REPORT ON THE PERFORMANCE AND LEVEL OF INTEGRITY FOR SAFETY AND LIABILITY CRITICAL MULTI-APPLICATIONS

-

EUROPEAN GNSS AGENCY
MAY 2015

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

AAIM	Aircraft Autonomous Integrity Monitoring
ABAS	Aircraft Based Augmentation Systems
ADAS	Advanced Driver Assistance System
AL	Alarm Limit
CR	Continuity Risk
CS	Commercial Service
DR	Dead-Reckoning
EC	European Commission
EDAS	EGNOS Data Access Service
EGNOS	European Geostationary Navigation Overlay System
EGNSS	European Global Navigation Satellite System
erfc	Complementary error function
ESA	European Space Agency
ETSI	European Telecommunications Standards Institute
FD	Fault Detection
FDE	Fault Detection and Exclusion
FTA	Fault Tree Analysis
GBAS	Ground Based Augmentation System
GIS	Geographic Information System
GIVE	Grid Ionospheric Vertical Error
GLONASS	Global'naja Navigacionnaja Sputnikovaja Sistema – Russian GLObal NAvigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSA	European GNSS Agency
HAL	Horizontal Alarm Limit
HMT	Hazardous Material Tracking
IBPL	Isotropy-Based Protection Level
ICT	Information and Communications Technologies
IGNSSRX	Integrity GNSS Receiver
IMU	Inertial Measurement Unit
INLU	Integrity of Navigation for Land Users
IR	Integrity Risk
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems

LAAS	Local Area Augmentation System
LBS	Location Based Service
LMSCM	Land Mobile Satellite Channel Model
MM	Map-Matching
NLOS	Non-Line-Of-Sight
OS	Open Service
PAYD	Pay-As-You-Drive
PCA	Payment-Critical Applications
PL	Protection Level
PPUI	Pay-Per-Use-Insurance
PVT	Position, Velocity, Time
RAIM	Receiver Autonomous Integrity Monitoring
RCA	Regulatory-Critical Applications
RNP	Required Navigation Performance
RUC	Road User Charging
SARPS	Standards And Recommended Practices
SBAS	Satellite-Based Augmentation Systems
SCA	Safety-Critical Applications
SCN	Satellite Communication and Navigation
SIL	Safety Integrity Level
SIS	Signal-In-Space
TC-SES	Technical Committee on Satellite Earth Stations and Systems
TTA	Time To Alarm
TTFF	Time To First Fix
UDRE	User Differential Range Error
WAAS	Wide Area Augmentation System
WAD	Wide-Area Differential
WG	Working Group
WLS	Weighted Least Squares

1. INTRODUCTION

The scope of this document is to discuss the guidelines that can bring to the definition of the minimum performance requirements in terms of position integrity for several classes of positioning-dependent applications in the road/ITS domain.

It is organized as follows: the following subsections of this Chapter are devoted to explain the rationale of the applied methodology (Section 1.1) and to give the initial and basic set of formal definitions (Section 1.2).

Chapter 2 contains the executive summary of this document.

Chapter 3 is a lightweight and practical review of the general positioning integrity framework, as developed so far in the civil aviation context. This represents the basis for the development of a similar framework for road/ITS users, provided that all the major differences of the two contexts are appropriately taken into account.

Chapter 4 briefly reviews the major classes of applications and their needs with respect to the performance features of the integrity framework. It re-uses the classification of applications already introduced and discussed in [RD01].

Chapter 5, leveraging on the analysis carried out in the two previous chapters, draws some guidelines towards an adequate and comprehensive definition of the integrity framework for road/ITS applications, by highlighting and discussing the issues recognized but still open which are peculiar to a terrestrial domain.

Finally, Chapter 6 concludes the analysis with a summary of the guidelines and an indication of the major gaps to be filled with priority, to timely arrive to the definition of integrity-enabled positioning services for road/ITS applications.

1.1. METHODOLOGY

The analysis conducted in document is driven by three major pillars:

- *Multi-technology approach,* meaning that the multi-faceted localization task for road users has been considered as much generic as possible, taking into account that a vehicular positioning module is likely to exploit several sources of localization information simultaneously, among which GNSS is the major one but not the sole.
- *Practicality,* meaning that most technicalities have been voluntarily avoided, in order to target the discussion to a systematic view and provide a usable working document on the path toward the definition of the minimum performance integrity requirements for road/ITS users.
- *Reference to the most authoritative sources in the international panorama;* in such a relatively young but complex context, there is still a lack of consolidated approaches to face the various aspects of the overall problem. For this reason we scouted the most authoritative sources in the international panorama which have addressed aspects of localization integrity in terrestrial/vehicular applications, trying to critically review and possibly harmonize their approaches and views.

The aim of our work is on the one hand to give a comprehensive idea of the complexity of the problem, on the other hand to draw a usable pathway toward the thorough definition of the integrity framework.

1.2. DEFINITIONS

The initial and basic set of general definitions of interest for the whole document is reported in this section.

The wide spectrum of technical features broadly associated to the localization task in a road/ITS context needs a new and broader concept for location systems, taking into account

hybrid solutions in which GNSS technologies are complemented with other sensor technologies to improve robustness and the performance [RD02]. In order to acknowledge this need and to adopt a shared language, we refer to the functional reference architecture and set of definitions proposed within the European Telecommunications Standards Institute (ETSI) by the Satellite Communication and Navigation (SCN) Working Group of the Technical Committee on Satellite Earth Stations and Systems (TC-SES), in the context of the definition of a common set of standards for GNSS-based Location systems [RD02]. The most detailed level of the functional architecture identified in [RD02] and used as a reference throughout this document is reported in Figure 1-1.

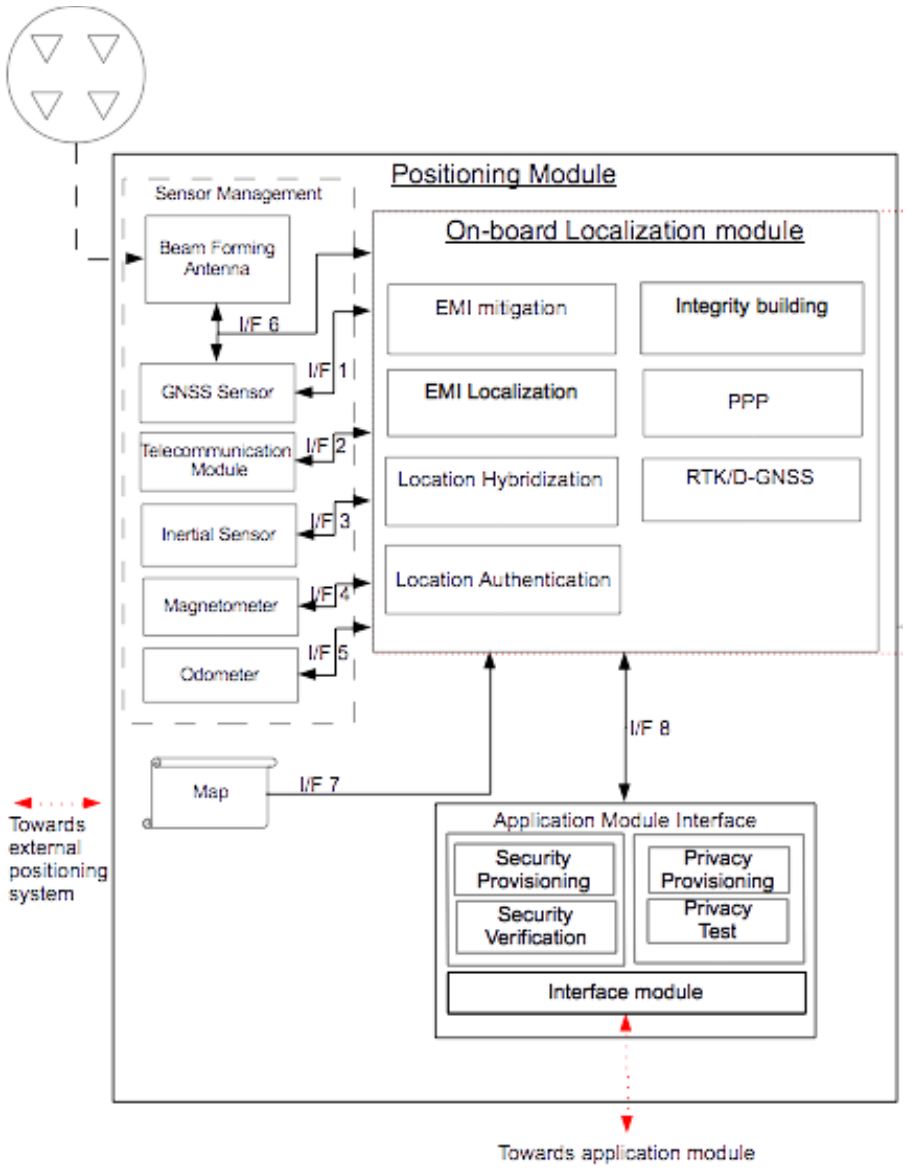

Figure 1-1: Reference architecture of a location system (adapted from [RD02]): the GNSS receiver is a component (functional block) of the positioning module, the fundamental component of a location system.

The major definitions applicable to this architecture are reported hereafter in alphabetical order [RD02]:

Localization information sensors	Localization information sensors include the *GNSS sensor* and *additional sensors.* The *GNSS sensor* is a mandatory component of the location system architecture. *Additional sensors* are optional components of the location system architecture and might be on-board the positioning module.
Localization module	The Localization Module is the entity in charge of transforming the measurements needed to determine the position of the location target. The Localization Module is a mandatory component of the location system architecture.
Location-based application	An application that is able to deliver a *location-based service* to one or more users.
Location-related data	A set of data associated with a given *location target*, containing one or more of the following time-tagged information elements: target position, target motion indicators (velocity and acceleration), and Quality of service indicators (estimates of the position accuracy, reliability or authenticity). This is the main output of a *Location system.*
Location system	The system responsible for providing to a *location based application* the *Location-related data* of one or more location targets.
Location target	The Location Target consists of a physical object (including a person, vehicle, interference source etc.) with which sensors or applications interact to provide a location.
Positioning module	The logical entity inside a *Location system* responsible for providing the *location target's location-related data* to the *application module*. It is composed of a GNSS receiver and possibly additional sensors.

It is worth noticing that the architectural view expressed in [RD02] is compliant, apart from some nomenclature choices, with the CEN/CENELEC draft document [RD03].

2. EXECUTIVE SUMMARY

The integrity of a certain estimate refers to the confidence one can give to correctness of the estimate with respect to the true (but unknown) quantity. This to say, the probability that the unavoidable estimation error averts the estimate from the true value by more than a certain level. This confidence is expressed in the language of GNSS positioning with the concepts of Integrity Risk (the probability) and Protection Level (the error level) (see Section 3.1).

A well established and trustable framework to set integrity risks and compute protection levels is mandatory for any applications wants to use an estimated position as an input for operations involving safety of life or economical transactions or any kind of law enforcement. Safety of life is evidently the case of civil aviation applications, for which a very challenging integrity framework, comprising also concepts of accuracy, availability and continuity (i.e., the so-called Required Navigation Performance), has been developed in the last two decades and still deserves refinements (see Sections 3.2, 3.3). Payment-critical and regulatory-critical applications are far more common and close-to-market in the road/ITS domain (see Chapter 4); however—although they mandatorily need to pose a level of trust on the position estimates they may use—the positioning integrity framework for them is far from being mature (see Section 5.1).

This gap is both technological and regulatory. From a technological point of view, there are many aspects that prevent the direct exploitation of the aeronautical integrity in a non-aeronautical context (see Section 5.2): the application requirements, and the way they must be dealt with, are different; the possible causes of error and their associated probabilities are different mainly because of the different environment; the sources of localization information can be far more heterogeneous and variously combined in a positioning module for road/ITS applications; the typical algorithms suitable to assess integrity in the aeronautical domain are consequently unsuitable in other domains. Such a scenario poses a strong demand for a more structured and complete analysis of the entire framework.

A reasonable and promising approach towards the standardization of integrity performance requirements can be identified including the following steps (Chapter 6):

1. Identification of classes of road user applications requiring GNSS and their specific needs in terms of required navigation performance;
2. Definition of realistic scenarios;
3. Implementation of an appropriate simulation environment;
4. Identification of suitable integrity algorithms;
5. Assessment of the integrity performance and validation of the models.

