain assistance information to the integrity computing entity.  2) We think addressing feared events during positioning data transmission using LPP protocol may require involvement of other WGs such as SA3. As the LPP protocol is E2E, it may be necessary to validate whether existing mechanisms are adequate to address any issues that can result in data faults.  4) We think for UE-assisted positioning case, the GNSS receiver measurement error can be indicated by UE to LMF to assist with integrity calculation. However, the feared events related to UE HW/SW faults can be handled via implementation and need not be signaled.  5) Can be handled via implementation and need not be signaled |
| vivo | Y | N | Y | N | N | 1) and 3): GNSS integrity assistant data is beneficial to support integrity. GNSS feared event is also needed to be addressed to mitigate the bad quality and unavailability of the GNSS signals.  2),4) and 5): it is difficult to define what are the specific hardware and software faults and GNSS receiver measurement error because they are different for different vendors. Besides, they can be handled by the implementation. As for feared events during positioning data transmission, it involves the security, etc which belongs to other working groups rather than only RAN2. |
| Fraunhofer | Partially Y | FFS | Y | N | N | (1) Incorrect computation, etc, should be part of conformance tests. For the part where external feared event impacting the GNSS Assistance Data are discussed, these could be candidates to be signaled to the UE.  (2) The loss of correction data or latency could cause issues and could be discussed.  (3): Multipath, spoofing and jamming: The UEs benefit from receiving assistance from the network about what is happening in the vicinity. We further believe that the capable UEs should also be able to report it to the network. How the UE determines such events and how the network uses these events to generate assistance data is up to network and UE implementation.  (4) We believe these could be tested as part of UE conformance testing.  (5) Handling the issues in the network (e.g. software faults) should be part of network implementation. To us it is not clear, what the UE is expected to do when it is signaled that there are faults with LMF. |
| Ericsson | Y | FFS | Y | Y | N | 1) and 3) stems from the integrity discussion in the SI  2) can be analyzed further  4) includes errors in UE measurement , calibrations etc, which naturally needs to be included for UEA positioning  5) handled by implementation |
| Intel | Y | N | Y | FFS | N | 1) and3) are important for GNSS integrity.  2) is out of RAN2 scope regardless of the evaluation and solution.  4) We tend to agree, the UE could indicate the Errors in UE measurement. However HW/SW errors shall not be specified.  5) Agree with others, network implementation. |
| ZTE | Y | FFS | Y | Y | Y | for 4) and 5), if the Integrity Computing Entity is UE, then LMF feared events should be included; if the Integrity Computing Entity is LMF, UE feared events should be included.  For 2), the feared events during positioning data transmission may contain non-3GPP and 3GPP procedures, which needs further study. |
| Huawei, HiSilicon | Y | N | Y | FSS | N | For 1) and 3), we think we have already had thorough discussion on the corresponding assistance data, which is also necessary to be captured in the standard.  For 4), our view is that only some of the UE feared events should be addressed in 3GPP, e.g. GNSS receiver measurement error, while leaving the others to implementation, e.g. hardware faults, software faults.  For 2) and 5), we don’t see much necessity to discuss in the WI phase. |
| ESA | N | No preference | Y | Partlly Y | FFS | 1. NO. Part of cat1 is covered in cat3. Incorrect computation assistance data is something that deals with the external corrections provider and thus not within scope of 3gpp architecture. Secondly, if the AD has problems LMF or external corrections provider can simply decide not to transmit such data (incorrect data). As a principle, we would be in favour to keep the signaling for integrity to the minimum necessary to achieve the objective. 2. We don´t see a benefit but if the group decides to go ahead we are ok with it 3. Yes, the obvious one. 4. Partly yes. For UE-assisted GNSS positioning, with integrity features, GNSS-MeasurementList IE needs revising. As a minimum, multipath reporting needs a finer resolution. Additional local feared events (see Ericsson and Fraunhofer) can be reported to LMF in this IE. 5. FFS – based on contributions. |
| Hexagon | Y | FFS | Y | FFS | FFS | Work done so far means we are on a path of addressing 1) and 3). The other 3 feared events categories also need to be addressed, in order to have a create a UE position with known integrity, but we consider this as FFS. |
| CATT | Y | N | Y | FFS | N | 1) and 3) are studied in SI for GNSS integrity.  2) is out of RAN2 scope.  4) may be discussed and specified what can be standalized in 3GPP.  5) is supposed as network implementation. |
| OPPO | Y | FFS | Y | FFS | FFS | 2）seems out of RAN2 scope, especially considering CRC could solve the problem.  4) and 5) should be based on online discussion |

