3GPP TSG-RAN WG2 Meeting #113-Bis-e
Electronic, April 12 – 20, 2021

R2-2103954

Agenda item: 8.11.5

Source: Swift Navigation, Intel Corporation, Ericsson

Title: Considerations on Positioning Integrity Determination

Document for: Discussion, Agreement

1. Introduction

A new WI for positioning integrity [1] has been defined with the following objectives:

- Specify the signalling, and procedures to support GNSS positioning integrity determination, including [RAN2, RAN3]:
  - The assistance information that will be used to support integrity determination
  - The information that will be used to provide the positioning integrity KPIs and integrity results
  - Support of integrity for UE-based and UE-assisted A-GNSS positioning.

  Note: This objective is applicable to NR and E-UTRA.

This submission expands on the Positioning Integrity findings from the Study on NR Positioning Enhancements [2]. It discusses key integrity concepts and information to be considered for specification into 3GPP.

2. Considerations for Specifying Positioning Integrity

The following sections review and extend on the findings from the Study [2], to introduce key positioning integrity concepts that are necessary for addressing the WI objectives.

2.1 Terminology

The following terms are used in this proposal in addition to those already defined in TR 38.857 [2].

- **Fault Feared Event –** A Feared Event that occurs intrinsic to the positioning system, i.e. caused by the malfunction of one of the elements of the positioning system (e.g. a software fault within the ICE).
- **Fault-Free Feared Event –** A Feared Event that is not caused by a malfunction of the positioning system. Fault-Free conditions are typically when the positioning system inputs are erroneous e.g., out of bound ionospheric and tropospheric conditions or a GNSS satellite fault.
- **GNSS Corrections Provider (GCP) -** Generates the A-GNSS integrity assistance data, external to 3GPP.
- **Integrity Computing Entity (ICE)** (adapted from [3]) - The logical entity responsible for computing the positioning integrity results. Such an entity can reside in either UE or LMF.
- **Integrity Monitor –** Any algorithm dedicated to the reduction of the integrity risk. In general either by detecting the presence of feared events, or by adapting any appropriate bound parameters. Integrity Monitors can reside at the UE, the ICE, the LMF and the external source (e.g. the GCP).

- **Nominal State –** A Nominal State occurs when the positioning system is operating in line with its performance specifications and no Feared Event is present, such that the Nominal State errors are considered to have a probability of 1.
- **Probability of Occurrence –** The probability of onset of a given Feared Event provided that it was not present before (usually defined per time unit and/or per time window).
- **State Probability -** The probability of a Feared Event to be present at a given epoch. This probability is unitless and is a consequence of both the probability of occurrence and the fault duration.
- **Probability of Missed Detection -** The probability that the Feared Event was not detected by the Integrity Monitor, given that the corresponding Feared Event is present.
- **Probability of Impact –** The probability that the system will not meet its integrity bounds under a given set of conditions.

2.2 Positioning Integrity Assistance Information

Positioning Integrity is a measure of the trust in the accuracy of the position-related data provided by the positioning system and the ability to provide timely and valid warnings to the LCS client when the positioning system does not fulfil the condition for intended operation [2].

To implement positioning integrity it is necessary to monitor for feared events in the positioning system. Generally speaking, Integrity Monitors are used to detect the feared events that occur more frequently than is acceptable to meet the Target Integrity Risk (TIR) and other KPIs, i.e., the monitor's purpose is to reduce the likelihood that feared events go undetected.

The Study [2] identifies that integrity monitoring can be undertaken by the UE, the ICE, the LMF and the external GNSS Corrections Provider (GCP), depending on the implementation. The resulting integrity parameters (e.g., alert flags, bounds etc.) can be signalled as assistance information between the LMF and the UE to support UE-based and UE-assisted positioning modes. A simplified relationship between these entities is presented in Figure 1, and the benefits of using integrity assistance data from an external source (e.g., the GCP), disseminated via NR and E-UTRA, are summarized below:

<u>Benefits of using positioning integrity assistance data from an external source (disseminated via NR and E-UTRA):</u>

1. Less overhead on the ICE, i.e. no need to monitor everything on the ICE. Monitoring responsibilities can be allocated between the ICE and the GCP (and/or the UE and LMF) and disseminated as assistance data.

