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.

Phase 2 feedback is due **Monday 02-Aug-2021 0900 UTC**.

**PHASE 1 contains the first round questions / comments (yellow).**

**PHASE 2 contains the summaries from Phase 1 and the updated questions / proposals (blue).**

# PHASE 1 Discussion

# 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 (Phase 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 |

## Summary of Phase 1 Comments (Question 1)

1. Feared events in the GNSS Assistance Data
   * Y: 13 (including Fraunhofer), N: 2, FFS:1
   * Swift, Nokia, u-blox, InterDigital, Vivo, Ericsson, Intel, Huawei, Hexagon and CATT think that these FEs are a common consideration for GNSS integrity, as confirmed in the study.
   * Qualcomm thinks that 3GPP assumes the network does not provide incorrect data and that these FEs are handled in the implementaiton. ESA also thinks some are out of scope.
   * U-blox , MELCO and ESA suggest that some of these FEs will be handled as part of other FEs (e.g. GNSS feared events) rather than needing an individual category for each.
   * Fraunhofer thinks the data link itself can be handled through conformance testing but agrees that GNSS AD may be subject to external FEs that need flagging in the assistance data.

Rapporteur’s proposal

* A clear majority have indicated that, as an extension of the study findings, the way in which we handle FEs in the GNSS AD at least needs to be discussed in scope of the WI. As noted by u-blox, MELCO and ESA, we tend to agree that some of these events may not need to be signalled as individual categories if they can be handled as part of other FE categories. However, we first need to identify and discuss the types of integrity information that can be used to address these FEs before we can assess which information is common between categories.
* We also agree with Qualcomm and ESA that detecting these FEs is the responsibility of the external corrections provider and is outside the scope of the 3GPP architecture. Based on the study findings, the remaining question then is ‘how will the corrections provider indicate to the integrity computing entity the validity of the assistance data’? Again, this depends on the types of information that can be used to address these types of FEs. Therefore, given a majority support, we think a useful next step is to begin discussing this information, which will help to determine if and how these FEs will be handled in the specification work.
* Refer to Question 1 (Phase 2) in Section 5.1.

1. Feared events during positioning data transmission
   * Y: 2, N: 5, FFS:9 (including ESA)
   * Swift, Nokia, u-blox, InterDigital, Fraunhofer, Ericsson, ZTE, Hexagon and OPPO think that further study may be necessary to determine whether transport of LPP is sufficiently error free to support the requirements of integrity.
   * Qualcomm, InterDigital and vivo think this topic may require involvement from other WGs such as RAN1 and SA3.
   * Intel, Huawei, CATT and OPPO think this topic may be outside the scope of RAN2 work.

Rapporteur’s proposal:

* + Based on the tallies and comments from those who answered Yes or FFS, a majority of companies think this topic requires further discussion to determine if existing mechanisms in 3GPP / LPP are sufficiently error free for the purpose of positioning integrity. Several companies who answered No have also suggested this topic is outside the domain of RAN2 but may require involvement from other WGs.
  + We think the consensus view is that this topic at least requires further discussion to properly define whether or not it is in scope of the WI, and if so, which WGs need to be involved.
  + Refer to Questions 2 and 3 (Phase 2) in Section 5.1.

1. GNSS feared events
   * Y: 16, N: 0, FFS:0
   * Fraunhofer thinks that capable UEs can also detect for GNSS feared events and should be able to report this information to the network.

Rapporteur’s proposal:

* + There is unilateral consensus that GNSS feared events will be addressed in the WI to support GNSS positioning integrity determination – refer to Proposal 1 (Phase 2) in Section 5.2.
  + We think a useful next step is to begin discussing the types of integrity parameters that can be used to address these FEs. This will also help to identify whether these parameters contain common elements that can be used to address other FE Categories (e.g FEs in the GNSS assistance data).
  + Refer to Question 4 (Phase 2) in Section 5.1.

1. UE feared events
   * Y: 5 (including ESA and InterDigital), N: 5, FFS: 6
   * Qualcomm, Nokia, vivo think the UE FEs are internal to the UE and can be addressed via implementation. Swift and u-blox agree that they can be handled via implementation for UE-based positioning. However, for UE-assisted positioning, Swift, MELCO, InterDigital, Ericsson, Intel, ZTE and ESA think they need to be considered.
   * InterDigital, Intel, Huawei and ESA think that only the GNSS receiver measurement errors are relevant for UE-assisted; HW/SW errors are handled on implementation.
   * Fraunhofer thinks this can be handled as part of conformance testing.

Rapporteur’s proposal:

* + No clear consensus emerged. From the comments, we think this Category should be divided into UE-based and UE-assisted requirements and further discussed.
  + UE-based: We think there is general consensus that the UE FEs will be handled via implementation when the integrity computing entity resides at the UE.
  + UE-assisted: For UE-assisted the consensus is less clear. Some suggest only GNSS receiver measurement errors are relevant, not the HW/SW faults. Some think all UE feared events may need to be considered, while others believe that all UE feared events are out of scope.
  + Refer to Questions 5 and 6 (Phase 2) in Section 5.1.

1. LMF feared events
   * Y: 1, N: 10, FFS:5
   * Swift, Qualcomm, InterDigital, vivo, Fraunhofer, Ericsson, Intel, Huawei and CATT believe the LMF feared events are out of scope and can be handled in the implementation.
   * U-blox thinks they are not relevant for UE-based positioning.
   * MELCO, Nokia, ZTE, Hexagon and OPPO think they may require further consideration based on the scope of discussion so far.

Rapporteur’s proposal:

* + There seems to be a general consensus that the LMF feared events are out of scope for both UE-assisted and UE-based positioning, although some companies suggest this topic may require further discussion, subject to the contributions.
  + Given the general consensus emerging, we think it is important to try and agree on this topic now which will help with scoping the remaining work to be undertaken in the WI.
  + Refer to Question 7 (Phase 2) in Section 5.1.

## 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 (Phase 1): 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 (Phase 1): 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 |

## Summary of Phase 1 Comments (Questions 2 & 3)

* There is uniletaral consensus that all A-GNSS positioning techniques in LPP should support positioning integrity and that each technique requires additional integrity assistance data.
* ESA thinks any changes to support integrity in the specifications will only be relevant to the positioning techniques introduced from Release 15 onward.
* Nokia thinks 5GS support for navigation message authentication as well as ranging authentication is also desirable.
* Swift, Nokia, vivo, Huawei and Hexagon think there are commonalities between certain positioning techniques meaning there will be commonalities in their associated integrity assistance data.
* Fraunhofer thinks the local environment feared events are not currently taken into account as part of these positioning techniques.
* Proposals 2 and 3 (Phase 2) are therefore presented in Section 5.2.

