3GPP TSG-RAN WG2 #111-e DRAFT R2-20xxxxx

Electronic Meeting, August 17 - 28, 2020

Agenda Item: 8.11.3.1

Source: Swift Navigation

Title: [AT111-e][607][POS] Integrity definitions, KPIs, and use cases (Swift)

Document for: Discussion, Decision

# 1 Introduction

This document provides templates and summaries for the following email discussion:

* [AT111-e][607][POS] Integrity definitions, KPIs, and use cases (Swift)

Scope: Discuss proposals and attempt to reach consensus on definitions, KPIs, and use cases for positioning integrity.

Intended outcome: Summary with potential agreeable TP

Deadline:  Thursday 2020-08-20 1100 UTC

The intention is to reach consensus on the initial principles of integrity as an input to the remaining Study objectives. Best attempts have been made to accurately capture and represent all submissions that contained proposals relating to one or more of the individual topics. Please let the email Rapporteur know of any accidental oversights as part of the initial review phase.

# 2 Integrity Definitions

The submissions containing integrity definitions are listed below. To assist the review process, they have been grouped according to those which included a broader suite of integrity definitions (including KPIs) (Table 1) and those which only proposed KPI definitions (Table 2).

|  |  |
| --- | --- |
| Tdoc [Reference] | Source |
| [R2-2006541](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006541.zip) [1] | Swift Navigation, Deutsche Telekom, u-blox, Ericsson, Mitsubishi Electric, Intel Corporation, CATT, UIC |
| [R2-2007646](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007646.zip) [2] | ESA |
| [R2-2007937](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007937.zip) [3] | ZTE Corporation, Sanechips |

**Table 1.** Submissions containing general integrity definitions (including KPIs)

|  |  |
| --- | --- |
| Tdoc [Reference] | Source |
| [R2-2006954](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006954.zip) [4] | Ericsson |
| [R2-2007050](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007050.zip) [5] | Spreadtrum Communications |
| [R2-2007102](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007102.zip) [6] | Apple |
| [R2-2007158](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007158.zip) [7] | OPPO |
| [R2-2006564](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006564.zip) [8] | Vivo |
| [R2-2006673](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006673.zip) [9] | CATT |
| [R2-2006754](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006754.zip) [10] | Intel Corporation |
| [R2-2007936](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007936.zip) [11] | ZTE Corporation, Sanechips |
| [R2-2006579](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2006579.zip) [12] | Huawei, HiSilicon |
| [R2-2007073](http://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_111-e/Docs/R2-2007073.zip) [13] | Sumitomo Electric |

**Table 2.** Submissions containing specific KPI definitions

* Please comment on the following:
1. Which of the definitions do you agree should be included in the Study?
2. Which of the definitions do you feel should be modified?

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | 1. We agree with the consensus view for the definitions provided in [1], which are decoupled from specific industry implementations and establish a consistent, principles-based framework for interpreting each term and the relationships between each term within the 3GPP architecture. These definitions are also independent of specific technologies, meaning they can apply to multiple positioning methods and use cases within 3GPP. This flexibility extends to the multitude of use cases and higher accuracy requirements supported by 3GPP (Section 4 of this document), meaning additional integrity factors (e.g. fault-free feared events) are also accommodated in the definitions [1].

We would also support adding the following definition from [2], including the suggested track changes to align the terminology with definitions in [1].**Positioning Integrity Function**Function within the Positioning System that, using the positioning measurements and other data provided to the positioning system, is able to generate the integrity-related data contained within the Positioning Information (e.g. Protection Level) so it can be employed by the positioning system to provide its service to the user application. 1. We believe that the definitions provided in [1] constitute a good baseline, but we acknowledge some definitions could be refined based on the additional views provided in the submissions. In particular, the precise definition of the Protection Level should be FFS.
 |
| Spreadtrum | 1. we agree with Swift Navigation’s view 2. For the definition of protection level, we agree with the definition provided in [2]. Protection level is a value calculated in real time. It needs to be compared with AL to determine whether the system is available. Therefore, when we define the PL, we cannot restrict PL to be less than AL. |
| Huawei, HiSilicon | 1. We mostly agree with the general integrity definitions provided in [1] and [2]. Meanwhile, we think some changes should be made:

1) For the comparison between integrity and accuracy described in [1], the differences provided in [12] should be considered to emphasize that: ***Integrity is a real time decision criterion for using or not using the system in the next period of time while accuracy is a global system characteristic for a nominal system.***2) For positioning integrity function, we suggest to make some changes:**Position Integrity Function**Function within the position/location system that, using the positioning measurements and other data provided by or to the system, is able to generate the position-related data/information (integrity data/information) so it can assist the user to make a real time decision for using or not using the positioning system in the next period of time.We think the definition for several integrity related concepts are missing in [1], e.g. threat model, failure mode.  |
| Sumitomo Electric | 1. We agree with the definition provided in [1] and [2].
 |
| Fraunhofer | In general, we agree with the definitions of terms provided in [1] and [2]. To the TP and comment from Swift, we would like to add that the "positioning system" need to be clarified. The current definition seems to cover the positioning filter which processes measurements to obtain a position/velocity/attitude estimate. However, integrity and accuracy are not fixed static system characteristics, but depends highly on environment the UE finds itself in. Therefore, accuracy and integrity need to be monitored in real time, as Huawei indicated. Hence, the positioning system definition should also be extended to cover selection of one or more RAT dependent or RAT independent technique depending on the real time conditions of the UE.Moreover, we would like to clarify the terms "positioning measurements" and "other data". Positioning measurements can be a UE/TRP measurement defined in LPP or 38.215 and other data could be generated from sources of additional integrity information, such as sensors or information from external system.Furthermore, the accuracy/integrity for different components of the positioning state may need to be specified/calculated separately. |
| ESA | 1. In general we agree with using the definitions provided in [1] as a baseline completing them with the definitions provided in [2] (e.g. Protection Level, Positioning Integrity Function).
2. For the definition of the protection level we propose to include this clarification to the definition provided in [1]:

**Protection Level (PL):** The PL is a bound on the Positioning State Error (the PL upper bounds the positioning state error with a certain probability). The PL ensures that, the probability per unit of time of the true error being greater than the AL and the PL being less than or equal to the AL, for longer than the TTA, are both less than the required TIR. i.e.Probability per unit of time (((True Error > AL) & (PL<=AL)) for longer than TTA) < required TIRNOTE 1: Typically, the PL is output as part of the Positioning Information for each Positioning State (i.e. in real-time).NOTE 2: When the PL bounds the Positioning State Error in the horizontal plane or on the vertical axis then it is called Horizontal Protection Level (HPL) or Vertical Protection Level (VPL) respectively.1. Regarding the proposed definition for the “Positioning Integrity Function”, we agree with it with the following modification:

**Positioning Integrity Function**Function within the Positioning System that, using the positioning measurements and other data, is able to generate the integrity-related data contained within the Positioning Information (e.g. Protection Level) so it can be employed by the positioning system to provide its service to the user application. Besides, as the “Positioining System” is mentioned, we would also need to include its definition:**Positioning System**System responsible for providing the positioning information (position and integrity related data) of one or several location targets.1. We also propose to include the following definitions provided in [2]:
* Authentication: because it plays an important role in the integrity concept (understood as trust that can be placed in the correctness of the Positioning State supplied by the Positioning System) in order to avoid HMI.
* Confidence Interval and Confidence Level: these concepts appear when bounding a statistical parameter like we are doing with the PL and the Positioning State Error.
* Integrity Risk (IR): it is needed to better understand the PL and related to the probability of an Integrity Event (MI and HMI).
1. Just for clarification, we propose to add a note in the definitions of TIR and IR to explain that the TIR is related to the probability of an HMI and the IR is related to the probability of an Integrity Event (MI and HMI).
 |
| ZTE Corporation, Sanechips | We also agree with the consensus view for the integrity definition in [1] and [2].We are fine with the modified Positioning Integrity Function in Swift Navigation’s comment. |
| Nokia | With respect to the definition of the integrity concept, we support the definition of [2].With respect to the definition of the positioning integrity function, we propose the following, derived from the Swift proposal above:“Function within the Positioning System that, using the positioning measurements and other data, is able to generate the integrity-related data so it can be employed by the positioning system to provide its service to the location-based application. Integrity data may relate to location, speed and orientation.”We believe that the applicability and value of using PL based methods should be studied on a case-by-case basis, depending on the integrity methods and use cases. |
| vivo | 1. We agree with the rapporteur’s view;
2. We also think the definition of Protection Level is confusion and it is not aligned with the definition of TTA. The definition of PL[1] is following:

*The PL is a bound on the Positioning State Error that ensures that, the probability per unit of time of the true error being greater than the AL and the PL being less than or equal to the AL, for longer than the TTA, are both less than the required TIR.* In the definition, TTA is not related to annunciate the alert, but indicates how long the position error exists before recovery. To solve the issue，we may decouple the PL with TTA. |
| Apple | Two top-level comments:1. The definitions introduced in [1] could be more 3GPP friendly so that can be more easily converted to normative work. No need to be as same as the ones used in other specs or systems.
2. It is not clear some high level system descriptions needs to be defined, or how relevant to the AS layer work, such as Hazard, Fault, Fault-free, Available, Availability. If not, better to put in Annex.