## 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 |
| MELCO | Yes | Yes | Yes | Maybe SPP user (who don’t use correction data) still want integrity information to be sent. |
| u-blox | Yes | Yes | Yes |  |
| InterDigital | Yes | Yes | Yes | We think all GNSS positioning techniques supported with LPP should support integrity |
| vivo | Yes | Yes | Yes | As suggested by WI “Support of integrity for UE-based and UE-assisted A-GNSS positioning”, all A-GNSS positioning techniques should support integrity given that no specific positioning techniques are required in the WI. |
| Fraunhofer | Yes | Yes | Yes | All positioning methods should support integrity. |
| Ericsson | Yes | Yes | Yes | All of them |
| Intel | Yes | Yes | Yes | All of GNSS positioning techniques should be considered. |
| ZTE | Yes | Yes | Yes |  |
| Huawei, HiSilicon | Yes | Yes | Yes | We think all the A-GNSS positioning techniques should support positioning integrity, even there are any new techniques in the future. |
| ESA | Yes | Yes | Yes | We agree with all three options. Regarding A-GNSS, based on 3GPP framework for GNSS – everything is generically labelled A-GNSS, we think there is nothing else needed for legacy A-GNSS (prior to Rel15 /RTK/SSR). According to an ESA paper [R2-2103750] these type of users can already make use of existing version of LPP to receive some integrity information – “bad” satellites and signals (see ***GNSS-RealTimeIntegrity*** IE). To address QCOM point, we propose that a simple update of stage 2 could reflect what we explained in short above. |
| Hexagon | Yes | Yes | Yes |  |
| CATT | Yes | Yes | Yes | Not only RTK / PPP / PPP-RTK but also all A-GNSS positioning techniques will be considered. |
| OPPO | Yes | Yes | Yes |  |

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 |
| MELCO | Yes | Yes | Yes | Some existing integrity messages provide useful information as a quality indicator for measurement or corrections, but does not sufficiently support integrity in various cases. |
| u-blox AG | Yes | Yes | Yes | The existing IE *GNSS-RealTimeIntegrity* is not sufficient |
| InterDigital | Yes | Yes | Yes | We share the same view with MELCO and u-blox that the existing IEs applied for the GNSS positioning techniques in LPP are inadequate for integrity. As such additional assistance data for supporting integrity would be necessary. |
| Vivo | Yes | Yes | Yes | Assistance data originating from the R17 integrity mechanism should be defined for all A-GNSS positioning techniques to introduce this new integrity feature. Besides, given the specific mechanism of positioning techniques, assistance data can be different or the same. |
| Fraunhofer | Yes | Yes | Yes | These approaches are affected by all events, but the proposal address only satellite and atmospheric events. However, local environment events are currently not taken into account. Here, the inclusion of local multipath, spoofing, interference information could benefit integrity awareness.  The UE and possibly also the RAN-nodes could assist the LMF in determining the strength and area of strength, so that the assistance message could be targeted at the impacted Ues. |
| Ericsson | Yes | Yes | Yes | Same view as Fraunhofer – local environment events are also important and means to booth acquire and provide from/to devices are relevant. |
| Intel | Yes | Yes | Yes | Agree with others, existing GNSS-RealTimeIntegrity IE is not sufficient. |
| ZTE | Yes | Yes | Yes | Additional assistance data is required for positioning integrity of all A-GNSS positioning techniques. |
| Huawei, HiSilicon | Yes | Yes | Yes | All. We share the same view as Swift. |
| ESA | Yes | Yes | Yes |  |
| Hexagon | Yes | Yes | Yes | All. These technologies have much in common, as do their underlying integrity concepts. |
| CATT | Yes | Yes | Yes | All. |
| OPPO | Yes | Yes | Yes | Share the view of Swift |