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 (Phase 1): 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 (Phase 1): 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. |
|  |  |
|  |  |
|  |  |

## Summary of Phase 1 Comments (Questions 4 & 5)

* Swift, Qualcomm (e.g. the ARAIM ISM), Nokia, MELCO (e.g. residual risk parameters), InterDigital, Vivo, Intel, Huawei, ESA, CATT think that all needed parameters can be communicated in the assistance data to avoid requiring hardcoded parameters.
* Swift, u-blox, Fraunhofer, Intel and OPPO also think that the algorithms are out of scope and are left to implementation. MELCO thinks a reference algorithm might be useful for interoperability testing.
* Qualcomm, u-blox, InterDigital, Vivo, ESA and CATT think that interoperability should be supported at the message / interface level. Qualcomm thinks that conformance testing can only occur at the message level (encoding / decoding of assistance data).
* Ericsson thinks any assistance data relating to interoperability requires well defined parameters. ESA think this is also the case for any hardcoded parameters that may be necessary in the spec.
* Hexagon thinks that interoperability at the interface level alone is not sufficient given the interpretation of the data content needs to be agreed between both ends of the system. Therefore, more work is needed to determine how integrity parameters can be properly defined to ensure they can be properly interpreted end-to-end via the network.
* Ericsson thinks RAN2 needs to discuss and agree on the scope of the integrity assistance data before we discuss how to represent the assistance data.

Rapporteur’s proposal:

* There is strong consensus that the integrity information that is needed to achieve interoperability at the interface level can be specified in the assistance data.
* Hardcoding of parameters should be avoided.
* Refer to Proposals 4 and 5 (Phase 2) in Section 5.2.

# 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 (Phase 1): 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. |

## Summary of Phase 1 Comments (Question 6)

* 11 companies (Swift, Nokia, MELCO, u-blox, InterDigital, vivo, Fraunhofer, Ericsson, Intel, ZTE and Hexagon) out of 15 agree that the *RequestLocationInformation* and *ProvideLocation Information* messages in LPP can be used to transfer the KPIs.
* Qualcomm thinks only *RequestLocationInformation* is relevant and that AL and TTA do not need to be included.
* Qualcomm, CATT and ESA (Question 7, Phase 1) wonder which specific IEs are being discussed (e.g. Common Positioning *(CommonIEsRequestLocationInformation)* or *A-GNSS Positioning (A-GNSS RequestLocationInformation (GNSS-PositioningInstructions))?*
* Huawei thinks that LPP *ProvideAssistanceData* may be an alternative to *RequestLocation Information* for UE-based MT-LR, whereas the LCS request in LCS message can be enhanced for UE-assisted MO-LR.

Rapporteur’s proposal:

* There is strong consensus that the existing LPP procedures can be used to transfer the KPIs (TIR, AL, TTA), including a majority of companies agreeing that the *RequestLocationInformation* and *ProvideLocationInformation* messages should be considered. However, there were also questions/comments on whether both messages are needed, and which specific IEs for these messages should be used. Altnerative procedures (LCS request) were also presented.
* Based on the discussion, we tend to agree that the first question to answer is whether a Location Information IE within Common Positioning or the A-GNSS Positioning will be used to transfer the KPIs – refer to Question 8 (Phase 2) in Section 5.1.
* To address the case for UE-assisted, we need to identify whether the LPP procedures are sufficient or whether we need to invoke the LCS request – refer to Question 9 (Phase 2) in Section 5.1.

Question 7 (Phase 1): 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. |

## Summary of Phase 1 Comments (Question 7)

* Swift, Nokia, Vivo, Fraunhofer, Ericsson, Huawei, ESA, CATT and OPPO all agree in principle that the KPIs can be associated to the QoS but the decision requires input from SA and/or CT.
* Qualcomm, Nokia, InterDigital, Ericsson, Intel and CATT think this decision is up to SA.
* Swift thinks the integrity KPIs can be characterized using a similar scheme to the two classes used for accuracy (Best Effort Class and Assured Class).
* U-blox thinks integrity and QoS are different concepts and should be separated.
* ZTE is not sure and thinks transmitting over LPP is enough.
* ESA think it is better to keep this topic FFS and await further contributions. They also seek clarity on which entity always has knowledge of the KPIs.

Rapporteur’s proposal:

* While there is a general level of support that the KPIs can be associated to the QoS, most companies think this decision requires input from other WGs and is difficult to agree via email discussion. It’s also tied to the feedback on Question 6 above (Phase 1), given the IEs used to transfer the KPIs in LPP will influence whether the QoS signaling is also involved. Therefore, we think this topic remains FFS subjsect to the Phase 2 feedback requested in Questions 8 and 9 (Phase 2).
* Regarding the question from ESA, the source of the KPIs for the UE-based (network-assisted) and UE-assisted (LMF-based) modes is summarised in Table 9.4.1.1.1 of TR 38.857.

Question 8 (Phase 1): Any other comments?

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

## Summary of Phase 1 Comments (Question 8)

* U-blox thinks the Integrity Availabiltiy should be included as a KPI.
* Refer to Question 10 (Phase 2) in Section 5.1.

# 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 (Phase 1): 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. |

## Summary of Phase 1 Comments (Question 9)

* PL (Y: 15, N:0)
  + There is unilateral consensus that the PL should be included in the integrity results.
* Integrity Flag (Y: 7 (incl ESA), N: 8 (incl Fraunhofer))
  + Nokia, u-blox, InterDigital, Ericsson, ZTE, Huawei and ESA (optional) think Mode 2 is useful to indicate if the integrity KPIs have been met or not (without needing to report PL).
  + Swift, u-blox, Ericsson and ESA think that the TIR, AL and TTA used in the integrity calculation also need to be provided as part of Mode 2 (and possibly Mode 1).
  + U-blox also suggests to add the Integrity Availability.
  + Swift, Qualcomm, MELCO, Vivo, Intel, Hexagon, CATT & OPPO do not think Mode 2 is required given the application can directly compare the PL with its KPIs.
* Other:
  + Swift, MELCO, u-blox and ESA think the TIR, AL, TTA used in the integrity computation should be reported alongside the PL.
  + InterDigital thinks the difference between the integrity result and KPIs should be reported.
  + Huawei thinks additional categories of integrity risk (e.g. Extremely High / High / Low / No Risk) could be introduced as part of reporting the system availability.
  + CATT thinks an alarm can be reported if the UE fails to compute the PL.