This is basically the approach proposed and followed by what is, at the time of writing, the most up-to-date and promising work focused on the standardization of integrity performance requirements for road users, which disclosed public results.

The aim of the present work is on the one hand to give a comprehensive idea of the complexity of the problem, on the other hand to draw a usable pathway toward the thorough definition of the integrity framework for road/ITS applications.

3. POSITIONING INTEGRITY

The quality of the positioning information is normally demonstrated by four parameters, i.e., accuracy, integrity, continuity and availability, which are usually referred to as Required Navigation Performance (RNP) parameters [RD04][RD05].

"**Positioning integrity**" (or simply "integrity") can be defined as a general performance feature referring to the level of trust a user can have in the value of a given position or velocity as provided by a location system [RD03]. Although integrity is a complex framework, its ultimate goal is to associate a confidence interval to any position estimate produced by the location system, provided that this confidence interval can be computed, in the hypothesis that the operational conditions are properly monitored, modelled or estimated. The confidence interval and the probability inherently associated to it are typically mapped to the concepts of "protection level" and "integrity risk".

Although the literature about integrity, in the GNSS field and focused to civil aviation, is almost exterminated [RD05][RD06][RD07][RD08][RD09][RD10][RD11][RD12], the goal of this section is to delineate the *fundamental aspects* of the integrity framework, aiming at a general and high-level presentation of the involved elements and concepts which keeps the mathematical details as limited as possible.

Pursuing a goal of clarity, we follow a "three layers" description (Figure 3-1):

1. *Layer 1*: Integrity from the point of view of the *estimation theory* (to answer the questions: "how statistical confidence is defined?", "which are the other involved quantities and how are they quantitatively defined?");
2. *Layer 2*: Integrity under a *system-level* point of view (to answer the questions: "which is the input information needed to the integrity framework and which are the information sources?");
3. *Layer 3*: Integrity under an *operative* point of view (to answer the question: "which is the algorithm to follow to assess the integrity of a location system?").

The following subsections (respectively, Sections 3.1, 3.2, 3.3) are devoted to discuss the integrity framework under the three different points of view, while Section 5.2 highlight the major open issues related to the application of this framework in road/ITS domain.

Figure 3-1: Points of view of the "three-layer" description of the integrity framework.

3.1. ESTIMATION THEORY: THE "LEVEL OF TRUST" OF AN ESTIMATED QUANTITY

In this subsection we briefly redraw the formal definition of confidence interval from the point of view of pure estimation theory. Furthermore, we introduce other formal concepts (e.g., integrity and continuity risks, alarm limit) typically associated to the analysis of integrity of a certain system. This view helps to establish a common understanding of the basic concepts widely used in the rest of the document.

It is worth noticing that the topic discussed in this section has *general scope*, meaning that it is not strictly tailored to a positioning problem nor to a GNSS field.

Confidence interval of an estimate

Let's suppose to measure a quantity x that we can model as a random variable X like:

$$X = x_t + E_x \qquad \textbf{(3-1)}$$

where x_v is the true value of the estimated quantity (e.g., in a problem of position estimate, one of the three coordinates of the target position) and E_x is the error associated to the measurement (or estimate), that is modelled as a random variable. Therefore, we can state that the probability of the event $|E_x| > C_x$ (error exceeding a given threshold) is

$$\mathcal{P}_{ex} = \text{Prob}\{|E_x| > C_x\} \qquad \textbf{(3-2)}$$

If the probability density function (pdf) of E_x is known, $f_{E_x}(e)$, and it is an even function, the probability $\mathcal{P}_{ex}$ can be expressed as

$$\mathcal{P}_{ex} = 2\int_{C_x}^{+\infty} f_{E_x}(e)\,\text{d}e \qquad \textbf{(3-3)}$$

In case of a Gaussian pdf with zero-mean value and variance σ_x^2, equation (3-3) can be computed in closed form through the so called "complementary error function" (erfc) as

$$\mathcal{P}_{ex} = \text{erfc}\left[\frac{C_x}{\sqrt{2\sigma_x^2}}\right] \qquad \textbf{(3-4)}$$

which can be resolved for the threshold C_x in the form

$$C_x = \sqrt{2\sigma_x^2}\cdot\text{erfc}^{-1}\left[\mathcal{P}_{ex}\right] = k_{\mathcal{P}}\cdot\sigma_x \qquad \textbf{(3-5)}$$

where $k_{\mathcal{P}} = \sqrt{2}\cdot\text{erfc}^{-1}\left[\mathcal{P}_{ex}\right]$ depends on the probability that $|E_x| > C_x$ and on the "Gaussianity" of E_x.

Equations (3-2)-(3-5) express the fact that the absolute value of the estimation error E_x exceeds the threshold C_x at the probability $\mathcal{P}_{ex}$, i.e., *the absolute value of the error* E_x *is bounded to within the* ***confidence interval*** C_x *at the* ***probability*** $(1-\mathcal{P}_{ex})$. This means that C_x is the confidence interval for the estimate X at the probability $(1-\mathcal{P}_{ex})$.

Integrity risk and Protection Level

The confidence interval says that the unknown parameter x_t is within the interval $X - k_{\mathcal{P}} \cdot \sigma_x \le x_t \le X + k_{\mathcal{P}} \cdot \sigma_x$ with a confidence of $(1-\mathcal{P}_{ex})$, where X is the estimate; $k_{\mathcal{P}}$ depends on the complementary confidence $\mathcal{P}_{ex}$; σ_x is the error standard deviation.

In the language of the integrity, the concept of *risk* (or hazard, or *loss of integrity*) is used, which is associated to the probability $\mathcal{P}_{ex}$ of the event that the absolute value of the error exceeds $C_x = k_{\mathcal{P}} \cdot \sigma_x$. Specifically, the **integrity risk** (IR, in formula $\mathcal{R}_I$), or **loss of integrity** is defined as the *probability that, at any moment in a certain reference interval T_{ref}, the error exceeds the confidence interval C_x.*

Under this perspective, the *limit of the confidence interval* C_x is called **Protection Level** (**PL**). In other words, the PL is the radius of an interval (of a circle in a plane), with its centre being at the true position, which describes the region which is *assured* to contain the estimated quantity. It is the region for which the confidence requirement $(1-\mathcal{P}_{ex})$ can be met.

Figure 3-2 graphically shows the concepts discussed so far: given the pdf of the error E_x associated to the estimate of the quantity x_t, the complementary confidence $\mathcal{P}_{ex}$ expresses the probability at which the protection level is required and depends from the integrity risk through (3-4). The error E_x gives a "misleading information" when it exceeds the PL (this happens with probability $\mathcal{P}_{ex}$, of course).

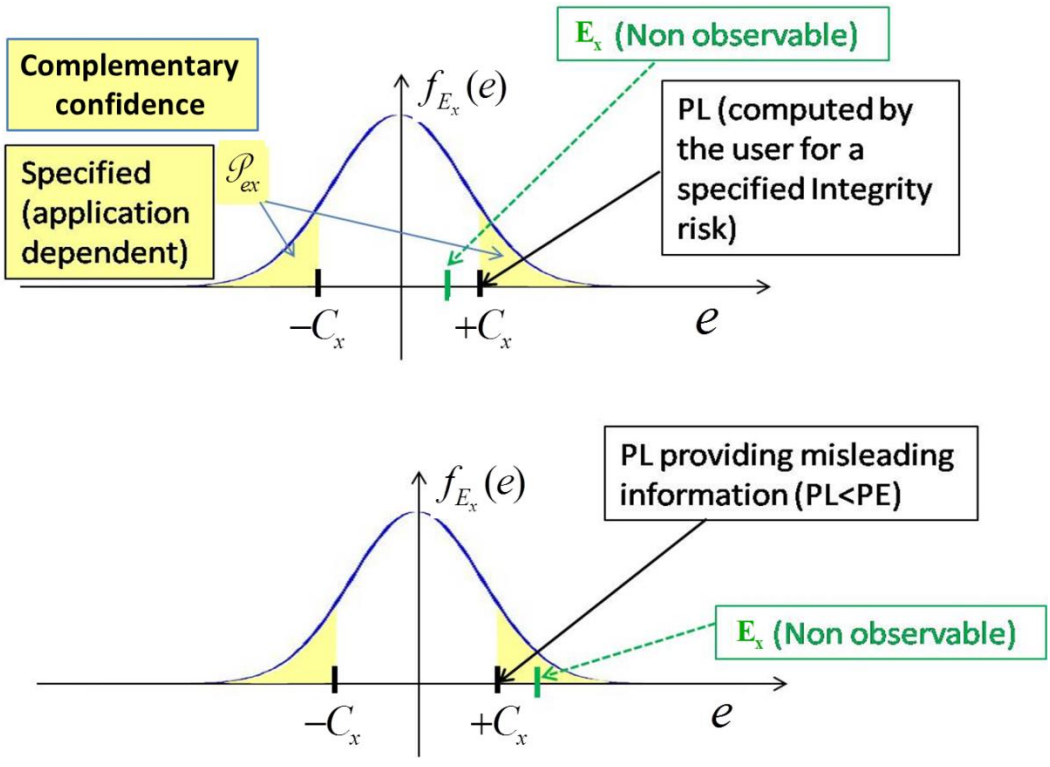

Figure 3-2: Concepts of confidence interval, complementary confidence probability and misleading information.

It is important to remark that the concept of PL introduced in this section is valid under the "zero-mean Gaussian hypothesis" introduced in (3-4): this is the so-called *nominal condition*, or *fault-free* condition. If this hypothesis is not verified (*non-nominal conditions*), then either the error has non-zero mean (so, it is a systematic *bias*) or its pdf is not Gaussian (or both). While the latter case can be handled with different modelling the non-nominal pdf, the former leads to a *faulty* condition which must be detected by the system.

In nominal conditions, indicating with N_{dec} the number of *independent* decisions (estimates or measurements of X) along the reference interval T_{ref} , the relationship between $\mathcal{R}_I$ and the confidence $(1-\mathcal{P}_{ex})$ can be approximated as

$$\mathcal{R}_I = \mathcal{P}_{ex} \cdot N_{dec} \qquad \textbf{(3-6)}$$

Therefore, $\mathcal{R}_I$ is the number of possibly erroneous estimates (risks, or hazards) in the reference interval (where "erroneous" means "out-of-bound") and is also known as *hazard rate*.

Integrity assessments

A set of other quantities are used in the integrity framework to assess the global "level of trust" of the current estimate. They are introduced hereafter.

An estimate (estimated quantity) X is said to be **integer** if its *error* E_x *does not exceed the PL* ($E_x < PL$). Since E_x is not observable (because x_t is unknown), the integrity of X is guaranteed at the probability $(1-\mathcal{P}_{ex})$.

Similar to the PL, the **Alarm Limit** (**AL**) is the *radius of an interval (of a circle in a plane), with its centre being at the true position, which describes the region which is* required *to contain the indicated position with a probability* $(1-\mathcal{P}_{ex})$. Theoretically, if the error exceeds the AL, then an *alarm* should be raised, because an "out-of-bound" error is currently measured. This leads to the concepts of:

- **False alarm probability**, $\mathcal{P}_{fa}$, which is the probability that an alarm is raised in the absence of system failures (fault-free conditions);
- **Miss-detection probability,** $\mathcal{P}_{md}$, which is the joint probability that the position error exceeds the AL and it remains undetected. Of course $\mathcal{P}_{md}$ results from the choice of the detection threshold.

The presence of a systematic error (*bias*) that alters the nominal operational conditions can exemplified as in Figure 3-3. In nominal conditions (bias-free, or *fault-free*), the estimation error has zero mean (the distribution of the absolute value is exemplified in the figure), then the probability that $E_x > AL$ can represent the probability of erroneously detecting a bias in the measurement (*false alarm probability*, $\mathcal{P}_{fa}$).

On the contrary, in case of non-nominal conditions (biased, or *faulty*), the event $E_x \le AL$ can represent the probability of missing the detection of a bias in the measurement (*miss-detection probability*, $\mathcal{P}_{md}$).

Notice that, for integrity-driven systems, the probability of faulty conditions should be kept as low as possible.