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. |
| MELCO | For interoperability, we agree that “Residual risk parameters” should be sent. In our understanding, these parameter is used to consume total TIR (in KPIs) and remaining TIR allocated to GNSS feared events should be used to compute K factor for PL. Additionally, we suggest that some reference algorithm for PL computation (and maybe fault tree) should be discussed, disclosed, and implemented by independent parties for interoperability testing purpose. The algorithm and fault tree can be basic (and maybe legacy) one.り |
| u-blox AG | For the definition of the messages and fields (syntax) interoperability is essential. We do not think this should extend to full semantic interoperability for which standardization of algorithms and interworking test compliance would be required. |
| InterDigital | We have similar understanding with Qualcomm and Nokia on this question. Interoperability can be achieved via the delivery of ‘dynamic parameters’ in assistance data to the entity that computes integrity (UE or LMF). We also agree, from RAN2 point of view, that interoperability should be supported at the message level. |
| Vivo | Considering that 3GPP typically requires interoperability at the interface level between different vendors, we should avoid or minimize “hardcoded” parameters and only specify the essential parameters by reusing the existing LPP signalling and procedure with modification for new IEs related to integrity. |
| Fraunhofer | To facilitate interoperability only high-level integrity indicators should be required. The algorithms should be left implementation specific both at the UE and at the network side. |
| Ericsson | Via clearly defined parameters from a RAN2 perspective |
| Intel | Agree with others. Algorithms should be left to implementation. We only need to specify assistance data and results in message level. |
| Huawei, HiSilicon | We note that there are three options mentioned in [13]:   * Option 1 - No interoperability, up to implementation to validate; * Option 2 - Explicit interoperability, communicate all needed parameters explicitly; * Option 3 - Implicit interoperability, parameters specified in standard.   We slightly prefer to Option 2. Our understanding is that the standard should leave enough flexibility for implementation since different vendors of UE and LMF may have different implementation to achieve positioning integrity. So it would be better to define what kind of information should be exchanged to support integrity determination explicitly. |
| ESA | We agree with many remarks from above, and agree with the observation from QCOM..  Based on the progress in WI and if any hardcoded parameters, interoperability will be considerably improved if the number of hardcoded parameters is minimized as much as possible. In addition, any hardcoded parameters that may remain should be clearly defined in the specifications together with a clear explanation of how the UE/LMF needs to use them for the purpose of GNSS integrity. |
| Hexagon | For interoperability on positioning+integrity, interoperability only the interface level alone is not sufficient. A key aspect of ensuring interoperability is that not only data content is agreed upon, but also the interpretation of data content is agreed upon and captured in documentation. Successful GNSS augmentation requires that both ends of the system, i.e. Correction Generation and UE positioning, have knowledge of some of the underlying models and processing techniques used. An example is the reference frame. We can’t state at the moment what criteria should be put on interoperability, but we agre that this topic has to be part of the remaining discussions. |
| CATT | Agree with ESA. |
| OPPO | agree with Fraunhofer |

Question 5: Any other comments?

|  |  |
| --- | --- |
| Company | Comments |
| Ericsson | Before initiating a discussion about representation of the integrity assistance data, RAN2 needs to agree on the scope of the integrity assistance data. |
|  |  |
|  |  |
|  |  |