Rapporteur’s proposal:

* Firstly, there is unilateral consensus to report the PL in the integrity results.
  + Refer to Proposal 6 (Phase 2) in Section 5.2.
* There’s a fairly even split on Mode 2, but those who do support Mode 2 provide quite detailed justifications. There’s also support from multiple companies (but not a majority) that the TIR, AL, TTA should be optionally enumerated as part of Mode 2 (and probably Mode 1).
* The remaining proposals from InterDigital, CATT, Huawei are new and need further discussion to determine if there is additional support.
* Now that all comments are available for review on Mode 2 and the Other options, we think it is useful to refine the questions and take another poll.
  + Refer to Questions 11, 12 and 13 (Phase 2) in Section 5.1.

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 |

## Summary of Phase 1 Comments (Question 10)

* Swift, MELCO, u-blox, InterDigital, Ericsson, ZTE, ESA and Hexagon think that both the RequestLocationInformation and ProvideLocationInformation messages are relevant.
* Qualcomm, Nokia, Vivo, Fraunhofer, Intel, Huawei (MT-LR UE-based), CATT and OPPO think that only ProvideLocationInformation is relevant.
* Huawei thinks the LCS message is also relevant in the case of MO-LR UE-assisted (LMF-based).

Rapporteur’s proposal:

* Similar to the Phase 2 analysis from Question 6 (Phase 1) above, there is clear consensus that the LPP procedures can be used to transfer the integrity results, although the specific messages and IEs still require further discussion and clarification. Therefore, the responses to Questions 8 and 9 (Phase 2) are also directly relevant to addressing this topic.

Question 11: Any other comments?

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

## Summary of Phase 1 Comments (Question 11)

* No other comments were provided.

# 5. PHASE 2 Questions & Discussion

## 5.1 Phase 2 Questions

### Follow-up questions from Q1 (Phase 1):

Question 1 (Phase 2): What types of integrity parameters should be used to indicate when a feared event has been detected in the GNSS assistance data?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | The external corrections provider is responsible for validating the integrity of the information that they compute and send via the network. The main type of FE we’re concerned about is that the information contained within the GNSS assistance data may not always be validated to the required level for integrity. If this is the case, the corrections provider needs a way to signal that the assistance data has not been validated. The simplest way to achieve this to send a **Do Not Use (DNU)** alert flag corresponding to each assistance data message – see Table 1 in [13]. The reason we use this flag, rather than not providing the assistance data at all, is because the corrections provider might still have assistance data that they think is valid (e.g. for general purpose positioning using LPP today), but the data has not been validated to the level needed for integrity.  Further, there may be the case that the quality of the assistance data as it pertains to integrity may vary (i.e. it’s not just binary), which is why the assistance data parameters should also be supplemented with indicators representing the integrity bounds and residual risks associated with them. This enables greater flexibility in how the integrity computing entity chooses to handle each assistance data parameter within its internal integrity solution. |
| Qualcomm | As summarized by the rapporteur in Phase 1 Question 1:  " the remaining question then is ‘how will the corrections provider indicate to the integrity computing entity the validity of the assistance data’?"  A "correction provider" is not indicating anything to the target device, and how a "correction provider" is indicating the validity of assistance data to an LMF is up to the "correction provider" and LMF vendor.  The basic principle of A-GNSS is that the target device assumes that any provided assistance data are valid. I.e., a LMF should not provide faulty or invalid assistance data to a UE.  If there is a need to declare already provided assistance data as invalid (e.g., broadcast assistance data), the existing IE *GNSS-RealTimeIntegrity* should be used (with extensions, if necessary). |
| u-blox AG | Feared events detected by the service provider or LMF should be indicated to the UE as flags (typically DNU). However we would prefer if the flags were presented as enumeration of the fault causes. |
| Huawei, Hisilicon | We think a simple way is to indicate the feared event in the LPP provide assistance data, which at least needs to indicate which kind of feared event, e.g. incorrect computation of the GNSS assistance data, external feared event impacting the GNSS Assistance Data. |
| Nokia | In agreement with the Swift Nav. we believe that the data should allow the most accurate calculation of the integrity parameters. For this purpose, all information related to residual risks and uncertainties computed by the GNSS Correction Provider should be made available for the integrity calculation. Table 1 in [13] constitutes an excellent source of information. |
| Xiaomi | How to detect feared event in GNSS assistance data is depended on external corrections provider, if LMF receives any indications from external corrections provider, the LMF can forward it to UE or only send a simple indication to UE. |
| vivo | If the correction provider finds GNSS assistance data is invalid, the correction provider should not provide it to the integrity computing entity because the invalid GNSS assistance data is useless.  If the correction provider finds GNSS assistance data is valid, considering that the quality of the assistance data may vary, so except for the valid GNSS assistance data, the correction provider should also provide the corresponding factor representing the quality of the GNSS assistance data to the integrity computing entity. For example, the better the quality of valid GNSS assistance data is, the bigger the corresponding factor value of this valid GNSS assistance data is. |
| MELCO | System failure should be addressed by Do Not Use (DNU).  If it is not the case, when a feared event has been detected in the GNSS assistance data, the same integrity parameter as usual case should be used. To indicate the feared event, the parameter (integrity bound and residual risk e.g. ) should take sufficiently large values which represent the event. If the bound and risk cannot be estimated, the parameter should take as “UNKNOWN” or “Undef”. |
| ZTE | The specific error source of feared events detected in the GNSS assistance data may need an enumeration. |
| InterDigital | We have similar views with Swift regarding the quality of assistance data in relation to integrity. Assuming different positioning services have different integrity requirements (e.g. AL, TIR). In this case, when sending the GNSS assistance data parameters along with the additional indications on the associated risks and integrity bounds achievable, the integrity computing entity (UE or LMF) can determine whether and how the provided assistance data parameters are usable based on the additional indications and the integrity requirements. |
| Fraunhofer | Additionally, if the LMF has any information on impairments such as interference (e.g. from DME, TACAN, malicious activity) or spoofing detected in a certain area (this could be obtained by external monitoring systems, RAN or by capable UEs), then some simple information like a flag or a couple of bits to indicate such impairments on the GNSS signals that are affected.  The UEs that are capable to detect such events (and some UEs would detect it anyway while processing GNSS signals) help the network to identify the area impacted and the severity of impact. This could be left optional for the UE. However, the feedback can help other UEs by helping them reduce processing effort.  We can agree on simple reporting:  GNSS-IntegrityError-r17::= SEQUENCE {  *measurementReferenceTime MeasurementReferenceTime*  lastKnownPosition EllipsoidPointWithAltitudeAndUncertaintyEllipsoid, -- Cond UEB  integrityErrorCauses ENUMERATED {spoofing, interference, jamming,...},  gnss-SignalID-r17 GNSS-SignalID OPTIONAL  sv-id-r17 SV-ID OPTIONAL  } |
| Intel | In general the network shall not provide invalid assistance data to a UE. Then for feared event, it would be good to provide the assistance data that can be used to detect the achieved quality level. |
| Samsung | We share the view with QC that in principle network should not provid any invalid assistance data to the target UE. Despite, if there is the case to be covered , then reuse the existing field to indicate the invalidity can be the simplest way. |
| OPPO | Invalid assistance data should not be provided to the UE. |
| Ericsson | We have the same view as Swift, that integrity information, residual risks, uncertainties etc computed by the GNSS Correction Provider shall be representable by LPP, given that there can be multiple requirememt levels simultaneously due to multiple simultaneous users with different requirements possibly. LMF can therefore not refrain from providing information etc |