Some detailed comments below:* **Positioning state** and **positioning state error**. We do not see a need to introduce the “state” concept here. we prefer some language more 3GPP-compatible.
* **Accuracy**. For position accuracy, there are existing 3GPP definition. No need to define new terms.
* Is there a need to define a “**Integrity Risk (IR)**”?
* Is there a need to define “**Error Distribution**” as it seems very relevant to integrity risk, according to [2]
* For **Protection Level**, if it is simply a derivative from integrity risk, we prefer just use the definition in [2].
* the name “Alert”, “Alert Limit”, “Protection Level” are better to be changed as:
	+ Alert -> Integrity Failure Report
	+ Alert Limit -> Integrity Failure Reporting Threshold
	+ Protection Level -> Position Error Threshold
 |

# 3 Integrity KPIs

There was strong consensus in submissions [1, 3, 4, 5, 6, 7, 8, 9, 10, 12] to agree on the four KPIs below (the definitions for which will be determined in Section 2):

* **Target Integrity Risk (TIR)**
* **Alert Limit (AL)**
* **Protection Level (PL)**
* **Time-to-Alert (TTA)**

While there were minor variations on the naming of some terms (e.g. Alarm versus Alert [9, 11]; Error Limit versus Alert Limit [6]; freshness of the positioning [13]), the names presented above represent the majority view. One proposal [4] also introduced the case for adding Continuity and Availability to the stated KPIs.

* Please comment if you agree with the list of four KPIs or think it should be modified:

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | Agree with the four KPIs. |
| Spreadtrum | Agree with the four KPIs |
| Huawei, HiSilicon | We agree with the list of four KPIs, and think the KPIs should be applied to both RAT-dependent and RAT-independent positioning methods. |
| Sumitomo Electric | Same view as Huawei, HiSilicon |
| Fraunhofer | We agree with the four KPIs.  |
| ESA | We agree with the four KPIs but we also think that it is important to clarify that, in this case, these four KPIs are not “independent”. As it can be seen from the definitions they are related to each other. Here is a description of the performance checks that we think will be needed:* **Integrity Performance:** the indicator is the capability of the Protection Level (PL) to bound the Positioning State error and satisfy the integrity required by the user application.
	+ The Positioning State Error is checked against the computed **Protection Level (PL)** and the **Alert Limit (AL) & Target Integrity Risk (TIR)** required by the user application (see PL definition):

Probability per unit of time (((True Error > AL) & (PL<=AL)) for longer than TTA) < required TIR* **Availability Performance:** the indicator is the size of the computed Protection Levels (PL) and how its statistical distribution satisfies the availability required by the user application.
	+ The computed **Protection Level (PL)** is checked against the **Alert Limit (AL) & Availability %** required by the user application**.**
* **Time-to-Alert (TTA) Performance:** the indicator is the elapsed time between when the Positioning State Error exceeds the AL and when the UE annunciates the corresponding Alert and it’s checked against the **Time-to-Alert (TTA)** required by the user application.
 |
| ZTE Corporation, Sanechips | We share the same view with Huawei.  |
| Nokia | The protection level being generally derived from the TIR, we do not understand why these 2 parameters are needed. Additionally, PL based methods may not be adapted to all cases. We believe that PL could be removed from the list.In addition, this KPI list does not reflect all the expectations of the location-based application, it seems necessary to define requirements on missed/false detection, according to the definition given in [2], as well as the maximum number of integrity failure events per time unit. |
| vivo | Agree with the four KPIs. |
| Apple | For integrity failure notification, we agree the two KPIs are needed (FFS name):* Alert Limit
* TTA

For “Target Integrity Risk” and “Protection Level”, they are basically inter-dependent and computed based on each other, so it shall be regarded as one KPI related to “Integrity Risk” |

# 4 Integrity Use Cases

A number of use cases were proposed in submissions [1, 2, 4, 8, 9, 12, 13] with respect to 3GPP.