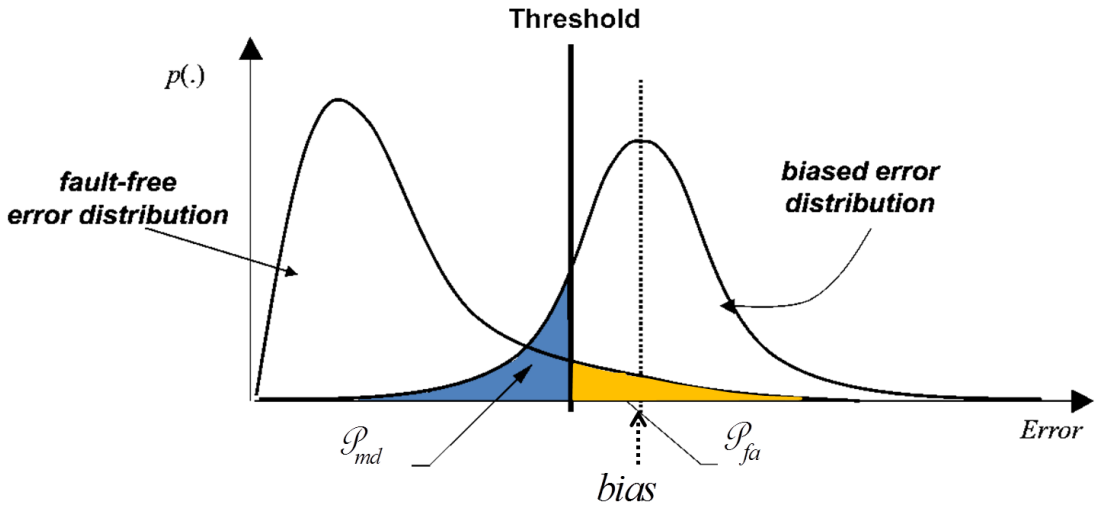

Figure 3-3: Nominal and non-nominal error density functions and associated miss-detection (in blue) and false alarm (in orange) probabilities.

Nonetheless, since the error E_x is not observable, the PL is compared against the AL to detect possible non-mitigated biases:

- In case the PL exceeds the AL ($PL > AL$), the integrity of the estimate cannot be assessed, then the integer estimate is said to be **not Available;**
    - In case the PL exceeds the AL but the error E_x is less than the AL, then a "**false alarm**" is generated ($PL > AL > E_x$); also in this case a "misleading information" is generated;
- Otherwise ($PL \leq AL$), the integrity of the estimate is said to be **Available.**

In the context of integrity, the concept of **availability** (which must be intended as "*availability of integrity*") expresses a *measure of the probability that the estimation system is able to produce an integer measurement (integer estimated quantity)* X *at any moment* at which the application needs to start an integrity-dependent operation. Availability of integrity means that the system is performing with the required level of accuracy.

The **Time To Alarm** (TTA) is the *maximum allowable time elapsed from the onset of the estimation system being out of tolerance until the equipment enunciates the alarm*.

The above integrity mechanisms protect the user against misleading information, caused by loss-of-integrity ($E_x > PL$) or by false alarms ($PL > AL > E_x$). The set of all the possible relationships among the estimation error, the PL and the AL is typically and quite clearly represented by a drawing like in Figure 3-4, where a two-dimensional error domain is assumed.

Finally, **continuity** is the ability of the estimation system to *perform its function without interruption during the intended period of operation or reference interval*. The **Continuity Risk** (CR, in formula $\mathcal{C}_I$) is defined as the probability that, at any moment and over a specified time interval, the integrity of the estimation system is compromised and an alarm is raised. Consequently, the CR is related with the $\mathcal{P}_{fa}$ defined above [RD12].

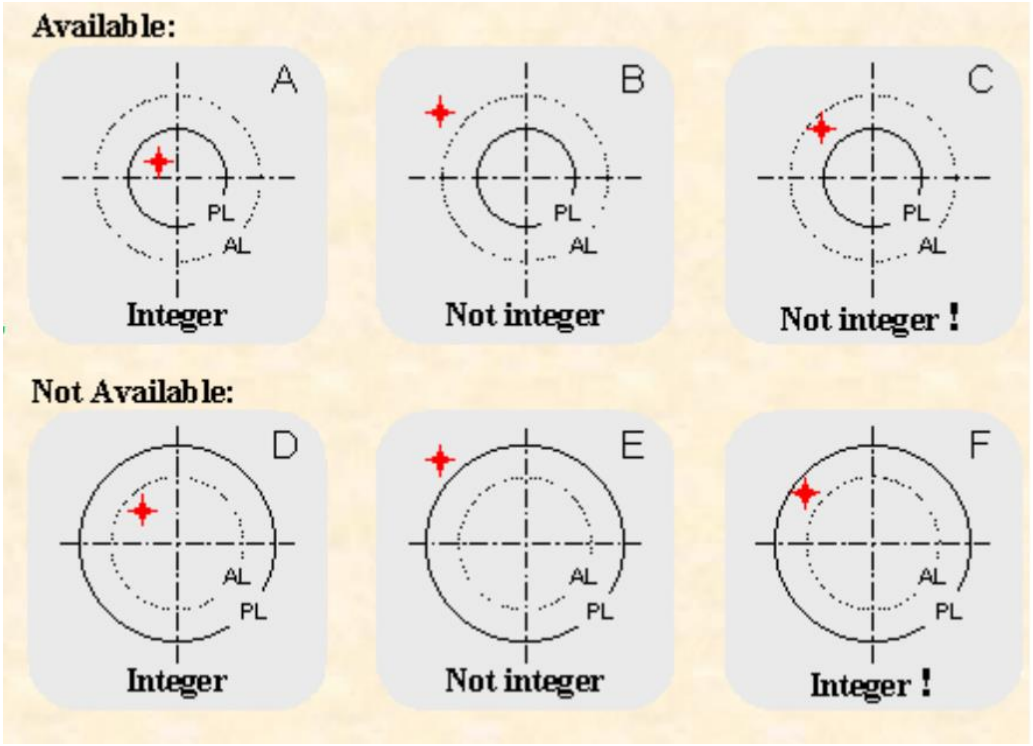

Figure 3-4: Possible cases of integer/non-integer estimate and availability/unavailability of integrity, defined as a function of the relationships among the estimation error (the red cross), the PL and the AL.

3.2. SYSTEM-LEVEL: INPUTS AND OUTPUT OF THE INTEGRITY FRAMEWORK

In this section we address the description of the integrity associated to a certain *location* system from a system-level point of view. In this sense, the generic "estimate" and "estimation error" used in the previous section become "position estimate" and "position error" hereafter. Still, no specific mention to the GNSS system and signal is necessary.

From a system-level point of view, there are three entities concurring to define the integrity of a certain location system (see Figure 3-5):

A. Application Requirements: the requirements set by the application;

B. Requirements given at localization level: the integrity requirements set upon each localization information source;

C. Positioning Module: the signal processing and operative conditions necessary to compute the position (and velocity) solution from certain sources of localization information.

All the three entities play a major role in determining the "**integrity level**" of the provided service (entity '**D**' in Figure 3-5). For this reason, they must be understood and characterized in deep when defining an integrity framework. This is what has been done since the past fifteen years in the civil aviation field; and what is not consolidated yet in other domains.

Once the inputs from entities B and C in Figure 3-5 are determined, the system integrity (entity **D**) can be assessed for the application at hand. From the previous discussion, it should be clear that this is done in terms of:

1) Protection level (level of integrity);

2) Availability of the integer location service.

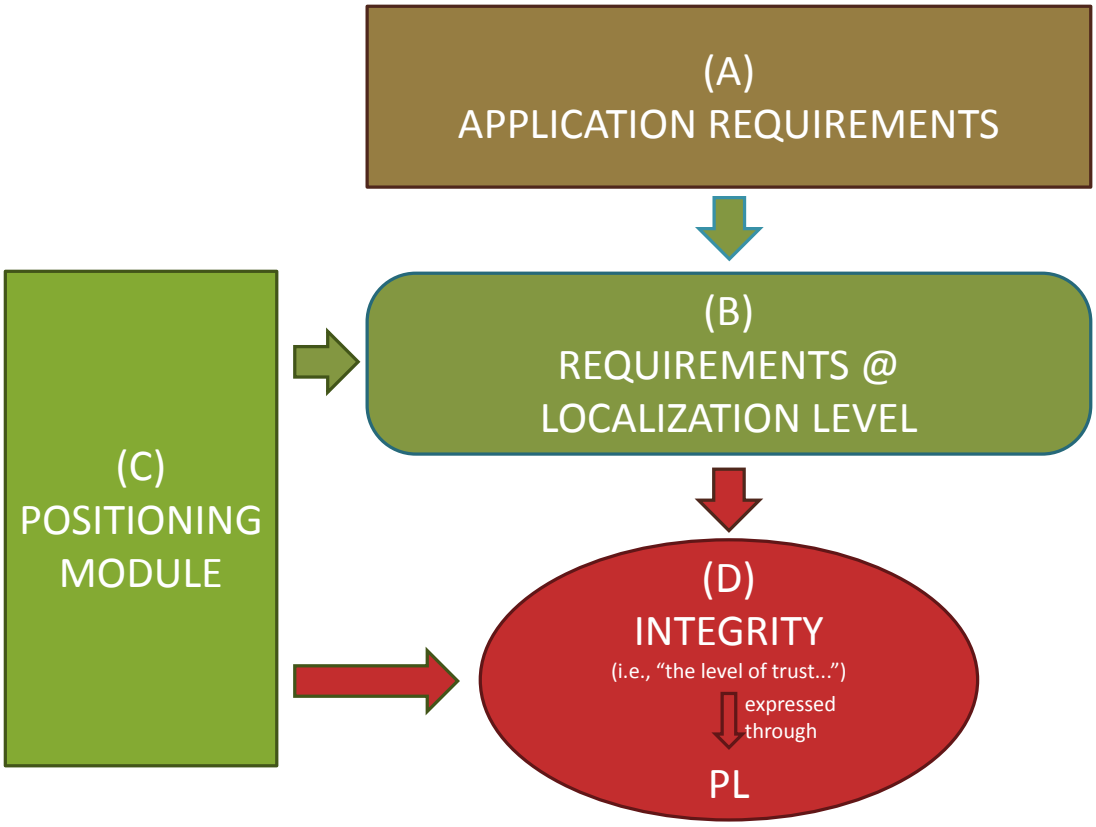

Figure 3-5: Integrity from a system-level point of view.

We can affirm that ***the location system at hand is integer within*** PL ***meters at*** $(1-\mathcal{R}_I)\%$, where:

- $\mathcal{R}_I$ is the integrity risk required by the application,
- PL is the protection level, to be computed for the system and geometry at hand;

Service availability, i.e., the probability that the location system is usable for that particular application at a particular time, requires that:

- There exists a localization solution with an associated protection level;
- The protection level is small enough to suit the requirements (AL) of the particular application, i.e.:
  - If $PL \leq AL$ ➔ ***the integer system is Available*** for the operation;
  - If $PL > AL$ ➔ ***the integer system is Not Available*** for the operation.

In the following subsections (respectively, Section 3.2.1 and 3.2.3) the issues associated to the characterization of entities A, B and C are revised.

3.2.1. (A) DETERMINATION OF THE APPLICATION REQUIREMENTS

Applications and services exploiting positioning information range from the aviation field, to maritime, rail, road and ITS, location-based commercial services, agriculture, Earth

observation and surveying, timing and synchronization [RD13]. Some of them express integrity requirements.

Application requirements may be given at two levels [RD14]:

1) **Requirements at user-service level.** It is the highest level, directly related with the performance of the service provided by the specific application;
2) **Requirements at operation level.** They map the probabilistic requirements expressed at the user-service level to probabilistic requirements associated to each operation that builds the service within the location system.

The two levels are interrelated each other and also interrelated with the requirements at localization level (entity 'B'), meaning that specifying the requirements in one level already sets or bound them in the other two. The first level represents the final performance of the system directly seen by the user and the service provider. The requirements at localization level are needed to build the integrity algorithm (i.e., the algorithm inside the "Integrity building" block in Figure 1-1), while the requirements at operation level are the intermediate step between the localization and the service levels.