Question 2 (Phase 2): Do you think data integrity faults need to be addressed (at some level) in order to achieve positioning integrity? If No, please explain your rationale.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Yes | Further to the comments from Qualcomm, errors may occur over the communication link that is providing the real-time corrections, which may cause erroneous data, data loss, or high latency. We need further analysis on whether LPP can sufficiently handle these data integrity faults to the level that is required for positioning integrity (we provided a worked example in Appendix C in [13] to illustrate this question). We think this issue must be resolved before it is possible to achieve the integrity objectives.  We also reiterate from [13] that the ability to verify the data integrity scheme can avoid the need to certify each component of the 3GPP system under ISO-26262, as required by certain automotive applications. |
| Qualcomm | Maybe | This requires a separate and dedicated study to answer (this is not a LPP issue). |
| u-blox AG | Yes | Corrupted or spoofed corrections could be disastrous for the integrity of corrections and therefore certainty that the data transport is sufficiently reliable is important. |
| Huawei, Hisilicon | No | We don’t see relationship between the data integrity faults and LPP spec or any other issues discussed in RAN2. |
| Nokia | Yes but | The possibility of undetected corrupted data caused by radio transmission or intentional jamming must be taken very seriously, considering the potentially disastrous impacts. Having said that, we do not think the required analysis is entirely in the RAN2 scope, and hence it is questionable if we can have sufficient time in Rel-17 due to involvement of multiple WGs. |
| Xiaomi | No | Data integrity is not positioning integrity specific issue. |
| vivo | Maybe | Further discuss to determine if existing mechanisms in 3GPP / LPP are sufficiently error free for the purpose of positioning integrity. |
| MELCO | Yes | Yes, if the probability of miss detection is not negligible. |
| ZTE | Yes | Data integrity faults involve 3GPP procedures such as LMF to NG-RAN and NG-RAN to UE, also involve non-3GPP procedures such as GNSS correction providers to LMF. Obviously it has impact to the integrity results. |
| InterDigital | Maybe | While we see the benefit in addressing any issues related to data integrity faults, this aspect may not be specific to LPP spec. |
| Intel |  | It is difficult for RAN2 to do the analysis on the level of integrity can be achieved in the whole 3GPP system. |
| Samsung | No | We think data integrity issue is not only related to POS but also should involve the whole security related area from SA. So the issue needs a separate study in that group. |
| OPPO | Maybe | Agree with Qualcomm this is not a LPP issue |
| Ericsson | Maybe | Needs to be studied more. |

Question 3 (Phase 2): If you responded Yes to Question 2, please indicate how this topic could be addressed, including any other WGs that may need to be involved.

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | The first step is to do an assessment of what existing mechanisms are in place within 3GPP to assure data integrity. We defer to the RAN2 experts to determine what existing specifications should be studied and what other WGs if any need to be involved. |
| Qualcomm | Via a dedicated study, incl. at least RAN1 and RAN2. For specific solutions (in case it turns out there is a problem), at least SA2 and SA3 need to be consulted. |
| u-blox AG | This may require a separate study, which could span multiple WGs. |
| Nokia | A dedicated study is needed including at least RAN1 and RAN2 |
| vivo | For feared events during positioning data transmission, it involves the security, etc which belongs to other working groups rather than only RAN2. SA3 and RAN1 and SA2 need to be involved. |
| MELCO | Whatever the data correction techniques are used, the prior probability of data integrity fault and those miss detection probability should be evaluated. These probability may be hard-coded or transferred as parameter. Once these parameter are available, integrity computing entity can compute PL given them. |
| ZTE | How to detect data integrity faults and who will be responsible for this need further study and may spread to other WGs. |
| InterDigital | At this stage it is unclear what integrity requirements are unable to be satisfied with the existing mechanisms related to data integrity fault detection and possible correction/recovery. To address this, further study may be necessary involving different WGs based on certain inputs related to integrity requirements. |
| Intel | For Uu interface, RAN1/RAN2 are needed.  For interface between network entities, RAN3, SA2, SA3, CT are needed. |
| Ericsson | A dedicated study can be needed |