2. The GCP can monitor specific feared events (e.g. satellite faults and ionospheric gradients) with higher resolution / sensitivity than the UE alone, using GNSS reference stations distributed across a wide area.

3. Higher sensitivity integrity monitoring enhances performance with respect to the positioning integrity KPIs and use cases, such as allowing for a lower TIR or Alert Limit (AL).

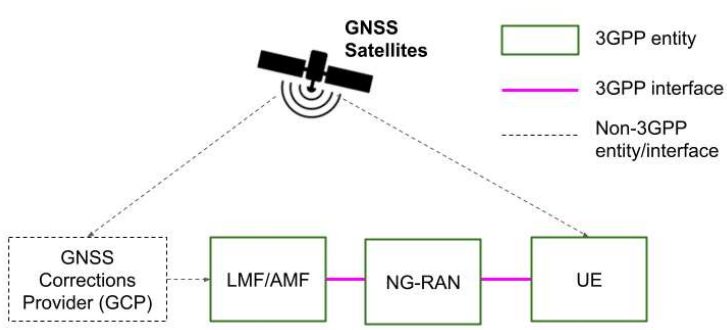

Figure 1. Simplified relationship between the 3GPP and non-3GPP entities and their interfaces for transferring positioning integrity assistance data between the LMF and UE (adapted from [2])

The following observations can be made from Figure 1 with respect to the Study findings [2] and WI objectives [1]:

- Feared events can be monitored by the GCP, the LMF, the ICE and the UE.
- The GCP is a non-3GPP entity whose interface to the LMF is implementation-defined.
- Integrity monitoring algorithms within each entity are implementation-dependent.
- The integrity parameters determined by each entity can be encoded as assistance information and signalled between the LMF and UE (i.e. using LPP).
- The ICE can reside at the LMF (UE-assisted) or the UE (UE-based) to compute the Integrity Results (e.g. a PL).
- The Integrity Results can be reported to the LCS Client, which may reside at the LMF or the UE.

These findings have therefore led to the WI objectives:

- Define the assistance information that will be used to support integrity determination
- Define the information that will be used to provide the positioning integrity KPIs and integrity results
- Support of integrity for UE-based and UE-assisted A-GNSS positioning.

A table of UE-based and UE-assisted integrity mode considerations examined in the Study [2] is also provided in **Appendix A** to assist with specifying the signalling procedures and assistance information.

2.3 Transfer Procedures

Simplified descriptions of the LPP procedures to be considered for transferring assistance data and other information described in Section 2.2 are provided in Figure 2 (UE-based) and Figure 3 (UE-assisted) to illustrate these concepts.

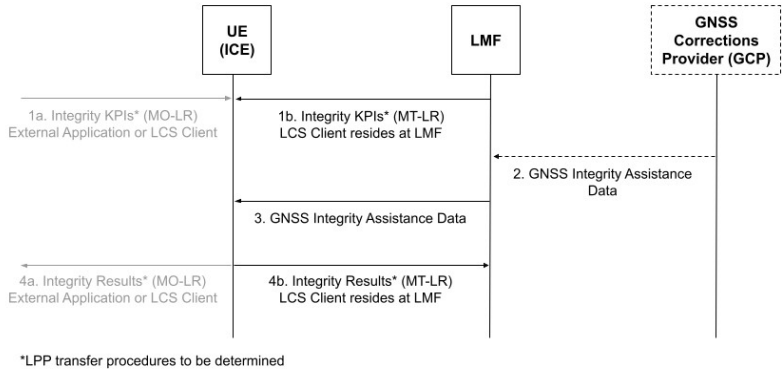

Figure 2. UE-based transfer procedures for supporting positioning integrity determination via LPP

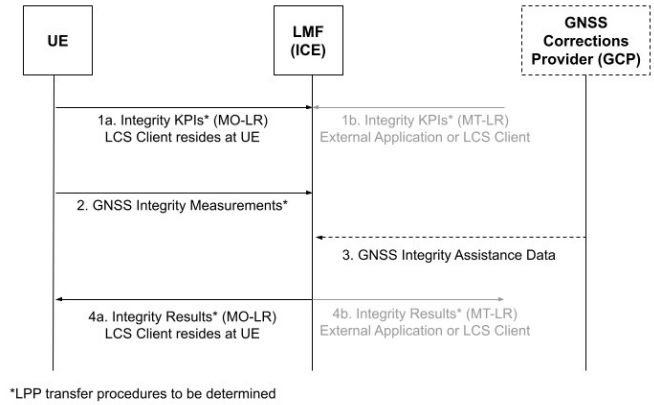

Figure 3. UE-assisted transfer procedures for supporting positioning integrity determination via LPP