A very instructive example of such an approach is reported in [RD14].

3.2.1.1. Requirements at user-service level

Requirements at the user-service level may be extremely heterogeneous, depending on the applications. Furthermore, they are typically not directly expressed in terms of integrity requirements for the location system.

For example, safety requirements in the rail domain are expressed in terms of Safety Integrity Level (SIL)-*n* level, where *n* is an integer ranging from 1 to 4, with SIL-4 being the most dependable and SIL-1 the least.

On the other hands, integrity requirements for the electronic fee collection systems are expected to be driven by charging performance requirements [RD15].

In this context, the first step to determine the requirements to be used in building the integrity function inside a positioning module is to quantitatively and univocally set the needs expressed by the user-service towards the location system. The example reported in [RD14] should clarify this approach.

3.2.1.2. Requirements at operation level

The location-based operations necessary to build the service offered by the application may perform a certain usage of the location information generated by the location system (for example, to compute the time spent by a user within a certain area).

This means that the user-service level requirements must be allocated to the elements of the technological chain that enables the service, for example defining the duration of each operation, the number of necessary location estimates for each operation and the maximum probabilities of failure admitted for the operation.

3.2.2. (B) REQUIREMENTS AT LOCALIZATION LEVEL

The requirements at localization level are the integrity risk, continuity risk and alarm limit imposed to each localization information source.

From the operational needs delineated above, integrity-specific indicators must be derived. The typical indicators (i.e., requirements) are the integrity risk, $\mathcal{R}_I$, and the *continuity risk,* $\mathcal{C}_I$, both introduced and defined in Section 3.1.

The typical approach used to deal with $\mathcal{R}_I$ and $\mathcal{C}_I$ in the civil aviation field is based on the co-called "Fault Tree Analysis" (FTA) [RD16]. FTA is a technique for the failure analysis which focuses on one specified undesired event and which provides a method for determining conditions and factors that can cause the failure. The undesired event represents the top event in a fault tree diagram, where the contributors to the undesired event (intermediate

events, down to the initiating events) are identified and organized in a logical manner and represented pictorially. In particular the fault tree shows the inter-relationships of the basic events that lead to the undesired event. Notice that the identified faults are not generally exhaustive, as they cover only the most credible faults as assessed by the analyst.

In short, the main steps to draw a fault tree are [RD17]:

- Identify the top event;
- Identify the intermediate and initiating events;
- Assign the probabilities (i.e., the ***risks***) to the initiating events.

Once the fault tree is drawn, the computation of the probability of occurrence (i.e., of the ***risk***) of the top event (and of any internal event corresponding to a logical sub-system) can be performed on the basis of the probabilities assigned to the initiating events, which represent failure events of the basic components.

An example of FTA is shown in Figure 3-6, adapted from [RD18], referred to a CAT I Local Area Augmentation System (LAAS).

FTA is also a way to sub-allocate a user-service level integrity *requirement* (expressed as the risk associated to the top event) to each basic system component (expressed as initiating events).

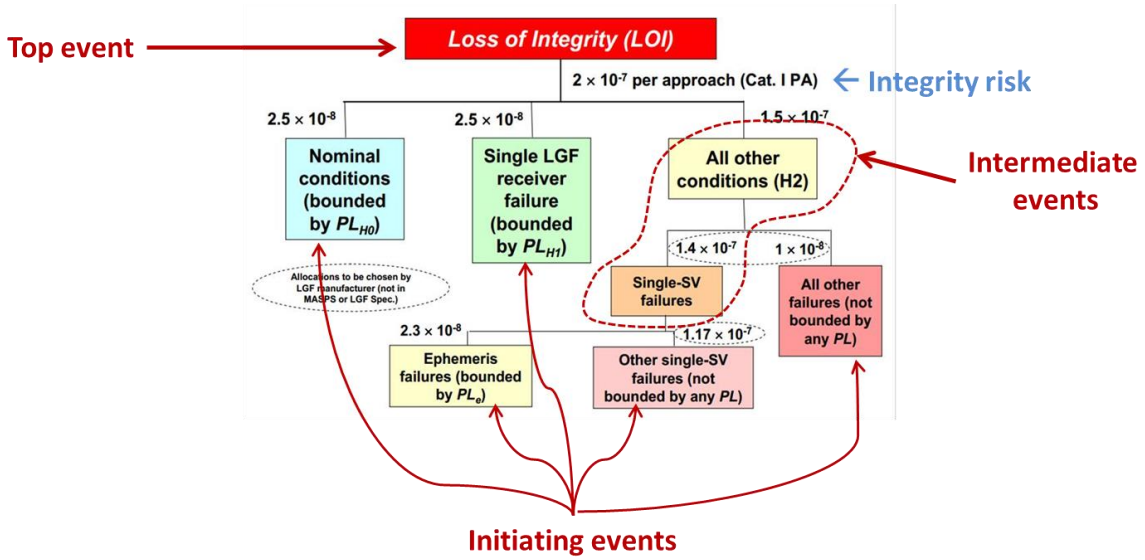

Figure 3-6: Integrity fault tree for CAT I LAAS, adapted from [RD18]. It shows the allocation of the CAT I total integrity risk requirement of 2×10^{-7} per approach to the various possible causes of integrity loss.

Typically, $\mathcal{R}_I$ and $\mathcal{C}_I$ (for any event considered) are given "per operation", i.e., along the whole duration of a certain event or operation (for example, "per CAT I approach" in Figure 3-6). In this way, the per-operation $\mathcal{R}_I$ is decomposed in the probability $\mathcal{P}_{ex}$ associated to each *independent* position estimate *in case of nominal conditions* and in the miss-detection probability $\mathcal{P}_{md}$ associated to each *independent* position estimate *in case of non-nominal conditions*.

Thus, the problem of the temporal correlation among measurements is important. For example, for the GNSS signals it is known that atmospheric errors make measurements strongly correlated. Reference [RD14] affirms that "pseudorange errors in *non-SBAS single frequency* receivers are driven by the ionospheric one, resulting in a correlation time close to *30 minutes*. On the other hand, dual-frequency receivers present an error correlation of a few seconds, mainly driven by the thermal noise and multipath. The dominant error source in

SBAS-enabled single frequency receivers depends on the GNSS signal robustness against noise and multipath [for which] a correlation time *around 1 second* has been obtained during simulations." Therefore dual-frequency receivers and SBAS-enabled ones are more likely to provide several independent position estimations in a reference interval, which improves per-operation performance.

3.2.3. (C) ROLE OF THE POSITIONING MODULE

The "positioning module" entity in Figure 3-5 encompasses several aspects. Their characterization under an integrity viewpoint might require to further distinguish the block C into two additional sub-entities (see Figure 3-7 and Figure 1-1):

- **C/1: Localization information sources**, which produce the observables or measurements to compute the next localization estimate;
- **C/2: Localization module**, which represents Localization engine to compute the localization solution.

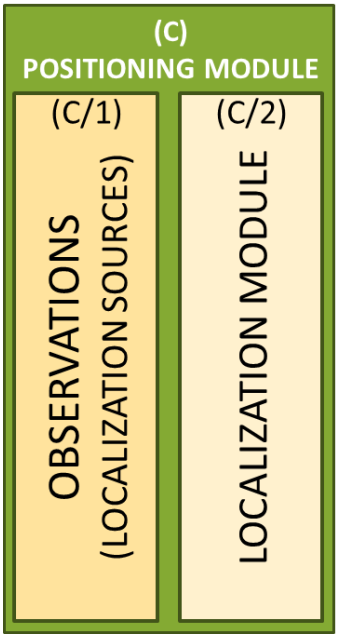

Figure 3-7: Logical components of the positioning module.

The characterization of the localization information sources in terms of error statistics (or statistics of the uncertainties in the observations) is fundamental in order to establish the confidence of the estimated localization solution (Section 3.1).

Error statistics (usually expressed in terms of **biases** and **variances**, the so-called σ's) are typically characterized (with a lot of effort) in the domain of the observations (e.g., the range domain in GNSSs), then they are mapped to the position domain, where the localization confidence is determined on the basis of the localization error standard deviation σ_x (Section 3.1).[1]

[1] The integrity assessment procedure drawn here is expressed in the *position domain*, as it is common for GPS used in the aviation field. However, an similar characterization in the *range domain* could be pursued [RD19].

3.2.3.1. C/1: Statistical characterization of the errors in the observation domain

The **statistical characterization** of all the error sources that impact on the observations (e.g., on the pseudoranges, for a GNSS-only positioning module) is in general a difficult task, as it requires to identify all the realistic error events, assign them a probability of occurrence, and discriminate between nominal and non-nominal conditions. However, it has a direct impact on the system performance under the integrity point of view.

Beyond the adoption of the correct statistical model, also its **validation** is critical as well: relating experimental error data to theoretical integrity bounds remains a key challenge for certifying navigation systems, in particular those with demanding integrity risks [RD20].

Being GNSS the primary source of localization information with associated integrity, this exercise is consolidated in the GNSS field (tailored for civil aviation, as usual). The approach is reviewed in the following example.

Example: statistical characterization of the pseudorange errors

The errors affecting the measured pseudoranges in a GNSS receiver depend on the following factors [RD06][RD07][RD08]:

- C/1.a Space segment;
- C/1.b Propagation in atmosphere;
- C/1.c Local propagation effects near the receiver antenna;
- C/1.d User segment (i.e., received signal processing, thermal noise, interference).

The proper determination of these factors has been widely addressed in the civil aviation field [RD06][RD11][RD12][RD21][RD22], where the concept of "nominal conditions" has been introduced. In this context, nominal conditions are Signal In Space (SIS) conditions in which the errors due to any GNSS segment are within their specifications and the magnitude of other external error sources is within its typical values [RD06][RD14].

For example, the factors C/1.a and C/1.b are efficiently managed by the current augmentation systems, namely Satellite-Based Augmentation Systems (SBAS: EGNOS and WAAS in the U.S.) and Ground-Based Augmentation Systems (GBAS, LAAS in the U.S.), which provide real-time corrections to the errors of type C/1.a and C/1.b as well as an estimation of the residual error statistics [RD12][RD23][RD24][RD25][RD26][RD27].

The effects of C/1.c have been subject of extensive studies. In the civil aeronautical field multipath and interference are potentially significant in the airport areas, during take-off and landing. Such limited areas may be covered by GBAS stations, which continuously monitor the received signal and can detect interference effects, while multipath (in particular, ground-reflected multipath and systematic antenna errors) is typically accounted for with an "inflation" approach, which modifies ("inflates") the statistics of the pseudorange error so as to take into account the effect of the "heavy tails" of the errors distribution caused by multipath [RD28][RD29]. Non-Line-Of-Sight (NLOS) propagation is very unlikely in aeronautical scenarios.

The effect of C/1.d depends on the signal processing algorithms adopted by the specific receiver and on their response to thermal noise, diffuse multipath, interference and other processing errors, etc. Also the adopted antenna and front-end play a relevant role.

This kind of characterization allows to determine the variance of the pseudorange error (σ_{pr}^2) for each satellite in view, typically computed as follows [RD06][RD12]:

$$\sigma_{pr}^2 = \sigma_{gnd}^2 + \sigma_{iono}^2 + \sigma_{tropo}^2 + \sigma_{rx}^2 \qquad \textbf{(3-7)}$$

where σ_{gnd}^2 refers to the residual errors of type C/1.a + C/1.c after ground-based corrections, $\sigma_{iono}^2, \sigma_{tropo}^2$ represent errors of type C/1.b due to ionosphere and troposphere gradients

(computed through elevation-dependent models), σ^2_{rx} refers to receiver errors of type C/1.d (this term is often found in the form σ^2_{air}, being specifically referred to the "air-borne" receiver). All these contributions are elevation-dependent. Other similar expressions to compute the pseudorange variance can be found [RD30], all based on the same rationale. It is worth noticing that the estimates of the $\sigma^2_{\bullet}$ parameters *do not depend on the actual measurements* of the receiver, but are always extracted from models tabulated as a function of certain operative conditions (e.g., the satellite elevation, the receiver type and configuration, etc.).

Source's error monitoring also includes the real-time detection of "big" errors, which significantly exceed the expected behavior modeled for the nominal conditions. Such big errors can be seen as *biases* of the measured pseudoranges and determine non-nominal (faulty) conditions. They must be detected in order to avoid the misuse of nominal models, which could likely cause non-integer situations.