Question 4 (Phase 2): What types of integrity paramaters are needed in the assistance data to address the GNSS feared events?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | The purpose of the integrity assistance information is to allow the integrity computing entity to both reduce *and* attribute a quantified bound to the errors within the user’s position. The regular assistance data (e.g. SSR or RTK corrections) allow the error to be reduced, but the integrity assistance data must in addition allow for the errors to be mathematically bounded. Therefore the parameters should encode information about the statistical distribution of errors. The current state-of-the-art within the field of positioning integrity is to use “Gaussian overbounding” to represent this distribution (as discussed in [11][12][13]), although other representations are also possible. This means that for each error there should be a corresponding **bound** (parameterized as mu and sigma) as well as a “**residual risk**”, i.e. probability that these bounds are exceeded. It is also possible that a feared event is detected such that these bounds cannot be reliably computed, in which case a Do Not Use (DNU) **alert** flag should also be issued.  The parameters described above apply to a single epoch of time. For users who wish to take advantage of time-based estimation techniques such as Kalman Filtering they must also be provided with information about the time **correlation** of the errors. Additionally, as a feared event may occur at any time, each of these integrity assistance data elements must be given a **time of validity** as well as being associated unambiguously with the correction data to which they correspond. This time of validity ultimately becomes a driver for the Time To Alert (TTA) KPI.  Therefore, the main types of integrity parameters that are needed to address the GNSS feared events can be broadly categorized as: **Integrity Bounds, Residual Risks, Correlation Times, Alerts and Validity Times**. Further details on each is described in [13]. |
| Qualcomm | Should await the response from RTCM. But generally, the information required to determine the measurement variances, incl. uncertainty of the satellite orbit.  satellite clocks, signal code bias, signal phase bias, ionosphere, troposphere (bounding pseudo-range error standard deviations). |
| u-blox AG | Flags indicating unhealthy satellites and/or signals and flags indicating atmospheric disturbances that cannot be modelled or corrected for. The flags would preferably be enumerated to indicate the fault cause. Future version may be parameterized and based on RTCM models but we think this is beyond the scope of the present WI. |
| Huawei, Hisilicon | As discussed in SI phase, we think there are several candidates:   * Satellite health or quality flags; * Ionospheric indicator; * Tropospheric indicator;   Trustable time reference, Data Authentication / Signature, Regionalized indicator of multipath, interference, jamming, spoofing, etc. |
| Nokia | We think input from RTCM is needed before we make decisions about this in 3GPP, to avoid fragment across the industry. |
| Xiaomi | Both of the positioning integrity assistance information on GNSS feared event identified in SI and the input from RTCM can be considered. |
| vivo | The specific type(e.g., Satellite feared events) of GNSS feared event and the specific parameters(e.g., satellite clocks ) of a certain type should be indicated. |
| MELCO | Integrity bound and its corresponding residual risk are necessary for all types assistance data. To address atmospheric disturbances, standard deviation and correlation time of residual error are useful. |
| ZTE | The type of detected GNSS feared events should be indicated as error source. Each of them should have a flag and contains in the GNSS assistance data. |
| InterDigital | We have similar views with u-blox on this where certain indicators indicating the satellite and atmosphere conditions may be beneficial. Further inputs from RTCM may be considered, when available, for future enhancements. |
| Fraunhofer | Additionally, simple information that does not put imply any algorithm or method on LMF or UE side – for example, informing which SVs and which GNSS signals have been subject to spoofing, interference (from authorized systems sharing the same frequency or from malicious activities (e.g. truck drivers using jammers to conceal activities), etc  The network provides this information to avoid the UE processing the signals that are anyway not usable.  The capable UEs report the detection of intereference/spoofing/jamming as an optional feature. |
| Intel | Ok to wait for the response from RTCM. In general, agree with the information listed by Qualcomm. |
| Samsung | Same view as other companies on waiting for RTCM. |
| OPPO | Prefer to wait for the response from RTCM. |
| Ericsson | The lintegrity parameters tlisted above by Swift, categorized as Integrity Bounds, Residual Risks, Correlation Times, Alerts and Validity Times are good candidates, and so is the local environment information mentioned by Fraunhofer. To align with RTCM can be a reasonable strategy, but not only wait for them but to interact. |

Question 5 (Phase 2): Do you agree that the UE feared events will be handled via implementation for UE-based (network-assisted) methods of positioning integrity determination?

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Yes | The integrity function resides at the UE in this case meaning the feared events are handled in the implementation. |
| Qualcomm | Yes | Since highly implementation dependent as well as complex, making any standard definition unsuitable. |
| u-blox AG | Yes | They occur in the UE and will be handled by the integrity function in the UE. |
| Huawei, Hisilicon | Yes | We think most of the UE faults should be left for implementation for UE-based positioning integrity. |
| Nokia | Yes | the requirement relating to UE feared event is difficult to specify. |
| Xiaomi | Yes | It is not feasible to specify UE feared events, such as hardware faults, software faults and GNSS receiver measurement error, and it should be left to UE implementation. |
| vivo | Yes | They can be handled by the implementation. Besides, 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. |
| MELCO | Yes | The UE feared events can be handled by the implementation. |
| ZTE | Yes | For UE based method, UE calculates integrity results itself, and no feared events should be transferred |
| InterDigital | Yes | For UE-based methods the feared events detectable and available at UE can be handled by the UE and left to implementation |
| Intel | Yes | It is used by UE for UE based methods. |
| Samsung | Yes | We think that UE faults should be left for the implementation for the UEB. |
| OPPO | Yes | For UE-based methods, the UE feared events should be handled by the UE itself |
| Ericsson | Yes |  |

Question 6 (Phase 2): Do you agree that UE feared events need to be considered for UE-assisted (LMF-based) methods of positioning integrity determination? If Yes, which of the UE feared events need to be considered? Please explain your reasoning.

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Yes | Yes, it is possible for the measurements to contain errors corresponding to feared events at the UE. The LMF must be provided with necessary information to indicate and bound these errors. As all existing deployed systems are UE-based, there is little precedent in the industry for how these measurement errors should be quantified and categorized. We believe that robust study and further contribution is needed to determine what information will be required (as suggested in [8]). Furthermore, as GNSS measurement engines differ in implementation, they are also expected to differ in their susceptibility to noise, multipath, spoofing and jamming, and its unclear how this should be addressed within a UE-assisted integrity system. |
| Qualcomm | No | Same as for Question 5, UE feared events are highly implementation dependent.  I.e., all local FEs (e.g., environment, etc.) and Rx FEs (hardware/software faults, etc.) would need to be determined and standardized, which seems impractical. |
| u-blox AG | Yes | Some local events can only be determined by the UE and not the infrastructure and network provider: for example multipath, jamming and perhaps spoofing. If the UE is able to detect these events it would be helpful if it can indicate them to the LMF so that they can be taken into account in the position and integrity computation. They could be reported as simple flags or presence indicators for a particular location and satellite or signal. The flags would preferably be enumerated to indicate the reason. |
| Huawei, Hisilicon | No | Please find our reply for Question 5. |
| Nokia | No | Specification complexity is not bearable for Rel-17 |
| Xiaomi | No | The UE feared events identified in SI are hardware faults, software faults and GNSS receiver measurement error, for hardware faults and software faults, it is totally based on UE implementation, for GNSS receiver measurement. And it is also difficult to define a unified GNSS receiver error for different UE vendors, moreover, how to define the GNSS receiver error may be out of 3GPP scope. |
| Vivo | No | 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. |
| MELCO | Yes | GNSS receiver measurement error needs to be considered. LMF should be able to have measurement error model of UE in detail to compute valid PL. |
| ZTE | Yes | We agree with MELCO that GNSS signal measurement error should be reported as UE feared events to LMF |
| InterDigital | No | The availability of the information related to GNSS measurement errors and local environment (e.g. multipath, interference) at LMF is useful for accurately calculating integrity. However, it may be challenging for defining and specifying the indications that the UE may send to the LMF given the involvement of numerous implementation specific aspects related to GNSS receiver. |
| Intel | FFS | The UE could indicate the Errors in UE measurement. However HW/SW errors shall not be specified. |
| Samsung | No | UE FE’s must be difficult to have commonality per each vendor. |
| OPPO | Yes | For LMF based integrity determination, UE feared event information shall be transmitted towards LMF |
| Ericsson | Yes | This is needed in order for LMF to properly assess integrity, but also to enable crowd-sourcing of information to improve the service |

Question 7 (Phase 2): Do you agree that the LMF feared events can be handled via implementation for both the UE-based and UE-assisted modes of positioning integrity?