2.4 Feared Event Categories

Five categories of feared events were examined in the Study [2] which are summarised in Table 1 below. In order to achieve positioning integrity, these feared events must be monitored and accounted for. The monitoring of feared events can occur in various places within the system as defined by the particular implementation. All feared events may be monitored by the ICE itself, but alternatively, or in addition to the ICE, may rely on monitors present in other locations where there may be additional information available to strengthen the monitoring process. For example, the UE may have additional measurements it can make to detect the presence of spoofing or multipath. The GCP may have the ability to monitor using a reference network consisting of many GNSS reference stations. Therefore we further categorize the feared events depending on where it is possible for them to be monitored.

Feared Event Category	**Feared Event**	**Location(s) of Integrity Monitor(s)**
1. Feared events in the GNSS Assistance Data	Incorrect computation of the GNSS Assistance Data, e.g. software bug, corrupt or lost data	GCP, ICE
	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	ICE
3. GNSS feared events	Satellite feared events e.g. bad signal-in-space or bad broadcast navigation data	GCP, ICE
	Atmospheric feared events	
	Local Environment feared events, e.g. Multipath, Spoofing, Interference	UE, ICE
4. UE feared events	GNSS receiver measurement error	
	Hardware faults*	
	Software faults*	
5. LMF feared events**	Hardware faults*	LMF (ICE) **
	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.

**NOTE: LMF feared events are only applicable to the UE-Assisted case and may be left up to implementation. In this case the ICE is located within the LMF.

Table 1: Summary of A-GNSS feared events categories (adapted from [2]) showing where in the system the integrity monitors can be located to detect the feared events

2.5 Mathematical Framework for Integrity

The notation below is first defined.

Parameter	Description
$P(I_{nom})$	Probability of impact in the Nominal State conditions
$P(FE)$	State Probability of a specific Feared Event (FE)
$P(MD_{GCP}\|FE)$	Probability that the monitor in the GCP fails to detect the FE (missed detection, MD), given that the FE is present
$P(I_{GCP}\|MD_{GCP})$	Probability that the FE causes the GCP to violate its bounds, given that the FE is present and was failed to be detected by the GCP
$P(MD_{ICE}\|I_{GCP})$	Probability that the monitor in the ICE fails to detect the FE (missed detection), given that the GCP is violating its bounds
$P(MD_{UE}\|FE)$	Probability that the monitor in the UE fails to detect the FE (missed detection), given that the FE is present
$P(I_{UE}\|MD_{UE})$	Probability that the FE causes the UE to violate its bounds, given that the FE is present and was failed to be detected by the UE
$P(MD_{ICE}\|I_{UE})$	Probability that the monitor in the ICE fails to detect the FE (missed detection), given that the UE is violating its bounds
$P(I_{FE}\|MD_{ICE})$	Probability that the integrity system fails to meet its bounds (HMI), given a missed detection at the ICE

Table 2. Description of positioning integrity probabilities

The governing equation for integrity [5] is that the sum of all the integrity risks must be less than the TIR. The integrity risk can be considered as a probability of impact to integrity in the Nominal State plus the sum of the probability of impacts of each of the feared events:

$$P(I_{nom}) + \sum_{FE} P(I_{FE}) < TIR$$

Equation 1. The positioning integrity inequality

Where $P(I_{nom})$ is the probability of impact in the Nominal State, and $P(I_{FE})$ is the Probability of Impact of a given Feared Event (FE). It is useful to decompose $P(I_{FE})$ into contributions from the various components of the integrity system as follows:

$$P(I_{nom}) + \sum_{FE_{GCP}} P(FE) \,.\, P(MD_{GCP}|FE) \,.\, P(I_{GCP}|MD_{GCP}) \,.\, P(MD_{ICE}|I_{GCP}) \,.\, P(I_{FE}|MD_{ICE})$$

$$+ \sum_{FE_{UE}} P(FE) \,.\, P(MD_{UE}|FE) \,.\, P(I_{UE}|MD_{UE}) \,.\, P(MD_{ICE}|I_{UE}) \,.\, P(I_{FE}|MD_{ICE}) < \mathrm{TIR}$$

Equation 2. Decomposing the positioning integrity inequality

Where FE_{GCP} are the FEs that can be monitored by the GCP, and FE_{UE} are the FEs that can be monitored by the UE. All FEs may additionally be monitored by the ICE itself. Note that LMF FEs (Table 1, Category 5) are not considered in this analysis as they are always up to the implementation to monitor and/or mitigate.