# 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. |
| MELCO | Yes. For us it seems no problem that these procedures are used. |
| u-blox AG | The KPIs need to be known by the ICE and/or the Location Client application (depending on operating modes) which may not be co-located in the same device so we support being able to optionally include them in both *RequestLocationInformation* and *ProvideLocationInformation*. |
| InterDigital | Yes, we think that the LPP Location Information transfer procedure, including the LPP RequestLocationInformation and ProvideLocationInformation messages, can be used for transferring the integrity KPIs for the UE-based (MT-LR) and UE-assisted (MO-LR) positioning. |
| vivo | Integrity information can be transmitted by existed signal modification without architecture change and new message introduced. Besides, ProvideLocationInformation can be used to transfer the KPIs. |
| Fraunhofer | Yes, both *RequestLocationInformation* and *ProvideLocationInformation*. The *ProvideLocationInformation* message could signal the regionalized indicators of multipath, spoofing, interference to the LMF. |
| Ericsson | Yes, this seems to be the most natural means for introduction |
| Intel | Yes, agree. |
| ZTE | Yes |
| Huawei, HiSilicon | Yes, but we think other LPP message or LCS message can also be used to transfer KPIs, as illustrated by Table 9.4.1.1.1 in TR 38.857. More specifically,   * For MT-LR UE-based (network-assisted) positioning, integrity KPIs (i.e. TIR, AL, TTA) should be delivered to UE from LMF, which can be achieved through LPP *ProvideAssistanceData* or *RequestLocationInformation*. * For MO-LR LMF-based (UE-assisted) positioning, integrity KPIs (i.e. TIR, AL, TTA) should be delivered to LMF from UE by enhancing the LCS request in LCS message.   Also, for MO-LR LMF-based positioning, we think we should discuss whether the KPIs can be associated to the QoS signalling, as mentioned in Question 7. |
| Hexagon | Yes |
| CATT | Yes for RequestLocationInformation. The KPIs (TIR, AL and TTA) to UE will be required for UE-based mode via RequestLocationInformation message. But it seems no need to include ProvideLocationInformation message from UE to LMF for KPIs. CommonIEsRequestLocationInformation or *A‑GNSS‑RequestLocationInformation* should be discussed.  Furthermore, the KPIs between LMF and LCS will be handled by SA2 and CT1. |
| OPPO | Two sencarios MT-LR UE-based and MO-LR LMF-based should be considered, since only these two scenarios involve integrity KPI indication towards the other end. For MT-LR UE based, the LMF should indicate the integrity KPI towards the UE, both LPP provide assistance data and LPP request location information could take the job. For MO-LR LMF-based scenario, the LCS request should have the information of integrity KPI. |

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. |
| MELCO | We don’t have any specific comment on this. |
| u-blox AG | No. We think that Integrity and QoS are different concepts and should be kept separate. |
| InterDigital | We think this can be left to SA1 and SA2 to decide. |
| Vivo | Yes. Referring to Section 9.2.4 of TS38.857, different location services and use cases may have different requirements for integrity. We think the detailed content and procedure should be discussed with SA and CT. |
| Fraunhofer | Yes. The KPI fields can be associated with QoS Signalling. However, the mapping of these two is probably not in RAN2 scope. |
| Ericsson | Agree that the KPIs can be extending the QoS parameters, up to SA2 to decide. |
| Intel | Out of RAN2 scope. Should be discussed and decided by SA2. |
| ZTE | Not sure. Transmitting KPIs over LPP signalling seems enough. |
| Huawei, HiSilicon | Agree. To guarantee the integrity performance, the system needs to monitor the status of integrity with the corresponding requirements for each service level. In the study item phase, we have agreed on the requirements of integrity for different use cases in Table 9.2.4 in TS 38.857. So we think it’s natural to associate the KPIs to the QoS signaling. |
| ESA | In principle, yes, but we propose to keep FFS and invite company to submit more contribtuions.  Can the rapporteur clarify some of the working assumption: who is the entity always knowledgeable of the KPIs? Does the LMF, as source of integrity assistance data, always knowledgeable about the KPIs? We would also appreciate if we look at this item from the use cases point of view – QCOM answer to question 9 is quite compelling and does not make obvious that KPIs needs always to be signaled. Won´t the TIR, AL, etc. be designed based on use cases integrity requirements and therefore leave it up to implementation?  Regarding Fraunhofer suggestions, if taken on board during the WI, the GNSS-SignalMeasurementInformation IEs is the correct place to add them (some basic multipath reporting is already supported in there).This is not a topic to be jointly addressed with the KPIs.  We tend to agree with Qualcomm that we also need to decide between Common Positioning or A-GNSS Positioning. |
| CATT | Yes in principle. SA2 should take lead this request and finalize how to deliver Qos which include KPIs to LMF in LCS framework. |
| OPPO | Yes. It falls into the scope of SA and CT. |