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Yes | For UE-based, the LMF is only passing data to the UE which can be handled by the data integrity scheme (see answer to Question 2). For UE-assisted, the integrity function resides at the LMF meaning these events are handled in the implementation. |
| Qualcomm | Yes | Note, that this also includes the provision of assistance data by an LMF (Question 1). |
| u-blox AG | Yes |  |
| Huawei, Hisilicon | Yes | As mostly agreed in SI phase, the LMF feared evetns, e.g. hardware faults, software faults, should be handled through implementation. |
| Nokia | Yes |  |
| Xiaomi | Yes |  |
| vivo | Yes | It is difficult to define what are the specific hardware and software faults because they are different for different vendors. |
| MELCO | FFS | Further discussion is needed to determine what could be the fault of LMF. If LMF cannot provide data (assistance data, integrity result e.g.) to UE (for some reasons such as time out), LMF should notify user of that (maybe by issuing “UNDEF” or “N/A” flag). |
| ZTE | yes | If LMF feared event only contains HW/SW errors, we think it is hard to detect or monitor. It should be left to implementation. |
| InterDigital | Yes |  |
| Intel | Yes | It is only related to UE based method, and do not see need to introduce additional assistance on LMF fear event for LMF to provide AD to UE. |
| Samsung | Yes |  |
| OPPO | Yes | Prefer the LMF feared event to be handled by the data integrity scheme |
| Ericsson | Yes |  |

### Follow-up questions from Q6 (Phase 1):

Question 8 (Phase 2): Should we use Common Positioning IEs (such as *CommonIEsRequestLocationInformation* and *CommonIEsProvideLocationInformation*) or A-GNSS Positioning IEs (such as *A-GNSS RequestLocationInformation* or *A-GNSS ProvideLocationInformation*) to transfer the KPIs and Integrity Results?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Common Positioning IEs – common positioning already includes the location estimate and associated requests on accuracy and confidence, so it makes sense to include the integrity KPIs and integrity results alongside these other positioning requirements. It also means these parameters can be commonly applied to more than one LPP positioning method (rather than A-GNSS alone), which may be relevant if integrity is extended to other techniques in future releases. |
| Qualcomm | Common Positioning IEs. However, it should be clarified (e.g., via a Note) that integrity reporting can only be requested for A-GNSS in this release.  The location estimate for all positioning methods is included in *CommonIEsProvideLocationInformation.* The location estimate normally includes an estimate of uncertainty (e.g., error ellipse). The "Integrity Information" (computed PL) could be added to *CommonIEsProvideLocationInformation*.  The desired TIR for the PL could be added to *CommonIEsRequestLocationInformation*. Whether the TIR (or integrity in general) should be part of the QoS concept or should be kept separate should be decided by SA1/SA2. For example, TS 22.071 (LCS Stage 1) lists examples of location services accuracy requirements. Similar exemplary integrity requirements for different user cases could be added to TS 22.071 as well. However, it seems integrity is not a "quality of service" but rather a "quality of the positioning system". |
| u-blox AG | We think it is more logical to put them in the Common Positioning IEs. |
| Huawei, Hisilicon | Common Positioning IEs.  We agreed with Swift that the positioning integrity is a common metric for positioning regardless of positioning methods. But we think other common IEs, such as *CommonIEsRequestAssistanceData* and *CommonIEsProvideAssistanceData*, can also be used to transfer the KPIs to assist the positioning integrity evaluation. |
| Nokia | Common Positioning IEs seem to be more logical and future proof. |
| Xiaomi | Common positioning IEs is more reasonable. |
| vivo | Common Positioning IEs. Integrity is a common function and not coupled with a specific positioning method, e.g., we can extend the integrity research to the RAT-dependent positioning method. |
| ZTE | Common Positioning IEs for more compatibility. |
| InterDigital | Common Positioning IEs |
| Intel | Common positioning IEs. |
| Samsung | Common IEs. |
| OPPO | *CommonIEsRequestLocationInformation* and *CommonIEsProvideLocationInformation* are preferred. |
| Ericsson | Common positioning IEs |

Question 9 (Phase 2): To address the case for UE-assisted, are the LPP procedures sufficient or do we need to invoke the LCS request and response to transfer the KPIs and Integrity Results?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | We prefer to use the LPP procedures and tend to agree with CATT that the interaction between the LMF and AMF/LCS client is FFS and outside of RAN2 scope. |
| Qualcomm | Integrity of positioning information belongs to a positioning protocol (LPP). LCS procedures should not be affected. |
| u-blox AG | It should be part of LPP. |
| Hisilicon | We think there may be some impacts on the LCS procedure for MO-LR cases. |
| Nokia | From our perspectives we should only consider LPP |
| Xiaomi | We should only consider LPP procedure. |
| vivo | For the KPI transfer,   * MO-LR UE-assisted Positioning Integrity Mode, integrity KPIs should be delivered to LMF from UE by LCS message (i.e., MO-LR Request). However, considering MO-LR Request can include LPP PDU(e.g., transfer location information, transfer capabilities, request assistance data), so in this case the LPP procedure is sufficient.   For the Integrity Result transfer,   * MO-LR UE-assisted Positioning Integrity Mode, Integrity Result should be delivered to UE from LMF by LCS message (i.e.,MO-LR Response). |
| ZTE | We think LPP is enough to transfer the KPIs and Integrity results |
| InterDigital | LPP procedures are sufficient |
| Intel | LPP is preferred as LCS is out of RAN2 scope. |
| Samsung | We think LPP is sufficient. |
| OPPO | In our opinion, LPP procedure is not enough. For the MO-LR LMF-based positioning integrity method, how would LMF know the KPI without transferring KPI using LCS procedure? |
| Ericsson | Part of LPP |

### Follow-up questions from Q8 (Phase 1):

Question 10 (Phase 2): Do you agree that Integrity Availability should be included as a KPI?