For example, it has been widely observed that in GBAS reference stations, while small and moderate errors are Gaussianly distributed, larger errors beyond 2-3 times σ_{gnd} occur with a greater-than-Gaussian frequency [RD22]. However, since PLs are typically computed under the Gaussian hypothesis and the integrity risk requirement is posed on the "tails" of the Gaussian distribution, if "Gaussianity" is not perfectly matched with the actual conditions, then the fulfilment of the integrity risk requirement cannot be guaranteed.

The aviation field also developed the Receiver Autonomous Integrity Monitoring (RAIM) approach, which do not rely on the use of augmentation systems. Nonetheless, RAIM as well requires the statistical characterization of the pseudorange error components, in a way similar to (3-7) and the detection (and possibly exclusion) of faulty conditions [RD07].

3.2.3.2. C/2: Role of the localization module

The localization module in Figure 3-7 (and Figure 1-1) is the entity responsible for collecting all the measurements from the localization sources and accordingly producing a localization estimate, associated to an integrity assessment.

If the localization module employs GNSS as a sole localization information source and solves a Least-Squares problem to obtain the localization solution starting from the measured pseudoranges, the **mapping function** from the observation domain (range domain) to the position domain can be written in the well-known (although simplistic) form [RD07]:

$$\sigma^2_{pos} = DOP \cdot \sigma^2_{UERE} \qquad \textbf{(3-8)}$$

where σ^2_{UERE} is the pseudorange error factor which expresses an "overall" pseudorange variance as a function of the pseudorange error variances σ^2_{pr}, σ^2_{pos} is the variance of the position error and DOP is the Dilution of Precision factor that depends on the current geometry. The determination of σ^2_{pr} depends on all the factors listed in paragraph 3.2.3.1.

Furthermore, more complicated expressions, which relates the different σ^2_{pr} associated to the different satellites to σ^2_{pos} are possible, with a mapping function always dependent on a geometry factor [RD12].

However, if the localization module includes different sources of position/velocity information (e.g., IMUs, motion sensors, videocameras, etc.), a new "unified" mapping rule from the observation domain to the position domain should be defined, together with the appropriate statistical characterization of the error sources on the additional measurements.

3.3. OPERATIONAL PROCESS FOR THE INTEGRITY ASSESSMENT

The fundamental steps that operatively lead to build the integrity functionality in Figure 1-1 (in terms of current PL and availability of the integer localization) can be described as follows – from a very high-level perspective:

1. Computation of the PL[2]:
   a. Exclude as much as possible non-nominal conditions, i.e., "big errors";
   b. *i)* If the hypothesis of system working in nominal conditions is accepted, then retrieve the statistical characterization of the possible errors, i.e., the σ_{pr}^2's and the resulting σ_{pos}^2;

      ii) Compute the protection level for the current localization solution, on the basis of σ_{pos}^2 and of the integrity risk (Section 3.1).
   c. *otherwise* (i.e., in case of non-nominal conditions) integrity cannot be assessed and the location system works as "Not Monitored" with respect to its integrity level;

   It is worth noticing that the procedure to actually compute the PL is not univocal. RAIM-based approaches are different than xBAS ones; furthermore, within the wide RAIM family several different methods exist. However, all the procedure share the same underlying idea of characterizing the distribution of the error sources in the observation domain, mapping the relevant statistics to the position domain, and computing the needed percentile to satisfy the application-dependent integrity requirement.
2. Check the integer system availability comparing the PL against the AL.

A slightly different sequence of steps is followed in the typical RAIM procedure, although conceptually equal to the presented one. RAIM first computes the PL, then checks the system Availability, finally performs "Fault Detection" (FD) or "Fault Detection and Exclusion" (FDE), based on test statistics associated to the current measurements. If FD detects a "faulty" condition, then the location system moves to a "Not Monitored" condition with respect to its integrity. If Exclusion (i.e., FDE) is possible, then the faulty satellite is excluded from the localization estimation, PL is recomputed and availability is re-checked with the reduced geometry.

[2] As said before, for the sake of simplicity the procedure drawn here is expressed in the position domain only.

4. ROLE OF POSITIONING INTEGRITY IN MAIN ROAD DOMAIN APPLICATIONS

A lot of new LBSs for land users in the road/ITS fields are going to enter the market in the near future, which would highly benefit from or even require integrity information. A comprehensive analysis and classification of such services has been proposed in [RD01]. The needs of each family of applications, in terms of certain quantifiable performance features, were summarized in Table 4-3 of the cited document.

Here we leverage on the analysis of the applications proposed in [RD01] to **focus on the integrity-related performance features** (namely, integrity, availability and continuity), associated to each class of applications.

4.1. DISCUSSION ON THE PERFORMANCE FEATURES PER CLASS OF APPLICATIONS

This section discusses the common needs of the clusters of GNSS-based road applications already identified in [RD01], focusing on positioning integrity, availability and continuity. Specific discussions on the required navigation performance for certain classes of road applications can be found in [RD31][RD32][RD33].

It is interesting to notice that literature references, although trustworthy, sometimes disagree on evaluating certain performance features. For example, reference [RD32] disagrees from [RD31] and [RD34] on weighting the "continuity" feature for tolling and other PCA solutions. While [RD32] assigns a high continuity requirement to PCAs, [RD31] and [RD34] convincingly affirm that "electronic toll collection systems do not require continuity" ([RD34] page 98, col. 1). Here we adopt this latter view not only for PCAs, but also for the case of RCAs (e.g. eCall, emergency navigation, digital tachograph).

Safety-Critical Applications (SCA)	
Road Navigation - enhanced	**Autonomous driving**
Autonomous vehicles are enabled by the combination of different technologies and sensors, allowing the in-vehicle system to autonomously identify the proper actions. Since actions in autonomous vehicles are most of the time driven by the current position of the vehicle itself (either absolute or relative), GNSS plays a key role in supporting autonomous vehicles by providing relevant inputs for integrated navigation. Since it is a highly safety-critical application, autonomous driving is expected to pose requirements for **availability**, **integrity** and **continuity**, being the latter two the most stringent.	
Road Navigation – enhanced	**ADAS (e.g. "safe" speed advice)**
In general terms, Advanced Driver Assistance Systems (ADASs) are systems intended to help the vehicle's drivers in ensuring a safety and better driving. For instance, ADAS may automate lighting, provide adaptive cruise control, automate braking, alert driver to other cars or dangers, keep the driver in the correct lane, or show what is in blind spots. For the purpose of our analysis, the "safe" speed advice feature is considered here as an example. Similarly to autonomous driving, also in this case safety-of-life actions could be involved, triggered from the positioning estimate. Furthermore, a wrong advice from an ADAS could be more dangerous than no advice. For this reason, the same needs as for autonomous driving in terms of **availability**, **integrity** and **continuity** can be recognized.	

Fleet Management – enhanced	**Hazardous Material Tracking (HMT)**

Considering the fact that this application is focused on the reliable tracking of dangerous goods, high **availability** of **integer** positioning is expected to be required. On the other hand, continuity seems of less relevance, since no positioning-driven hazardous manoeuvres are foreseen.

Payment-Critical Applications (PCA)

Tolling	**Road User Charging (RUC), on-street parking billing ("*location-based charging*" in general)**

In this case the computed position and velocity are used as the basis for an economic transaction. As such, an error in those magnitudes above certain threshold can provoke the computation of a wrong charge.[3] In order to keep the probability of those harmful effects below certain (very small) limit, it is essential to also bound the errors and to ensure that the probability that errors are not properly bounded is extremely small. This feature is directly linked to the concept of **integrity**.

Furthermore, also the **availability** of the integrity-enabled service is important to foster acceptance through the velocity at which the transaction is performed.

On the other hand, continuity seems less demanding, since no continuous critical operations depend on positioning.

Pay-per-use services	**PAYD, PPUI**

Pay-As-You-Drive (PAYD) and Pay-Per-Use-Insurance (PPUI) are the typical applications which charge a user on the basis of the time spent driving across certain extended areas (for example, an insurance fee per hour could be higher if the car is driven across a city area than along rural roads).

For this reason, a correct assessment of the **integrity** of each estimated position is fundamental, although the requirements will be likely less stringent than for tolling applications, where charging is related to more accurate position estimates in shorter temporal windows and position outliers can directly lead to mischarging events.

Furthermore, in order to assure an acceptable service, **availability** is an important feature, while continuity of operations is less (or no) demanding.

Regulatory-Critical Applications (RCA)

Emergency Services	**eCall**

Whatever the trigger for the emergency call (i.e., either automatic by vehicle's sensors in case of an accident or manual by the driver or witnesses in nearby cars), the caller's position provided to the emergency responder shall be **available** (as output of the positioning system in the vehicle) and should be supported with a reasonable degree of **integrity** to drive the rescue team straight to the accident location.

Since no critical operations that depend on the continuity of integer positioning are expected, continuity appears less demanding.

Road Navigation – enhanced	**Navigation for emergency vehicles**

Similar to the eCall, the navigation of the rescue vehicles alerted after an eCall poses requirements of **high availability**, in order not to delay the time of intervention, **integrity**, in order to allow a precise and secure coordination of the rescue intervention, but no special necessity for continuity of integrity.

[3] Note that economic liabilities are also associated to the legal aspects due to the repercussion of potential claims.

Vehicle Tracking	**Digital Tachograph**
For the purposes of DT, the start and the end position of the any work session shall be automatically recorded with a reliable time stamp. New regulations are being issued in Europe in order to increase the reliability and the trustworthiness of the recorder data by mandating the inclusion of GNSS capabilities in future DT devices. As such, a demand for the **integrity** of the estimated position is clearly posed, as well as for **availability**, whereas the requirement in terms of continuity seems less stringent with respect to SCA applications.	

The above considerations are summarized in the last three columns of the following table (Table 4-1), in terms of *qualitative* scores assigned per application. Their aggregate evaluation will allow conducting the analysis *per class of applications* (i.e., SCA, PCA, RCA), which gives a synoptic view of the quite variegate panorama of the location-dependent road/ITS applications. This will be the topic of the following subsection.

4.2. SUMMARY ON PERFORMANCE EVALUATION

The following table reports a qualitative evaluation of the performance features (in terms of **H**igh, **M**edium, and **L**ow scores) associated to various location-dependent road/ITS applications, with particular emphasis on the features pertaining to the integrity framework (last three columns, highlighted by the black border).

		Position accuracy	Time accuracy	TTFF	Position authenticity	Robustness to interference	GNSS sensitivity	Availability	Position integrity	Continuity
SCA	Autonomous driving	H	H	M	L	M	L	**M**	**H**	**H**
	Road Navigation – enhanced (ADAS)	M/H	M	M	L	M	L	**M**	**H**	**H**
	Fleet Management – enhanced (HMT)	L/M	M	M	H	H	M	**H**	**H**	**L/M**
PCA	Tolling – Location based charging	L/M	L	M	H	H	M	**H**	**H**	**L**
	PAYD	L	L	L	H	H	M	**M**	**H**	**L/M**
RCA	Emergency Services – eCall	M	L	M/H	L	H	H	**H**	**M**	**L**
	Road Navigation – supporting emergency	M	L	M/H	L	H	H	**H**	**M**	**L**
	Vehicle Tracking – DT	L	L	L	H	H	L/M	**M**	**M/H**	**L**

Table 4-1: Classification of location-dependent road/ITS applications (on the rows) and allocation of performance features (on the columns), from [RD01].

As far as the **SCA applications** are concerned, their qualitative scores in Table 4-1 have been allocated taking into account the stringent integrity requirements related to this class of applications. In detail, applications involving possible safety-of-life actions (e.g. autonomous driving and ADAS) require a high level of position integrity and continuity whereas, in case of enhanced fleet management, the availability feature is more relevant than the continuity.

Focusing on the **PCA applications**, this class includes liability-critical applications where the position errors can have a direct economic impact on the service providers and on the users (mischarging or overcharging). For this reason, the position integrity has the highest score. On the other hand, the accuracy and continuity features have slightly different roles for each application in this class (e.g. RUC and PAYD), depending on the specific requirements and constraints.