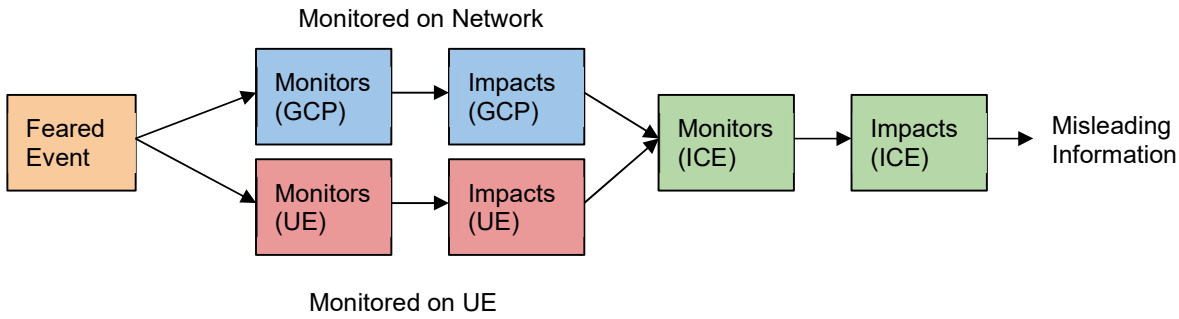

Figure 4. Illustrating the positioning integrity inequality relative to the system components

In order for there to be an impact, the FE must first occur, with associated probability $P(FE)$. Then the FE must be missed by the monitors checking for that FE. The monitors may be implemented by the GCP, the ICE and/or UE.

For each monitor there is a corresponding probability of Missed Detection (MD) given the presence of a specific FE, $P(MD|FE)$, as well as the probability that if there is an MD that this will result in an impact to the integrity bounds. The Probability of Impact is denoted as $P(I|MD)$. This additional impact term is useful as, for example, a FE that has a very small magnitude may be difficult to monitor but may also have a lower chance of causing an impact. In general, the constraint in Equation 2 should be maintained for any FE magnitude.

Note that the final term $P(I_{FE}|MD_{ICE})$ denotes the probability of an impact on positioning integrity, i.e. an integrity event / Hazardously Misleading Information (HMI). However, the intermediate term $P(I_{GCP}|MD_{GCP})$ denotes the probability of an impact on the integrity assistance data provided by the GCP, i.e. an assistance data parameter is outside of its specified bounds.

2.6 Interoperability Considerations between the ICE and the GCP/UE

The ICE needs all of the parameters in Equation 2 in order to compute the integrity results. These parameters represent the assumptions made by the system about certain probabilities resulting from the system design and implementation. These parameters must also be agreed between the UE, the GCP and the ICE in order for interoperability.

These parameters can be set in various ways, as illustrated in Table 3:

- **(IM)**: Implementation-defined (i.e., 3GPP does not specify how these parameters should be agreed upon).
- **(HC)**: Specified explicitly in the normative work (i.e., "hard coded")
- Dynamic parameters communicated between the entities of the 3GPP Network:
    - **(AD)**: In the GNSS Integrity Assistance Data
    - **(ME)**: In the Measurements from the UE (UE-Assisted)

In Table 3 we consider three options for how these parameters can be agreed to ensure interoperability. In Option 1, agreement on the parameters is considered to be out of scope of 3GPP and must be handled by implementation or by some other mechanism outside of 3GPP. Option 3 on the other hand implicitly defines in the specifications the exact parameters and probabilities that need to be met in order to be interoperable (i.e., essentially setting thresholds of performance that the GCP or UE integrity monitors must meet). Option 2 provides the highest flexibility in the implementation by enabling the GCP and/or UE to dynamically communicate the parameters, allowing the ICE to know explicitly what parameters should be used.