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | No | Integrity Availability is the percentage of time that the PL is below the required AL. According to the definition, a time series of PL results first needs to be recorded and aggregated so that the percentage of time that the PL is below the AL can be derived over this period. In this sense, while Integrity Availability is definitely a key indicator of performance, it is not a KPI in the same sense as AL, TIR, TTA. Availability can only be determined after the fact whereas the current KPIs are *inputs* to the integrity computation. |
| Qualcomm | No | The terms QoS and KPI are bit overloaded in this discussion. Integrity Availability should be implicit. I.e., if PL is requested but not provided, integrity of the position is obviously not available. |
| u-blox AG | Yes | The SI report TR 38.857 in section 9.1.1.2 lists four KPIs: TIR, AL, TTA and Integrity Availability.  TTA and Availability are performance requirements – they are the measured performance of the Integrity solution and as such are both key indicators of the achieved performance. AL and TIR are inputs to the integrity function and are used in the integrity function to compute the integrity output – yes safe / no unsafe.  However, Availability is not specific to integrity so there is an argument for not including it as an integrity KPI, even though “Integrity Availability” is listed as a KPI in the SI TR. |
| Hisilicon | No | We don’t see any benefit of integrity availability to be discussed in this phase, e.g. what does this indicator used for with the PL already being derived? |
| Nokia | No | It is not clear what difference can this KPI make in terms of integrity derivation and reporting |
| Xiaomi | No | We think the integrity availability is the result of the positioning integrity but not the KPI. |
| vivo | No | Referring to the PL calculation format “Prob per unit of time [((PE> AL) & (PL<=AL)) for longer than TTA] < required TIR”, Integrity Availability does not involve in it. Besides, Integrity Availability is the percentage of time that the PL is below the required AL. So Integrity Availability is not like a KPI as AL, TIR, TTA. |
| MELCO | Yes | We should agree with what “Integrity Availability” does mean.  If “Integrity Availability” means 1 minus probability of false alarm, it should be included as a KPI. Integrity computing entity needs the probability to determine threshold of statistics as well as to compute PL. |
| ZTE | no | Integrity Availability is a result of positioning integrity, not the requirement of positioning integrity |
| InterDigital | No | We share same views with Swift in that integrity availability is a derivative measure and not a KPI. |
| Intel | No | Agree with Swift and Qualcomm. |
| Samsung | No |  |
| OPPO | No | Integrity Availability could be derived implicitly from comparing the output of the PL with AL over time |
| Ericsson | Yes | We have the same view as u-blox that availability is relevant for service evaluation and assessments |

### Follow-up questions from Q9 (Phase 1):

Question 11 (Phase 2): Should an Integrity Flag for Mode 2 be Optionally reported in the Integrity Results to identify whether the PL satisfies the KPIs that are used in the integrity calculation?

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | No, with comments | We still don’t see the need to add this functionality within the UE given the same result can be derived in the LCS client by comparing the computed PL to the AL. If there’s a consensus view to support then we are ok to go with the group decision. |
| Qualcomm | No | There is no need to determine at the UE whether the PL satisfies the "KPIs". This can be done at the LMF. |
| u-blox AG | Yes | Mode 1: the integrity function computes a PL for a given TIR which the application compares with AL (for the same TIR) and if PL > AL sets a “potential loss of integrity” flag which causes the position output to become unavailable. In this case the integrity function is split between the entity that computes the PL and the part in the application that assesses the delivered PL against the required AL.  Mode 2: the integrity function computes whether the probability of the position error exceeding the AL is greater than the TIR directly and outputs the resulting “potential loss of integrity” flag to the application. In this mode there is no need for an exchange of PL as an intermediate variable between two separated parts of the integrity function.  Both Modes 1 and 2 could have roles to play in integrity implementations, each having advantages and disadvantages. Both modes should be supported. |
| Hisilicon | Yes | We believe Mode 2 can reduce the complexity for LCS client since 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. So the LCS client doesn’t need to conduct further evaluation. |
| Nokia | Yes | Mode 2 may allow LMF to react quicker by implementation, as the LMF can become aware that some positioning performance improvement is needed without further instructions from the LCS client. This is particularly more future proof when positioning integrity is considered in RAT-dependent positioning. |
| Xiaomi | No | Even if UE calculates the positioning integrity on whether the positioning system is available or not and reports it, the UE following actions can’t be decided by UE itself. So we think mode 1 is enough. |
| vivo | 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. |
| MELCO | No | PL is enough to handle the integrity. |
| UE | Yes | If integrity computing entity has the capability, it is more flexible to choose whether to report PL, or one step further, to report integrity flag. |
| InterDigital | Yes | Mode 2 as an integrity event flag is beneficial for certain position sensitive applications (e.g. IIoT) and as pointed out by Nokia could serve a useful purpose as a future proof metric for positioning integrity. In the case when PL is already reported then optionally reporting a flag in the integrity result, as pointed out in the question, may not be needed. |
| Intel | No | It would be good to avoid multiple solutions for the same purpose. Mode 1 should be sufficient. |
| Samsung | Yes | It is obvious that including this makes less computation at the LMF. |
| Ericsson | Yes | With Mode 2, this is natural |

Question 12 (Phase 2): Do you think the TIR, AL & TTA that are used in the integrity calculation should be Optionally reported in the Integrity Results (for either Mode)?