Please indicate the use cases which you feel should be considered for integrity.

|  |  |
| --- | --- |
| Company | Comments |
| Swift Navigation | We have a preference to prioritise the Automotive (e.g. navigation, V2X, autonomous driving, vulnerable road users) and Rail use cases, which typically have clearly defined safety and integrity requirements specified by the operator. Some submissions presented examples of threshold values for the KPIs, which we agree will be useful in future stages of the SI/WI when determining value ranges for the relevant IEs. However, we think it is important to first agree on the KPI definitions and the priority use cases that require positioning integrity before analysing potential KPI thresholds (noting the TIR, AL and TTA are all implementation-defined).  |
| Spreadtrum | We think that safety and life related use cases, i.e autonomous driving, vulnerable road users, emergency and mission critical related use cases, must be supported. And these use cases should be prioritized. Other use cases can also be supported. But the priority may be lowered.  |
| Huawei, HiSilicon | First, we think the criteria for categorizing the use cases as the ones requiring integrity should be discussed.Second, we believe that “integrity” and “time to alert” are specified for **safety-critical or liability-critical applications**, in terms of insurance of the quality of service. For example,* + Emergency & Mission Critical
	+ Road user charging (RUC)
	+ V2X
	+ eHealth
	+ Location based service
	+ Rail & Maritime
	+ Aerial (e.g. UAVs)
 |
| Sumitomo Electric | We understand that integrity is essential for the automotive and rail use cases. Therefore, we can agree to have the priority for these use cases. However, we believe that the resulting integrity spec. should be use-case agnostic. Instead, 3GPP should clarify applicability of the integrity schemes to be specified for other use cases so that users can clearly understand the risk to use this feature for other use cases. For example, such observation can be captured in TR. |
| Fraunhofer | In addition to the autonomous driving, we think integrity is equally important for autonomous devices requiring precise positioning in factory environment. |
| ESA | We agree with prioritising the different use cases and with having a preference with Automotive. We can also include IIOT as proposed in some contributions. For us the priority order can be: 1. Automotive;
2. Rail; IIOT
3. UAV/drones

We also agree that it is important to first agree on the KPI definitions and the priority use cases that require positioning integrity. The AL, TIR and TTA KPIs are application dependent and the contributions show that different user applications require different values, so the prioritzation in the use cases can help to select the range to cover. |
| ZTE Corporation, Sanechips | We prefer to support the use cases which are mentioned in [1].Although based on our understanding, all use cases should support positioning integrity, we are fine to prioritize the safety and life related use cases. |
| Nokia | We would like to prioritize the IIoT use case, and make a careful selection of those which require an integrity support |
| vivo | We prefer first define use cases below :Trolley,Traffic Monitoring & Control,Road User Charging,UAV,IIOT those are following some routes and easy to define threshold. |
| Apple | We think V2X use cases, especially VRU protection can be prioritized, but have a feeling that the solution framework provided in AS layer can be extended to any use case with different integrity requirements. |

# 5 References

1. R2-2006541 TP for Study on Positioning Integrity and Reliability, Swift Navigation, Deutsche

Telekom, u-blox, Ericsson, Mitsubishi Electric, Intel Corporation, CATT, UIC.

1. R2-2007646 Discussion on use cases and KPIs for position integrity, ESA.
2. R2-2007937 Discussion of the integrity events and integrity failure, ZTE Corporation, Sanechips.
3. R2-2006954 Positioning integrity KPIs and support for RAT dependent use cases, Ericsson
4. R2-2007050 Discussion on positioning integrity KPIs and use cases, Spreadtrum Communications
5. R2-2007102 Discussion on Positioning Integrity, Apple
6. R2-2007158 Discussion on the KPIs of integrity, OPPO
7. R2-2006564 Identify positioning integrity use case and KPIs, Vivo
8. R2-2006673 Discussion on integrity KPIs and use cases, CATT
9. R2-2006754 Consideration on positioning integrity, Intel Corporation
10. R2-2007936 Discussion of the positioning integrity definition, ZTE Corporation, Sanechips
11. R2-2006579 Discussion on positioning integrity KPIs and relevant use cases, Huawei, HiSilicon
12. R2-2007073 Discussion on integrity and reliability for positioning based on an IIoT use case,

Sumitomo Electric