We believe that Option 1 should not be considered, as it is contrary to interoperability and there is risk of incompatible systems being used in conjunction, which could easily lead to integrity being violated. Due to the complex trade-offs between parameters that depend on choice of implementation, we also do not recommend Option 3. Option 3 would reduce the possibility for innovation by the vendors and create a large burden on the standardization effort to research and correctly set each parameter. We believe that Option 2 should be pursued as it allows explicit interoperability, improved safety and allows for vendors to innovate on different implementation choices.

	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	
Parameter	**UE-Based**	**UE-Assisted**	**UE-Based**	**UE-Assisted**	**UE-Based**	**UE-Assisted**
$P(FE)$	IM	IM	AD/ IM	AD / ME	HC / IM	HC
$P(MD_{GCP}\|FE)$	IM	IM	AD	AD	HC	HC
$P(I_{GCP}\|MD_{GCP})$	IM	IM	AD	AD	HC	HC
$P(MD_{GCP}\|I_{GCP})$	IM	IM	IM	IM	IM	IM
$P(MD_{UE}\|FE)$	IM	IM	IM	ME	IM	HC
$P(I_{UE}\|MD_{UE})$	IM	IM	IM	ME	IM	HC
$P(MD_{ICE}\|I_{UE})$	IM	IM	IM	IM	IM	IM
$P(I_{FE}\|MD_{ICE})$	IM	IM	IM	IM	IM	IM

Table 3. Comparison of options for how integrity parameters can be agreed for interoperability

Observation 1: Integrity assumed probability parameters can be signalled between the GCP/UE and the ICE. These parameters do not need to be hardcoded in the specifications.

Observation 2: The transfer of the assumed probability parameters can be accomplished between the LMF and the UE using the existing LPP transfer procedures.

Proposal 1: Agree that for UE-based positioning the assumed probability parameters relating to the GCP can be transferred from the LMF to the UE using the Assistance Data Transfer Procedure.

Proposal 2: Agree that for UE-assisted positioning the assumed probability parameters relating to the UE can be transferred from the UE to the LMF using the Location Data Transfer Procedure.

2.7 Interoperability Considerations between the ICE and the LCS

The LCS and the ICE must agree together on the KPIs to be used for an integrity computation. The LCS may have some requirements on the KPIs depending on the application and use case. The ICE may have some constraints on what ranges of KPIs it is able to achieve depending on the implementation. The ICE may also be constrained in what KPIs it is able to achieve depending on the assumed probability parameters received from the UE and/or GCP.

Our proposed solution (Section 2.3, Figures 2 & 3) is that the LCS should request the KPIs that it hopes to achieve from the ICE. The ICE must then return, together with the integrity results, the actual KPIs that were achieved during the integrity computation, which may sometimes be lower than the requested KPIs from the LCS.

As shown in Figures 2 and 3, the KPIs can then be transferred between the LMF and the UE depending on the Location service type (e.g., MO-LR, MT-LR) and chosen the positioning mode (e.g., UE-based, UE-assisted), as described in Appendix A. We propose to reuse the LPP transfer procedures for this purpose.

Further to the Study findings [2], we do not believe it is practical to set predefined discreet levels for the KPIs as there are too many combinations and trade-offs between the multiple KPIs. Such predetermined levels would be too constraining on the implementation and would limit innovation in the integrity monitors and ICE, without providing any additional benefit compared to the request/provide method of transferring KPIs.

3. Addressing the WI Objectives

3.1 The assistance information that will be used to support integrity determination

3.1.1 GNSS Integrity Assistance Data

This section focuses on identifying the types of messages that can be sent as GNSS Integrity Assistance Data (see Figures 2 and 3) from the GCP to the ICE. These messages correspond to mitigating the FEs represented by Category 1 (GNSS Feared Events in the Assistance Data) and Category 3 (GNSS Feared Events) in Table 1. The assistance information corresponding to Categories 2 (Feared events during positioning data transmission) and 4 (UE feared events) are further addressed in Sections 3.1.3 and 3.2 respectively. Further discussion and agreement is needed before the messages in Table 4 can be fully defined and proposed for adoption into the specifications.

The message types are grouped into the following categories:

- **Alerts:** instruction not to use certain GNSS Assistance Data IEs due to feared event.
- **Snapshot:** information necessary for the UE to monitor its integrity if it makes no assumption on the residual error dynamics in time.
- **Sequential:** additional information necessary for the UE to monitor its integrity when using sequential algorithms (e.g. Kalman) that makes assumptions on the dynamics of the error in time.