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Swift Navigation | Yes | Depending on several factors, it may not always be possible to achieve the requested integrity KPIs. This may depend on the quality and type or assistance data available as well as the specific implementation choices. Therefore it is necessary to report out what KPIs were achieved vs what was requested. Conceptually this is similar to the Best Effort vs Assured modes in the LCS QoS message. |
| Qualcomm | No | The UE should provide the PL for the TIR requested. If needed, multiple TIRs could be included in the request. |
| u-blox AG | Yes | TIR and AL are the two defining parameters which the output has to meet in order to determine the state of integrity – yes safe / no unsafe. As such they need to be known by both the integrity function and the application, and, therefore there cannot be a common understanding of the interpretation of the PL without shared knowledge of the TIR and there cannot be a common interpretation of the loss of integrity flag without a shared knowledge of TIR and AL.  TTA is a measure of the performance of the integrity function. As such it is not used in computation of the integrity output. However, there are potential advantages in having shared knowledge of the required TTA in both the Integrity computation entity and the Location client application.  Integrity is very important and transparency between the integrity function and the user application is equally important. |
| Hisilicon | Yes | We think the KPIs used in the integrity calculation may provide additional assistance information for the integrity results.  For example, for UE-based positioning integrity, the computing entity (i.e. UE) can report the integrity results (PL or Integrity Flag) together with the related KPIs to LMF. Then LMF may be aware the gap between “what can or has been reached” and “what is required”. This may be helpful especially when the integrity requirement is not satisfied, e.g. LMF can make some adjustment to approach the requirement. |
| Nokia | Yes | Yes, If the question is about the TIR or AL **achieved** by the integrity calculation. Having the TIR achieved for the specified AL or the AL achieved for the specified TIR (or combinations of both) can be useful information. This can allow the application to adapt (downgrade) its performance requirements when possible. This functionality should remain optional. |
| Xiaomi | No | For the UE based positioning integrity, if the location service is MO-LR, the positioning integrity KPIs are based on UE internal implementation, so it is not feasible to deliver the implementation based KPIs to LMF. |
| Vivo | No | PL is only calculated according to the requested KPIs. But if requested KPIs have several values, then the chosen requested KPI can be reported in the Integrity result. |
| MELCO | Yes | TIR is necessary if LMF returns alternative for example when original PL exceeds AL and LMF computed other PL with larger TIR. |
| ZTE | no | The indicated KPIs are the requirements from LCS client, and LCS client only focuses on whether the required KPIs can be achieved or not by the UE. |
| InterDigital | Yes | We share similar views with Huawei and Nokia in that when reporting the integrity result it is useful to provide the gap/difference with respect to the KPIs (i.e. AL, TIR). Based on this information, the LMF may perform certain adaptations that may result in minimizing the gap. |
| Intel | No | Should not PL is sufficient for Client to judge whether the result can be used? |
| Samsung | Yes | We can see the case that Swift said. |
| OPPO | No | Only integrity Results but not the integrity KPI should be informed |
| Ericsson | Yes |  |

Question 13 (Phase 2): Which Other indicators should be considered in the integrity results?

* Option 1: Difference between the calculated integrity result and the KPIs (InterDigital)
* Option 2: The degrees of integrity risk (e.g. Extremely High/High/Low/No risk) (Huawei)
* Option 3: Failure to calculate the PL (alarm) (CATT)
* Option 4: Integrity Availability (u-blox)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Company | Opt 1 | Opt 2 | Opt 3 | Opt 4 | Comments |
| Swift Navigation | No | No | FFS | No | All options can be computed by the LCS client. Opt 3 will likely be handled as part of the procedures for signaling the integrity results. |
| Qualcomm | No | No | No | No | All these Options can be determined by an LMF based on the location request and the reported PL. |
| u-blox AG | No | No | Yes | No | Opt 1: If the integrity computation entity is unable to compute a result for the requested KPIs it should return no result rather than one for different KPIs.  Opt 2: we don’t see a need for this. Classifying risk is difficult to do and depends on the degree of safety criticality in the application.  Opt 3: Needed in Mode 1 but not Mode 2.  Opt 4: It needs to be possible to calculate the integrity availability (it is a KPI according to TR 38.857) for performance measurement purposes but it is not necessary to include it as part of the integrity results. |
| Hisilicon | No | Yes | No | No | We prefer to Option 2. Now the system operation state is roughly divided into two categories: System Available (PL<AL) and System Unavailable (PL>AL). 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)”. We can refine the integrity results with the degrees of integrity risk (Extremely High/High/Low/No risk). Then with the refined integrity results, the LCS client may know how to react according to different alarm levels, e.g., shutting down the system or making some adjustment. |
| Nokia | No | No | No | No | We think only Option 1 may be useful but we believe both Mode 1 (PL reporting) is already sufficient for LCS clicent to derive by itself. Therefore we do not see the need of additional signaling. |
| Xiaomi | No | No | No | No | At this stage, we think above options are not needed. |
| vivo | No | No | No | No | There is no need to include these 4 indicators in the integrity result. Because the LCS client can obtain them based on the PL situation. |
| MELCO | No | No | No | Yes | As answer to Q. 10, it is good idea to include “Integrity Availability” if means 1 minus probability of false alarm. |
| ZTE | no | no | yes | no | For opt 1, there is no need to define the difference as LCS client wants to know the results of satisfied or unsatisfied. LCS client can acquire the answer of Opt 2 and 4 based on PL reporting.  Opt 3 makes sense that some UE may not calculate PL or integrity results |
| InterDigital | Yes | No | No | No | We have a slight preference towards Opt 1 as an optional indication when supporting Mode 2 (integrity event flag) for integrity result. This is mainly for indicating how far is the achieved integrity result with respect to KPIs. |
| Intel | No | No | No | No | Agree with Qualcomm. |
| samsung | No | No | No | No | At current stage, we think LMF can calculate what it needs. |
| OPPO | No | No | No | No | All options are unnecessary. |
| Ericsson | No | No | No | Yes | Integrity availability can enhance servive evaluations from the operator perspective |

## 5.2 Phase 2 Proposals

### Proposals resulting from Q1 (Phase 1):

Proposal 1 (Phase 2): Agree that the GNSS feared events will be addressed in the WI.

### Proposals resulting from Q2/Q3 (Phase 1):

Proposal 2 (Phase 2): Agree that all A-GNSS positioning techniques in LPP (including RTK / PPP / PPP-RTK) should support positioning integrity determination.

Proposal 3 (Phase 2): Agree that all A-GNSS positioning techniques in LPP (including RTK / PPP / PPP-RTK) require additional assistance data in order to support positioning integrity determination.

### Proposals resulting from Q4/Q5 (Phase 1):

Proposal 4 (Phase 2): The specific algorithms used for positioning integrity shall be up to implementation.

Proposal 5 (Phase 2): For interoperability, the use of “hard-coded” parameters should be minimized and instead the needed parameters should be sent explicitly in the assistance data.

### Proposals resulting from Q9 (Phase 1):

Proposal 6 (Phase 2): RAN2 agrees that the PL will be reported in the Integrity Results.

Any further comments on the proposals?

|  |  |
| --- | --- |
| Company | Comments |
| u-blox AG | Proposal 2: Suggested wording: “All GNSS methods shall support integrity in LPP.” A particular implementation may not support the integrity feature but LPP must include it.  Proposal 3: This proposal is not clear – is it saying that in order to support integrity additional IEs are needed in LPP?  Proposal 6: PL is reported only for Mode 1. If Mode 2 is supported the “loss of integrity” flag is reported instead of PL. This proposal can only be agreed after an agreement whether support for Mode 1 and Mode 2 has been clarified. |

# 6. Conclusions

## Easily Agreeable…

TBC in the Final round

## Further Discussion Required…

TBC in the Final round

# 7. 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.