Question 8: Any other comments?

|  |  |
| --- | --- |
| Company | Comments |
| u-blox AG | We propose including Integrity Availability as a KPI (See TR [2]) |
|  |  |
|  |  |
|  |  |

# 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. |
| MELCO | Yes | No | Yes | From point view of manufacture of UE like as locator, knowing PL is essential. Also, as proposed, it is interesting to send “Achieved KPIs” which we believe useful. |
| u-blox AG | Yes | Yes | AL, TIR, TTA and Availability | Mode 1: The PL is computed for a given probability (usually the TIR) and may take into account the TTA, therefore these two KPIs need to be provided to the ICE with the request and should be included with the calculated PL. AL and the integrity flag are not output in this mode.  Mode 2: We support Mode 2 in which the ICE generates a flag indicating whether the position output meets the integrity requirements or not. In this case the PL is not output but the KPIs used in the integrity calculation (AL, TIR, TTA) should be provided with the output flag. The Availability KPI should also be provided. |
| InterDigital | Yes | Yes | Difference between the calculated integrity result and the KPIs | We think both modes of integrity result reporting have merits, depending on granularity of integrity information required by the LCS client/application. Both Mode 1 and Mode 2 can also be applicable for UE-based and LMF-based integrity.  Mode 1 can be used in scenarios where the application requires the calculated PL result based on monitoring of feared events and positioning information. Mode 2 can be useful in simpler applications where the integrity KPIs are provided to UE/LMF and the application requires only information on whether integrity performance is met with respect to the KPIs. For Mode 2,  the additional information reported can include the difference between the calculated integrity result and the KPIs, to indicate richer information to the application on the closeness of the achieved integrity with respect to the KPIs. |
| Vivo | Yes | No |  | PL is enough to support integrity. Network or UE where LCS client resides can directly compare PL and AL to decide if the positioning system is still available. |
| Ericsson | Yes | Yes | FFS | It shall be configurable from LMF whether the UE shall use mode 1 or 2, AL, TIR and TTA can be provided in both cases. There are use cases for both mode 1 and 2. |
| Intel | Yes | No |  | It would be good to avoid multiple solutions for the same purpose. |
| ZTE | Yes | Yes | FFS | Mode 2 should be supported under general cases. However, there still exists a case that LCS client didn’t transmit all parameters to LMF, so the integrity computing entity may not figure out the integrity flag. In this case, reporting PL is useful that the integrity computing entity can provide the calculated PL to LCS client which can determine the positioning integrity itself.  As for other information, we haven’t discover the use case/necessity of reporting KPIs so far. Further study may be needed on this. |
| Huawei, HiSilicon | Yes | Yes | The degrees of integrity risk (e.g. Extremely High/High/Low/No risk) | 1. For the above two modes, we think both of them show benefit in different cases.  * Mode1 can be useful when the LCS client does not want to expose the integrity KPIs to the LMF/UE, e.g., AL. In this case, the LMF/UE does not need to know the AL, which might be considered as private within the LCS client, and the LCS client itself to determine if the positioning system is still available. * For Mode 2, we think it can reduce the complexity for LCS client.  1. In order to evaluate the system availability more properly, more refined integrity results should be introduced, especially for the case of “System Available (PL<AL)”. With the refined integrity results, the LCS client may know how to react according to different alarm levels in advance, e.g., shutting down the system or making some adjustment. |
| ESA | Yes | As complementary or optional info | TIR, AL, and TTA for which the PL has been computed | The calculated PL for a specific TIR is the raw integrity info that needs to be directly reported to the LCS client that requested it. Then, at the LCS client it will be checked if the PL accomplishes what is needed by the application. Some applications or some system functionalities may need the integrity flag (if the computed PL is lower or greater than the AL), but others may need to perform other checks (e.g. if PL is also lower than 50% or 75% of the AL, etc.) or will just need to employ the actual value of the PL for other computations. Therefore, to cope with all the possible application needs, the computed PL should always be directly provided to the LCS client. The integrity flag can also be provided as complementary integrity info.  If, as Swift points out, the actual TIR, AL and TTA for which the PL was computed may differ from the KPIs that were requested or there can be any confusion between the requested and the achieved ones, then they should be reported within the integrity results along with the computed PL (and integrity flag). |
| Hexagon | Yes | No |  | Only the PL should be reported |
| CATT | Yes | No | Fail to calculate PL alarm | From RAN2 perspective, the PL between UE and LMF is good enough. Then the LMF can assess the integrity by comparing the PL with the required AL and decide on the system availability. If UE failed to calculate the PL, the failed alarm may be reported to LMF. As for the further indication on integrity such as Achieved KPIs or integrity flag between LMF and LCS, it’s out of RAN2 scope. |
| OPPO | YES |  |  | Reporting of the PL meets the requirement of the mode 1, which should be taken as baseline. We are OK to remove the support of the mode 2 in WI phase if majority companies agree so. |