Message Type	Update Rate (TBD)	Message Content
GNSS Service		
Alert	TBD	● Service DNU Flag
	TBD	● Constellation Health Status
Satellite		
Alert	TBD	● Satellite Vehicle DNU Flag
Snapshot	Low	● Time of validity ● Satellite Vehicle probability of fault ● Satellite Vehicle maximum fault duration ● Constellation probability of fault ● Constellation maximum fault duration
	Low	● ID of correction that can be used with this bound ● Time of validity ● Range degradation factor ● Range rate degradation factor ● Yaw error bound ● Yaw rate error bound ● Code bias error bound ● Code bias rate error bound ● Phase bias error bound ● Phase bias rate error bound
	Medium	● ID of correction that can be used with this bound ● Time of validity ● SV Orbit and clock residual error bounds covariance/bias shape ● SV Orbit and clock rate residual error bounds covariance/bias shape
	Fast	● ID of correction that can be used with this bound ● Time of validity ● SV Orbit and clock residual error bounds scale factors ● SV Orbit and clock rate residual error bounds scale factors

Sequential	Low	● Time of validity ● Correlation time SV range error orbit ● Correlation time SV range error clock ● Correlation time SV range rate error orbit ● Correlation time SV range rate error clock
Ionosphere		
Alert	TBD	● Ionosphere DNU Flag
Snapshot	Low	● Time of validity ● Ionospheric residual risk ● Probability of cycle slip due to ionosphere condition ● Maximum ionospheric fault duration
	Low	● ID of correction that can be used with this bound ● Time of validity ● Iono degradation parameter ● Iono rate degradation parameter
	Medium	● ID of correction that can be used with this bound ● Time of validity ● Iono residual error bound ● Iono rate residual error bound
Sequential	Low	● Time of validity ● Correlation time ionospheric range error ● Correlation time ionospheric range rate error
Troposphere		
Alert	TBD	● Troposphere DNU Flag
Snapshot	Low	● Time of validity ● Tropospheric residual risk ● Maximum Tropospheric fault duration
	Low	● ID of correction that can be used with this bound ● Time of validity ● Tropo degradation parameter ● Tropo rate degradation parameter
	Medium	● ID of correction that can be used with this bound ● Time of validity ● Tropo residual error bound ● Tropo rate residual error bound
Sequential	Low	● Time of validity ● Correlation time tropospheric range error ● Correlation time tropospheric range rate error

Table 4. Message types that can be sent as GNSS Integrity Assistance Data from the GCP

Observation 3: The integrity messages in Table 4 can be transferred between the LMF and UE as LPP GNSS Integrity Assistance Data to meet the requirements of UE-Based Integrity.

Proposal 3: Agree to define the GNSS Integrity Assistance Data IEs corresponding to the integrity messages identified in Table 4.

Proposal 4: Agree to define extensions to the LPP GNSS Assistance Data IEs within the existing Assistance Data Transfer Procedure to incorporate new GNSS Integrity Assistance Data IEs.

3.1.2 Interpretation of the Integrity Assistance Data Parameters

The proposed GNSS Integrity Assistance Data parameters include several different kinds of information:

- Residual risk values
- Bound values
- Additional assumed probability parameters (as detailed in Section 2.5)
- Correlation time parameters

The principle of operation is that the probability of impact (i.e. that some true value exceeds the stated bound, without a corresponding alert being raised) is guaranteed to be less than the corresponding residual risk value. The residual risk is denoted as $P(I_{GCP})$ and is the product of three of the parameters detailed in Section 2.5:

$$P(I_{GCP}) = P(FE) \,.\, P(MD_{GCP}|FE) \,.\, P(I_{GCP}|MD_{GCP})$$

$$\geq P(NOT\ alert\ \&\&\ true\ value\ >\ bound)$$

3.1.3 Requirements on the Transport Layer

To prevent the FEs of errors during data transmission (Table 1, Category 2), the communications between the entities must be protected against accidental data corruption as well as manipulation of the data by a malicious attacker.

We propose that state-of-the-art security measures are used to prevent deliberate attack on the data communications, and that no integrity budget is allocated to this case, i.e. the residual risk of malicious attack on the data communications after the security measures have been implemented is assumed to be zero. An example of a measure that could be employed is a digital signature of the assistance data that provides end-to-end validation of the authenticity of the data.