Last but not least, most of **RCA applications** (e.g. eCall and navigation for emergency vehicles) require high availability, in order to increase the service coverage in terms of space and time, moderate integrity, ensuring the trustworthiness of the position information, but no special necessity for continuity. The DT application represents a special case, with slightly different requirements in terms of the availability and integrity features.

The assignment of proper *numerical quantities* to the performance features discussed above is anything but straightforward. The first step, which can be directly derived from the classic integrity framework, is the identification of suitable performance *metrics* to quantitatively characterize each feature. However, being the second step the quantitative assessment of such metrics, still there is an evident lack of adequate, consolidated and comprehensive analysis of the overall framework as per Figure 3-5.

For the sake of practicality, as pursued anywhere throughout this document, we will try to give quantitative performance indications in the next Chapter (Section 5.1 and Table 5-1), but their *validity must be considered limited to a reasonable exercise bounded by the mentioned lack of a consolidated framework*.

5. GUIDELINES FOR THE DEFINITION OF GNSS POSITIONING INTEGRITY PERFORMANCE

The need for a new definition of the integrity framework in the non-aviation contexts has become clear for some years [RD14][RD18][RD30][RD31][RD35].

The major works available in the literature which deal with the definition of an integrity framework tailored to the land/road domain are:

- The earliest GMV's activity, dated back to 2008-2009, which led to define the concept of Isotropy-Based Protection Level (IBPL), tailored to terrestrial environments and liability-critical applications [RD31][RD36];
- The activity carried out at ENAC and Thales France (2010-2012), tailored in particular to the Electronic Toll Collection application [RD14][RD30][RD33][RD34];
- The EC's "Integrity GNSS Receiver (IGNSSRX)", dated 2012-2014 and focused on characterizing integrity faults in terrestrial environments [RD37];
- The ESA's "Integrity of Navigation for Land Users" (INLU) project, developed by Airbus and dated 2014-2015 (on-going at the time of writing) [RD32].

Considering the relevance of the cited projects, the authors back the following analysis with a comprehensive critical revision of the lessons learned from them.

5.1. KEY PERFORMANCE METRICS

With the purpose of defining an integrity framework for road/ITS applications, the following key *metrics* should be quantified *for each class of application*, which specify the performance features of Integrity and Continuity discussed in the previous Chapter (Table 4-1):

1. **Integrity Risk**, per class of applications, in terms of probability per a reference time interval (Page 13);
2. **Continuity Risk**, per class of applications, in terms of probability per a reference time interval (Page 15);
3. **Horizontal Alarm Limit** (HAL), per class of applications, in meters (Page 14);
4. **Time To Alarm**, per class of applications, in seconds (Page 15).

Furthermore, in order to admit an increased degree of flexibility, each metric might be specified for two (or a few more) different *categories of operations* (e.g., "stringent", "loose"), so as to achieve a full specification of the integrity framework. For example, the integrity risk for an application which belongs to the PCA class could be given as:

$\mathcal{R}_I$ (stringent) = $x{\cdot}10^{y}$ or $\mathcal{R}_I$ (loose) = $z \cdot 10^{t}$.

Aiming at providing at least some preliminary quantitative values of the selected metrics, possible ranges of values have been identified for each metric and for each identified class of application (SCA, PCA, RCA), as summarized in Table 5-1.

The values reported in Table 5-1 must not be considered as definitive values, but just as a first tentative for the identification of suitable ranges for each metric. In detail, these ranges of values have been derived/ inferred from the limited information (few explicit numerical values) available at time of writing from few papers in scientific literature [RD33][RD38] [RD39]. It is worth to point out that the available information has been critically reviewed and complemented, leveraging the technical expertise of the authors in GNSS applications, in order to cover all the three identified classes of road applications (SCA, PCA, RCA). As discussed in Section 5.2, some important open issues still need to be further investigated and solved in order to achieve the complete definition and validation of the numerical values of each performance requirement.

Metrics	Integrity Risk		Continuity Risk		Horizontal Alarm Limit (m)		Time To Alarm (s)	
Category of operation / Class of applications	Stringent (every 5–150 s)	Loose (every 10 min–1 h)	Stringent (every 5–150 s)	Loose (every 10 min–1 h)	Stringent	Loose	Stringent	Loose
SCA	$1\cdot10^{-8}$ – $1\cdot10^{-7}$	$1\cdot10^{-7}$ – $1\cdot10^{-5}$	$1\cdot10^{-6}$ – $1\cdot10^{-5}$	$1\cdot10^{-5}$ – $1\cdot10^{-3}$	5–10	10–25	1–6	6–10
PCA	$1\cdot10^{-6}$ – $1\cdot10^{-5}$	$1\cdot10^{-4}$ – $1\cdot10^{-3}$	$1\cdot10^{-5}$ – $1\cdot10^{-4}$	$1\cdot10^{-3}$ – $1\cdot10^{-1}$	10–20	20–40	6	≥60
RCA	$1\cdot10^{-5}$ – $1\cdot10^{-4}$	$1\cdot10^{-4}$ – $1\cdot10^{-3}$	$1\cdot10^{-4}$ – $1\cdot10^{-3}$	$1\cdot10^{-3}$ – $1\cdot10^{-1}$	10–25	25–50	6	≥60

Table 5-1: Identified key performance metrics for GNSS positioning integrity and identified ranges of values for each class of application.

As a general comment/remark, it is worth noticing that in Table 5-1 , the IR and CR performance metrics are expressed with respect to "relatively short" time intervals (i.e. 5–150 seconds) for "stringent" categories of operations and "relatively long" time intervals (i.e. 10 minutes – 1 hour) for "loose" categories of operations. This is in line with the aeronautical specifications for different phases of flight (SARPS and European GNSS High Level Document requirements, summarized in [RD39]).

Focusing on the first row of Table 5-1, it must be pointed out that the reported metrics for the **SCA applications** have been identified taking into account as a starting point the stringent integrity requirements for safety-of-life applications in the aviation domain [RD39]. These ranges of values have been adapted considering the peculiarities of possible safety-critical applications in the road domain, for example ADAS applications [RD38][RD39].

References [RD38][RD39] have also been considered for the identification of the metrics related to **PCA applications** (reported in the second row Table 5-1). In addition, the information reported in [RD33] has also been considered. This document contains detailed analyses and performance results related to a specific tolling application. For this reason, [RD33] has been selected as a key source of information for the PCA case and it has been critically reviewed. A suitable range of values for the Integrity Risk has been derived from the values of probability of missed detection (P_{MD}) considered in [RD33] for a RAIM algorithm. On the other hand, Continuity Risk values have been extrapolated from the results in terms of probability of false alarm (P_{FA}) obtained in an urban scenario and considering a dual constellation receiver (GPS L1 + Galileo E1) augmented with SBAS corrections (i.e. EGNOS in Europe).

As far as **RCA applications** are concerned, similar continuity requirements have been considered with respect to the previous case (PCA), due to the similarities already noticed in Table 4-1. A slight difference is related to the integrity risk requirements, which seem to be slightly more stringent in the PCA case.

5.2. OPEN ISSUES FOR THE ROAD DOMAIN

The application of the positioning integrity concept drawn in Chapter 3 to road/ITS users and the preliminary values for the performance metrics reported in Table 5-1 entail several open

issues, which need to be addressed in order to achieve the full definition of positioning integrity in such domain.

The major issues can be listed in the following points:

- Identification of the application requirements, per class of applications;
- Suitable fault analysis, per class of applications;
- Characterization of the errors in the observation domain, including the presence of hybrid (i.e., multi-source) localization solutions;
- Role of the European GNSS (i.e., EGNOS and Galileo);
- Appropriate integrity algorithm;
- Validation of the models.

These open issues are then discussed in the paragraphs below.

5.2.1. IDENTIFICATION OF THE APPLICATION REQUIREMENTS

The requirements strictly depend on the applications. The levels "user-service" and "operation" identified in Section 3.2.1 (entity (A) in Figure 3-5) are not clearly posed nor standardized so far. For example, charging performance metrics associated to Electronic Toll Collection are defined in [RD40], but numerical values of these metrics are not standardized [RD34]. For other emerging applications the situation is similar, or even less stable.

A thorough analysis of the application requirements, at both user-service and operation levels, is necessary in order to identify the accepted risk of the application at hand. This analysis should be general enough to categorize the risks per each class of applications (as identified in Section 4.1), in order to delineate a framework of requirements in which even new services and applications easily fit.

5.2.2. FAULT ANALYSIS

The fault analysis necessary to apportionate the risk to the various subsystems of the positioning module is a fundamental but non-trivial step of the integrity definition procedure (Section 3.2.2 and entity (B) in Figure 3-5).

For example, [RD32] proposes the *integrity fault-tree* shown in Figure 5-1 for a GNSS-only positioning for land users. The assignment of the actual values for these integrity risks depends on (*i*) the user's needs ("root to leafs") and (*ii*) the technical feasibility ("leafs to root"). Thus, the integrity risk allocated to each node of the tree depends on the integrity risk allocated to the top of the tree, which in turn depends on the type of application. On the other hand, the integrity risk associated to each reasonable cause of error at each tree's leaf must be assessed and driven to the tree's root. Four major aspects are worth being noticed:

1. The scheme assumes GNSS+IMU positioning;
2. The IMU characteristics are not specified; they are considered as "mixed together" with the SIS errors;
3. The "non-receiver" branch of the tree is derived from SBAS integrity [RD41]. The assigned integrity risk is split between a fault-free branch and a faulty branch;
4. The work to derive the actual values for the integrity risks on the "receiver" branch is ongoing; it is based on extensive simulation campaigns aimed at estimating the integrity risk associated to each cause of integrity events (i.e., the tree's leafs). Results are expected to be available by mid-2015.

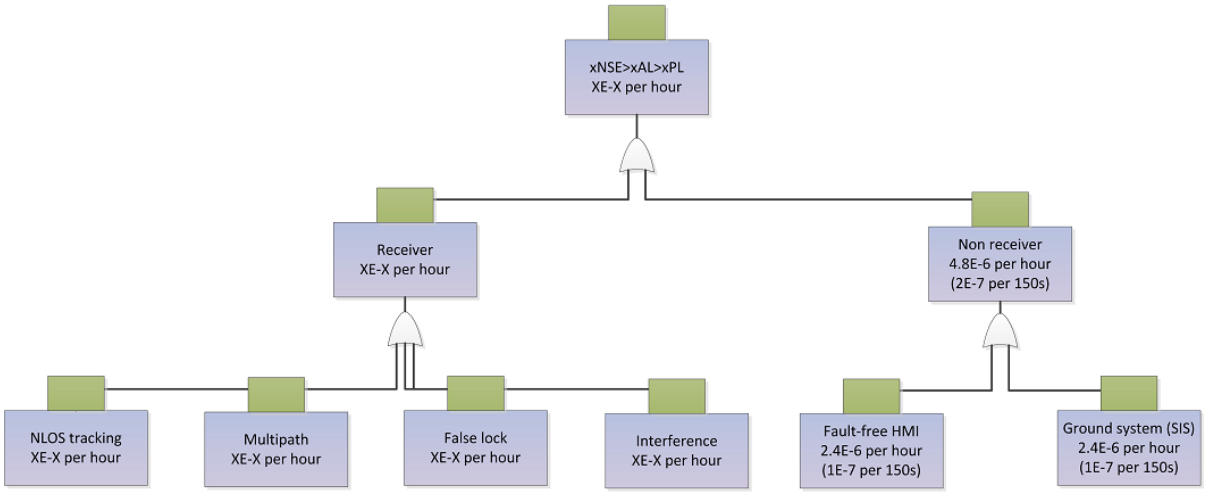

Figure 5-1: Land user integrity fault tree used within the INLU study in [RD32].

The integrity fault tree proposed in [RD14] is somehow similar to the one in Figure 5-1, if some fundamentals are considered:

1. The scheme assumes a GNSS-only positioning;
2. The integrity risk is quantified in [RD14] in terms of *probability of hazardous misleading information;*
3. Probabilities are given *per independent sample*, not per hour; the samples independency is an important issue, discussed in Section 5.2.3;
4. The integrity tree is populated "from the root to the leafs", starting from a specific application requirement (namely requirements from an Electronic Toll Collection system); the resulting admissible "SIS integrity risk" is quite elevated, so that the SBAS-related term is considered negligible.