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 | Partly yes - For MT-LR, we think *ProvideLocationInformation* should be used to report the integrity results.  *RequestLocationInformation*, on the other hand, should be used to transfer integrity requirements (i.e. KPIs) rather than integrity result reporting. |
| MELCO | Yes. For us it seems no problem that these procedures are used. |
| u-blox AG | Yes. Since the ICE needs to know at least TIR and TTA for Mode 1 and all KPIs for Mode 2 they should be included with the request and output delivering the integrity result. |
| InterDigital | Yes, we think the LPP Location Information transfer procedure, including the LPP RequestLocationInformation and ProvideLocationInformation messages, can be used for requesting and transferring the integrity result. |
| Vivo | Yes, considering the simplicity and efficiency, integrity results can be transmitted by existed signal modification (i.e., ProvideLocationInformation procedure in LPP) without architecture change and a new message introduced. |
| Fraunhofer | The *ProvideLocationInformation* message could be used by the UE to signal the regionalized indicators of multipath, spoofing, interference to the LMF but we are also open to other options – for example a new message. |
| Ericsson | Yes, and also specific mensurements with estimated precise position to support integrity. |
| Intel | Yes for ProvideLocationInformation. Regarding RequestLocationInformation, how can it to be used for the transmission of integrity results? |
| ZTE | Yes |
| Huawei, HiSilicon | Agree with the view from Intel  We think the case may be different for MO-LR LMF-based positioning. More specifically,   * For MT-LR UE-based (network-assisted) positioning, the integrity results (e.g. PL and Integrity Availability) obtained at UE side can be transferred to LMF with LPP *ProvideLocationInformation*. * For MO-LR LMF-based (UE-assisted) positioning, the integrity results (e.g. PL and Integrity Availability) obtained by LMF can be delivered to UE through lCS response with LCS message. |
| ESA | Yes |
| Hexagon | Yes, this makes sense |
| CATT | Yes for *ProvideLocationInformation* to report PL from UE to LMF in UE-based, and to report measurement from UE to LMF in UE-assisted in LPP from RAN2’s perspective. As for the the integrity results from LMF to AMF/LCS client, it’s out of RAN2 scope. |
| OPPO | Agree with Intel and Huawei |

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.