For accidental corruption the data should be protected using a CRC, parity check or other suitable method. It is FFS whether the existing mechanisms provided in the transport layers underneath LPP are sufficient to meet the needs of integrity.

<u>Worked Example:</u>

Allocate an integrity budget (residual risk) of 10^{-8}/hr, i.e.,

$$P(I_{FE}) < 10^{-8}/hr$$

$$P(FE) = \text{message rate} * \text{message length} * \text{Bit Error Rate (BER)}$$

$$P(MD|FE) = 2^{-L}, \text{ where L is the CRC length in bits}$$

$$P(I_{FE}) = P(FE) \,.\, P(MD|FE) \,.\, P(I|MD) < 10^{-8}/hr$$

Assume P(I|MD) = 1, as any undetected bit error could cause an integrity failure

Assume 1 Hz message rate, 250 bits message, BER 10^{-5}/bit:

$1 * 3600 * 250 * 10^{-5} * 2^{-L} * 1 < 10^{-8}$

$2^{-L} < 10^{-9}$

$L > \log_2(10^9)$

$L > 30$ bits

Observation 4: It is FFS whether the existing mechanisms provided in the transport layers underneath LPP are sufficient to meet the needs of positioning integrity, to mitigate feared events during data transmission.

Proposal 5: Agree to identify the BER and CRC length in the existing LPP data integrity mechanisms and determine if they are suitable to support positioning integrity.

3.2 The information that will be used to provide the positioning integrity KPIs and integrity results

In Section 2.3 it was illustrated that the KPIs can be sent between the UE and the LMF depending on the positioning mode. From the Study [2], the KPIs for supporting positioning integrity determination should include the:

- TIR: Target Integrity Risk
- AL: Alert Limit
- TTA: Time to Alert

For the Integrity Results reporting, we propose to include the:

- PL: Protection Level
- Achieved KPIs: i.e., the actual KPIs that were achieved during the integrity computation, which may sometimes be lower than the requested KPIs.

Any other data, such as an overall integrity flag, can be derived from these values for comparison and does not need to be explicitly reported.

In Section 2.3 the procedures for transferring the KPIs and integrity results between the LMF and UE are to be determined. Several options were investigated in the initial contributions to the Study, including [4]:

- *Location Information Transfer*: procedures to request/provide integrity KPI's (e.g., as part of QoS) to the target, and for the target to provide integrity results to an LMF and/or UE (e.g., as part of the location estimate).
- *Assistance Data Transfer*: procedures to transfer the requested KPIs.

We agree that the LPP transfer procedures can be reused for this purpose and that the most suitable option can be determined as part of the normative work.

Proposal 6: Agree that the existing LPP procedures can be used for transferring the integrity KPIs (TIR, AL, TTA) and integrity results (PL, Achieved KPIs) between the UE and the LMF.

3.3 Support of integrity for UE-based and UE-assisted A-GNSS positioning.

Section 3.1 has identified examples of GNSS Integrity Assistance Data that can be sent from the GCP to the ICE to mitigate the FEs corresponding to Categories 1 and 3 in Table 1. Requirements on the transport layer (Category 2, Table 1) are then examined in Section 3.1.3 and remain FFS on whether existing LPP mechanisms will be sufficient. For UE-based positioning, the UE FEs (Category 2, Table 2) are handled on implementation given the GNSS measurements remain internal to the UE.

The study item discussion about GNSS local environment feared events including multipath, interference and spoofing indicated a need to undertake more work during the work item phase to define what information UEs can detect and report to the LMF and what assistance data can be provided from the LMF to the UE. Hence, there is a potential overlap between UE-based and UE-assisted aspects of integrity that will become more clear after further discussions about local environment feared events.

Observation 5: The UE Feared Events are handled in implementation for the UE-based positioning mode, while detected UE feared events can be reported to the LMF for the UE-assisted positioning mode.

Proposal 7: Agree to prioritize definition of the GNSS Integrity Assistance Data IEs and transfer procedures.

4. Conclusions

Observation 1: Integrity assumed probability parameters can be signalled between the GCP/UE and the ICE. These parameters do not need to be hardcoded in the specifications.

Observation 2: The transfer of the assumed probability parameters can be accomplished between the LMF and the UE using the existing LPP transfer procedures.