The lesson learnt from all the cited works can be summarized in the following major points:

- Fault tree construction is a complex system-level discipline: apportioning of risks is a non-trivial task, which can be faced under different points of views [RD35];
- So far, integrity fault trees associated to road/ITS applications are not consolidated; they should be produced on a per-class of applications basis, possibly using a common rationale;
- The effect of errors events on sources of localization information other than GNSS is not clearly addressed at the fault tree level in the available literature;
- An allocation tree for the continuity risk has not been proposed so far.

It is worth mentioning here that [RD18][RD35] discuss in deep the actual limitations of the risk allocation in the fault tree assumed for civil aviation. Although the approach used to apportionate the risk in Figure 3-6 is forced by the civil aviation requirements (the so-called "specific risk assessment" in [RD18][RD35]), it is far from optimal in the perspective of non-aviation applications. Indeed, the authors demonstrates how the conservatism implicit in the "specific risk assessment" built in SBAS to meet civil aviation specific needs penalizes non-aviation users in term of size of the resulting protection levels (and so, in term of availability): for example the broadcast Grid Ionospheric Vertical Error (GIVE) values that bound worst-case ionospheric errors (and thus the resulting PLs) are proven to be much higher than they would be if the worst-case error addressed by the "specific risk" approach were not the dominant concern, as it is expected for non-aviation users. For this reason, [RD18][RD35] assert that the risk analysis previously done for civil aviation users should be

redone for road/ITS users under an "average risk" perspective, which is expected to be less conservative but more suitable for non-aviation applications. More details on the subject of using SBAS integrity for road/ITS applications are discussed in Section 5.2.4.

5.2.3. CHARACTERIZATION OF THE ERRORS IN THE OBSERVATION DOMAIN

The major difference between aviation-borne and non-aviation user groups is the GNSS threat space: for the aviation user, the main GNSS threat is an erroneous Signal-in-Space (SIS) caused either by the upload of wrong navigation message data or by a satellite malfunction. On the other hand, the very complicated land user environment makes the error induced at user level very difficult to model and bound, as the propagation channel is governed by a combination of different multipath effects, signal shadowing, and interference [RD32].

The approach used in [RD30] models the pseudorange measurement error in nominal conditions as the overbounding result of the convolution of several independent error sources, whose variance is the sum of the variance of all error sources:

$$\sigma^2_{pr} = \sigma^2_{clock\&ephem.} + \sigma^2_{iono} + \sigma^2_{tropo} + \sigma^2_{multipath} + \sigma^2_{noise} \quad \textbf{(5-1)}$$

While erroneous SIS's can be monitored and mostly corrected thanks to the SBAS signals (whose contribute will be better discussed in Section 5.2.4), the proper characterization of the "local environment" ($\sigma^2_{multipath}$) nearby the receiving antenna is still a hot topic for road/ITS applications. This characterization entails the identification of error statistics in the pseudorange domain, but is complicated by the fact that the local environment, affected by variable multipath propagation, signal blockage, and interference, makes conditions quite variable and difficult to predict.

Works [RD30][RD32][RD33] address the problem using a simulative approach: extensive simulations, based on the Land Mobile Satellite Channel Model (LMSCM) standardized by the ITU [RD42][RD43], are used for generating comprehensive error statistics and for consequently characterizing the $\sigma^2_{multipath}$ component.

On the other hand, the work [RD37] and also the approach presented in [RD44][RD45] aim at measuring the actual errors and deriving the error bounds through extensive on-field data collections.

Finally, the proposal [RD31][RD36] uses some real data collections to validate an error model for multiple errors developed in the domain of the pseudorange residuals.

Exclusion of NLOS measurements

A first clear indication emerges from the cited works: the presence of Non-Line-Of-Sight (NLOS) pseudorange measurements is extremely detrimental; the pure reflection of signals (NLOS multipath) is particularly critical as it can introduce large errors with non-negligible probability. High Sensitivity receivers that are essential to ensure position availability in urban environments are even more affected by NLOS multipath and, as a matter of fact, the mentioned improvement of availability is very in particular achieved due to their capability to acquire and track reflected signals [RD31].

The large data collection campaign used in [RD31] confirmed that the predominant error cause in urban environments is multipath; the distribution of the errors is far from having a Gaussian behaviour what makes the error bounding more difficult. This also implies that further accuracy improvements in the satellite segment (GPS, EGNOS and Galileo) will not substantially improve the accuracy performance in a city, if the problem of multipath propagation is not appropriately addressed.

Therefore the pure space-segment signal integrity (that in civil aviation is almost directly translated into position integrity) is far from enough for ensuring the position integrity

[RD31], so that the use on NLOS exclusion techniques in the receiver can make a big difference in terms of integrity performance.

Interference models

So far, little emphasis has been put on the characterization of the interference effects with regard to the integrity implications. Radio-frequency interference has been considered a reasonably negligible threat in the civil aviation domain, but this could be not the case for terrestrial applications [RD37].

Unfortunately, a proper characterization of the interference errors is a hard task, as the actual type of interference is typically unknown [RD37].

For these reasons, the probability of capturing detrimental interference signals in real environments should be carefully assessed, and an appropriate failure mode should be developed.

Error correlation

When operational requirements express the need for a bunch of *independent* position estimates to complete a certain operation (e.g., the association of a user to a certain road segment [RD14][RD31]), then the time correlation among successive measurements has to be taken into account.

The correlation time of the position error depends on the characteristics of the pseudorange measurements used in the estimation, which are derived from the error sources identified in the nominal measurement model. Except for the thermal noise and multipath, the error correlation times defined in civil aviation are valid.

Pseudorange errors in non-SBAS single frequency receivers are driven by the ionospheric one, resulting in a correlation time *close to 30 minutes*. On the other hand, dual-frequency receivers present an error correlation of *a few seconds*, mainly driven by the thermal noise and multipath. The dominant error source in SBAS-enabled single frequency receivers depends on the GNSS signal robustness against noise and multipath and results on the order of *some seconds* [RD14].

In conclusion, the correlation time will be longer in single-frequency receivers than in dual frequency ones because of the effect of the ionospheric delay. Then, it is more probable that single frequency receivers produce less independent position estimates available for a certain operation. Dual frequency receivers are more likely to provide several independent position estimations per operation, which improves the performance of certain applications [RD14].

Other localization sources

The conceptual model of the positioning module in Figure 1-1 clearly refers to the presence of several sources of localization information other than GNSS. Since they concur to determine the localization estimate in the localization module, their effect on the distribution of the position-domain error must be taken into account.

The work [RD32] performs global error measurements for a receiver architecture which integrate also an IMU, at different possible levels of integration (namely, loose, tight and ultra-tight). However, in this approach the accuracy and stability grades of the IMU are not system parameters, but are somehow “buried” in the resulting measurement statistics; this means that the error statistics obtainable with an IMU of different grade are likely different.

The integration with other sensors seems suffering from the same lack of structured analysis under the viewpoint of the positioning integrity.

Hybrid positioning systems merge satellite navigation with other sensors (inertial sensors, odometer, pressure sensors that estimate the altitude, laser, cameras, etc.) with the aim of improving the performance of standalone GNSS, especially in environments of reduced satellite visibility. Inertial measurement units (IMU), composed of accelerometers and gyroscopes, are one of the most common sensors used in civil aviation, road and urban applications [RD01].

Hybridization techniques are usually implemented with Kalman filters, which are recursive loops. Although they are a powerful tool for integrating data from different sensors, integrity analysis with Kalman filters are complicated because once a faulty measurement with a large error enters the system, it contaminates the rest of the measurements and remains in the recursive loops. This fact makes it difficult to predict the performance of the integrity monitoring system at a given instant.

For this reason, most literature offers examples in which a receiver structure with no Kalman filter is chosen. The navigation solution is typically calculated applying the weighted least squares (WLS) estimator to the pseudorange linear measurement model. This fact strongly limits the sensors that can be hybridized and seems not to be representative of an actual situation in which commercial receivers for vehicular users widely use hybridization techniques. However, as soon as a more integrated integrity assessment takes place, the need for a suitable characterization of the errors associated to the non-GNSS sources becomes mandatory. A preliminary example is given in [RD46].

Digital maps

There are three key components of a positioning module used to determine vehicle position on a road [RD47]:

1) Localization sensors: GNSS receiver, Dead-Reckoning (DR), or an integrated GNSS and DR module;
2) Geographic Information System (GIS)-based road map;
3) Map-Matching (MM) algorithm.

Due to errors associated with raw localization fixes (obtained from the localization sensors) and the GIS-based road map, these raw localization fixes do not always fall on the correct road links. An MM algorithm is used to augment the raw localization data with a spatial road network to correctly identify the road segment on which a vehicle is traveling and to determine the vehicle's location on that road segment [RD47].

Digital maps include errors that can be geometric, e.g., displacement and rotation of map features, or topological, e.g., missing road features. Even where the raw positioning data and the map quality are good, MM techniques sometimes fail to identify the correct road segment, particularly at roundabouts, level-crossings, and Y junctions; in dense urban networks; and on parallel roads. Any error associated with the raw localization fix, the digital map, or the MM process can lead to wrong location identification. Thus, when monitoring the integrity of a positioning system it is also necessary to consider errors associated with a spatial map and an MM process.

To date, research has separately focused on either the integrity of raw localization data obtained from stand-alone GNSS (or, sometimes, hybrid GNSS+IMU with the limitations cited above) or the integrity of the MM process and digital map errors. However, any time a map-matched positioning fix is provided for the operations of an application layer, these sources of error should be simultaneously considered, in order to concurrently take into account all the potential error sources affecting the output of the positioning module. An example of such an approach is offered in [RD47], however such kind of techniques seem not to be at the state of the art.

5.2.4. ROLE OF EGNSS

The European GNSS (EGNSS) panorama is dominated by **EGNOS** and **Galileo**, which both potentially play a big role in integrity-enabled road/ITS applications.

Role of EGNOS

EGNOS (and, in general, SBAS) broadcasts augmentation information that allows error correction and integrity monitoring in a wide area, typically a continent. Any user with an EGNOS receiver can obtain the augmentation information throughout the coverage area. ITS

systems just need to equip vehicles with the adequate receiver to be able to use EGNOS corrections and integrity, without any additional infrastructure.

SBAS satellites are typically in a geostationary orbit, which results in relatively low elevation angles at high latitudes like those of the European territory. This fact may cause signal masking in scenarios with important obstacles such as urban environments. This problem of satellite visibility is solved with technologies like EDAS that uses internet as a complementary transmission link of EGNOS messages, allowing the access to augmentation information in environments were satellites are likely to be blocked. In this case the receiver is not required to receive the EGNOS signals, being enough with an internet connection. The SBAS-based PL represents nowadays the unique accepted approach to satellite-based integrity provision in aviation. Nonetheless, the inherent limitations of the GNSS navigation in the road domain affect its performance, resulting insufficient for some critical applications [RD46][RD48].

SBAS integrity has been conceived under civil aviation requirements and assumptions [RD35]. For example, broadcast parameters UDRE (User Differential Range Error) and GIVE (Grid Ionospheric Vertical Error) are computed in compliance with the civil aviation integrity risk (i.e., 2×10^{-7} per approach) and under a "specific risk" perspective [RD18][RD35], in which each type of credible failure is assessed assuming that it occurs in a "worst-case" fashion, thus obtaining extremely conservative assessments [RD35].[4] Most of these assumptions are not suitable for roads. Furthermore, SBAS integrity monitoring cannot detect failures generated in the user's immediate environment, NLOS multipath for example, because it relies on differential corrections computed by a network of reference stations.

EGNOS error corrections are still applicable and highly recommended for ITS to cope with system failures related to the space segment and the ionospheric propagation [RD14][RD30][RD33][RD34][RD46].

If EGNOS corrections are used for applications with integrity requirements different from the civil aviation ones, their residual error distributions are assumed to overbound always the real error (and not to be designed only to assure the civil aviation integrity risk). However, a likely problem of over-conservatism might arise [RD35]. Simulation results from [RD33] show how the application of the EGNOS corrections (only for satellite and ionospheric errors, without implementing the complete SBAS integrity computation) can reduce of nearly one order of magnitude the variance of the pseudorange error in a road-urban environment, still not resolving the multipath problems. Of course, failures of different origins, like those caused by the local environment, must be monitored in a different way.