Observation 3: The integrity messages in Table 4 can be transferred between the LMF and UE as LPP GNSS Integrity Assistance Data to meet the requirements of UE-Based Integrity.

Observation 4: It is FFS whether the existing mechanisms provided in the transport layers underneath LPP are sufficient to meet the needs of positioning integrity, to mitigate feared events during data transmission.

Observation 5: The UE Feared Events are handled in implementation for the UE-based positioning mode, while detected UE feared events can be reported to the LMF for the UE-assisted positioning mode.

Proposal 1: Agree that for UE-based positioning the assumed probability parameters relating to the GCP can be transferred from the LMF to the UE using the Assistance Data Transfer Procedure.

Proposal 2: Agree that for UE-assisted positioning the assumed probability parameters relating to the UE can be transferred from the UE to the LMF using the Location Data Transfer Procedure.

Proposal 3: Agree to define the GNSS Integrity Assistance Data IEs corresponding to the integrity messages identified in Table 4.

Proposal 4: Agree to define extensions to the LPP GNSS Assistance Data IEs within the existing Assistance Data Transfer Procedure to incorporate new GNSS Integrity Assistance Data IEs.

Proposal 5: Agree to identify the BER and CRC length in the existing LPP data integrity mechanisms and determine if they are suitable to support positioning integrity.

Proposal 6: Agree that the existing LPP procedures can be used for transferring the integrity KPIs (TIR, AL, TTA) and integrity results (PL, Achieved KPIs) between the UE and the LMF.

Proposal 7: Agree to prioritize definition of the GNSS Integrity Assistance Data IEs and transfer procedures.

5. References

[1] RP-210903, “WID: NR Positioning Enhancements”, RAN Plenary, March 2021.

[2] TR 38.857, “3GPP TSG RAN Study on NR Positioning Enhancements; (Release 17)”, V2.0.0.

[3] R2-2100719, “Text Proposals of Definitions Relating to Positioning Integrity Modes”, Nokia, RAN2#113-e.

[4] [Post112-e][618][POS] Finalise integrity text proposals (Swift) – Phase 2 Email Discussion.

[5] Pullen, S., “Augmented GNSS: Fundamentals and Keys to Integrity and Continuity”, ION GNSS 2011, <http://www-leland.stanford.edu/~spullen/ION%20GNSS%202011%20Tutorial%20-%20Aug-GNSS%20final%20(Pullen,%2009-16-11).pdf>.

Appendix A

Summary of network-assisted (UE-Based) and UE-assisted (LMF-Based) positioning integrity mode considerations [2].

Positioning Integrity Mode	Location service type	Source of KPIs*	Source of Integrity results*	Positioning Integrity assistance information**	Specification impact
Network assisted (UE-based): Positioning integrity result is derived by the UE	MO-LR	UE internal implementation	UE internal implementation	From LMF to UE: - Feared events in the GNSS Assistance Data - Feared events in transmitting the data to the UE - GNSS feared events	Procedure to transfer Integrity assistance information from LMF to UE
	MT-LR	From LMF	From UE	From LMF to UE: - Feared events in the GNSS Assistance Data - Feared events in transmitting the data to the UE - GNSS feared events	Procedure to transfer Integrity assistance information and KPIs from LMF to UE Procedure to transfer Integrity results from UE to LMF
UE assisted (LMF-based): Positioning integrity result is derived by the LMF	MO-LR	From UE	From LMF	From GNSS corrections provider (external source) to LMF: - Feared events in the GNSS Assistance Data - Feared events in transmitting the data to the UE - GNSS feared events From UE to LMF: - UE feared events - GNSS feared events	Procedure to transfer Integrity assistance information and KPIs from UE to LMF Procedure to transfer Integrity results from LMF to UE
	MT-LR	LMF implementation	LMF internal implementation	From GNSS corrections provider (external source) to LMF: - Feared events in the GNSS Assistance Data - Feared events in transmitting the data to the UE - GNSS feared events From UE to LMF: - UE feared events - GNSS feared events	Procedure to transfer Integrity assistance information from UE to LMF

NOTE: The table provides a summary of considerations and the final details and specification impacts are FFS in the WI.
*NOTE: Examples of KPIs are the TIR, AL, TTA. Examples of Integrity results are the PL and Integrity Availability.
**NOTE: From LMF to UE does not mean the integrity assistance information is generated by the LMF.