Role of Galileo

Benefits from multiple constellations are well documented for urban scenarios, in which medium-to-low elevation satellite visibility is made difficult because of obstructions from buildings and NLOS propagation [RD49]. Today multi-constellation receivers are already in place to exploit the advantage of an increased number of satellites in the sky; with the beginning of the commercial operation of Galileo, triple-constellation-capable devices will enjoy a coverage given by more than 90 satellites in orbit, with further possibilities to improve positioning availability and integrity [RD46]. Furthermore EGNOS V3 is going to be extended to augment also the Galileo signals, while augmentation for GLONASS is under study: this fact will extend space and ionosphere segments corrections to two or three constellations, with an immediate advantage to the integrity performance of enabled receivers.

[4] UDRE and GIVE are statistical estimates of the satellite and ionospheric errors remaining after applying the wide-area differential (WAD) corrections. These are used to compute a certified error bound for the position solution in an integrity assessment. At user level, the receiver estimates corrections for satellite clock and ephemeris errors using the WAD data. The UDRE term characterizes statistically the residual range errors after having applied the clock and ephemeris corrections. The receiver predicts also ionospheric delays for each range interpolating from the surrounding grid points which have been estimated by the augmentation system. The GIVE term is applied to the range vector to characterize statistically the residual ionospheric errors.

Besides **multi-constellation** positioning, Galileo presents at least two intrinsic advantages with respect to legacy GPS satellites:

1) **Reduced clock & ephemeris error**: the worst signal-in-space accuracy associated to the Galileo clock and ephemeris error is about one order of magnitude less than the user range accuracy broadcast in the navigation message of legacy GPS satellites [RD30]. However, the GPS user range accuracy is expected to decrease as the system evolves.
2) Very **precise ionospheric correction model** for single frequency receivers (NeQuick G [RD50]): the performance evaluation of GNSS positioning error on L1 with single-frequency NeQuick G corrections, performed at a low-latitude station for more than one year, showed in average better precision than using GPS Klobuchar corrections and better accuracy than dual-frequency ionospheric-free solution [RD50].

The capability of correcting for most of the ionospheric error without relying on dual-frequency receivers but using either EGNOS or the Galileo-intrinsic NeQuick G, can be a distinguishing feature in dense urban environments: indeed, it is well known that dual-frequency processing has the major drawback of magnifying multipath and receiver noise error components in the measurements. In propagation conditions where multipath is the major error source, namely, dense urban conditions, magnifying such error component could be more penalizing than accepting a residual ionospheric error from EGNOS or NeQuick corrections. This fact has been demonstrated by simulation campaigns in [RD33].

5.2.5. INTEGRITY ALGORITHMS

Airborne receivers are operated in a relatively well-controlled environment regarding satellite visibility, interference, and multipath distortions. A loss of integrity caused by the Signal-in-Space (SIS) is the only threat considered by the aviation user. Thus, state-of-the-art integrity algorithms mainly focus on the detection of misleading information originating from the system such as incorrect satellite ephemeris or clock errors [RD32]. However, integrity algorithms for non-aviation users have not yet been developed with a comparable level of maturity, essentially because of the dramatically more complex description of the surrounding environment and error sources.

Considering the multi-faceted road-user environment, the most promising approach to provide integrity in GNSS-based land navigation is given by a methodology based on the exploitation of all the available on-board sensors to autonomously determine the integrity level of the estimated positioning. An analogy with Aircraft Based Augmentation Systems (ABASs) can be recognized. The ABAS integrity monitoring scheme is a set of algorithms that autonomously monitors integrity using redundant range measurements; they are classified as receiver autonomous integrity monitoring (RAIM) when they use exclusively GNSS information, and as aircraft autonomous integrity monitoring (AAIM) if they include additional on-board sensors [RD33][RD51].

ABAS integrity monitoring involves algorithms, run at the receiver, that process redundant GNSS measurements and, optionally, information from other sensors installed in the vehicle. For this reason it appears an appropriate integrity monitoring scheme for vehicular receivers, in which integrity is monitored at the receiver via software and, if sensors are used, these are on board the vehicle. ABAS deals directly with GNSS user's measurements which procure information about all errors and failures affecting vehicle positioning, including those that cannot be detected by other systems based on reference receivers. Furthermore, ABAS can be adapted to multi-constellation receivers and to road applications needs [RD33].

Under this perspective, autonomous integrity monitoring algorithms of the type RAIM have appeared suitable, in principle, for road applications [RD32][RD33][RD34]. This family of techniques, initially created for aerial navigation, is based on an over-determined solution to evaluate its consistency, and therefore it requires a minimum of five satellites to detect a satellite anomaly, and six or more to be able to reject it [RD07]. Unfortunately, this cannot

be assumed in usual road traffic situations, especially in cities. In addition, the RAIM method makes the assumption that only one failure appears at the same time at the receiver. While this assumption may be easily accepted in the aerial field, the scenario is very different in the road sector, in which a vehicle drives in very different conditions. For instance, in the very usual case of one car driving through the city center of any medium size European capital, it is quite probable that several satellite signals are affected by simultaneous multi-path propagations. Since classic RAIM does not consider this possibility (NLOS is not identified as a failure threat in civil aviation, being its probability negligible [RD31]), its integrity test may easily fail when it appears [RD46] .

As a consequence of the above considerations, the following evaluations arise:

- A suitable reference methodology to evaluate the integrity of the positioning information provided by the localization module must be identified;
- This methodology is likely to fit into a family of "Vehicle Autonomous Integrity Monitoring" algorithms, derived from RAIM/AAIM approaches but better suited into the vehicular context;
- The additional information from multiple localization sources should be taken into account in such methodology;
- Algorithms for detection of NLOS tracking, loss-of-lock indicators, and multipath detection should be included;
- The probability of multiple simultaneous faults should be taken into account.

To give some examples, [RD32] considers an architecture encompassing three different groups of algorithms:

1) Algorithms for fault detection and exclusion or overbounding at signal processing level (detection of NLOS tracking, loss-of-lock indicators, multipath detection);
2) Algorithms for fault detection and exclusion at PVT level (classic Fault Detection and Exclusion, FDE);
3) Algorithms for protection level calculation (classic Weighted Least Squares Residuals RAIM).

On the other hand, an experimental RAIM scheme suitable in the presence of multiple faults is proposed in [RD31][RD36].

Finally, [RD46] proposes a method to evaluate an integrity indicator, slightly different than the classic PL, suitable for multi-sensor fusion in terrestrial domains.

Nonetheless, **a consolidated approach** to assess the integrity of the multi-source positioning solution computed by the localization module **is not available yet**.

5.2.6. MODEL VALIDATION

Aiming to a full definition of a positioning integrity framework in the road domain, another open issue that needs to be addressed is the validation of the selected models and algorithms. In fact, a key aspect to provide an integrity service in terrestrial environments is to understand and characterise the local environment, mainly in terms of signal multipath and interference. The result of this characterization is a model of the local degradations, to be further validated by means of extensive data collections and field tests.

This important issue is discussed for example in [RD37], where three main objectives are mentioned:

a) The development of two *platforms to capture and store GNSS radio frequency signal samples and a reference trajectory* from representative low-, medium- and high-end sensors in terrestrial applications;
b) An ***extensive data collection campaign*** aiming to characterize error sources, magnitudes and probabilities for two important GNSS terrestrial application areas: automotive and pedestrian users;

c) The *research and development of techniques and algorithms to mitigate the integrity threats* in the two terrestrial environments studied using the collected data, thus allowing reliable terrestrial applications within these domains.

The need for an extensive validation of the models and algorithms is also pointed out in [RD32]. In this case the integrity performance of the algorithms under test will be assessed by means of a proper Integrity Analysis Tool, carrying out the following tasks:

1. First, the capabilities regarding detection and mitigation will be assessed, especially at signal processing level, for example by calculating the ***probabilities of missed, true, and false exclusion of measurements*** under the *different operating conditions* the land user is faced with, e.g. NLOS signals, severe multipath, fading and interference;
2. Another important performance indicator is the ***time required to detect*** non-nominal conditions like the ones mentioned before, but other non-nominal conditions like locks to a false peak in case of BOC tracking will need to be considered, too;
3. Finally, the ***validity*** of the calculated Protection Levels will need to be assessed, e.g. by means of Stanford plots, and investigations regarding ***continuity*** and ***availability*** will be performed.

However, it is worth to mention that the final results of this study, i.e. the proposal of a concept that allows to provide integrity for the land user, are not available yet (expected in 2015 [RD32]).

Once available, these results will represent a key input for subsequent standardization activities. For example, in the case of the CEN/CENELEC draft document [RD03], the results obtained from extensive validation and performance assessment activities might be used in order to explicitly quantify the integrity performance requirements. A detailed analysis of the obtained results will allow to bound feasible values and then to define specific numbers for the integrity performance metrics, as for example in terms of statistical distribution of the Protection Levels in a specific scenario (i.e. the set of three statistical values given by the 50^{th}, 80^{th} and 95^{th} percentiles of the cumulative distribution of Protection Levels computed for a target Integrity Risk).

6. CONCLUSIONS AND PERSPECTIVES

The results of this study represent a **first step in order to completely define an integrity framework suitable to road applications**.

A complete discussion on the integrity performance metrics and the related open issues in road domain has been reported in previous sections. In detail, after a review of the positioning integrity concept from a general point of view (in Section 3), its role in the road transport sector has been focused in Section 4. The integrity **performance features** have been discussed for the main road domain applications and a preliminary performance evaluation has been carried out, aiming to clearly identify the relevance of each performance features in each class of application.

Starting from the lessons learned from the available scientific literature covering GNSS integrity aspects in the road domain, guidelines and a possible reference methodological approach towards the completion of the definition of the GNSS positioning integrity performance requirements have been analysed. Among the considered references, the results from the Signal Processing Techniques for the Integrity of Navigation for Land Users (INLU) study [RD32] appear to be the most promising. Since the final conclusions are not available yet (expected by mid 2015), we recommend to take into account the outcomes of this project when public.

Following this methodology, the identified performance features have been expressed in terms of **key performance metrics** in Section 5. In addition, preliminary quantitative ranges of values have been identified for each selected metric and for each identified class of application (SCA, PCA, RCA) in Section 5.1, based on "reasonable extrapolations" from the available literature. However, the validation and practical suitability of those ranges cannot be guaranteed without properly resolving a series of open issues which basically differentiate the aviation integrity from the vehicular/terrestrial one.

These **open issues,** related to the definition of performance requirements and of the quantities involved in the integrity assessment, have been discussed in Section 5.2. Their structured solution is not straightforward, but a possible **approach towards the standardization of integrity performance requirements** could be basically the one followed in [RD32], which includes the following steps:

1. **Identification of road user applications requiring GNSS and their specific needs** in terms of integrity, continuity, and time to alarm (a detailed fault analysis must be performed). This step also involves the description of algorithm candidates that are able to compute and evaluate actual integrity bounds for said use cases;
2. **Definition of realistic scenarios** which are representative for the applications under investigation and **characterization of the errors** in the observation domain, in order to define proper error models (characteristics and frequency of occurrence of non-line of sight signals, locks to secondary peaks of the correlation function, as well as multipath propagation and interference);
3. **Implementation of a versatile simulation environment**, suitable to extensive analyses and comparative performance assessments by means of realistic software and hardware simulations involving a variety of tracking and mitigation algorithms, as well as conventional and novel integrity algorithms for the calculation of protection levels for the road user's PVT errors;
4. **Assessment of the integrity performance** of the different combinations of tracking, mitigation and integrity algorithms under test. The results of this integrity algorithms evaluation will be used as feedback to iteratively improve the techniques used and, potentially, to **validate and select candidate algorithms**;
5. A further step of **Validation** of the models **through extensive data collection campaigns** in real environments is also needed.

7. REFERENCES

[RD01]	Fostering the European GNSS Adoption in Road/ITS: Additional Analysis and Actions Implementation. "Technical Analysis of New Paradigms Increasing EGNSS Accuracy and Robustness in Vehicles," April 2015.
[RD02]	R. Mort, P. Crosta, J. Giraud, K. Judge, and M. Pini, "Standardisation of GNSS-Based Location Systems Architecture and Performance in ETSI," in *Proc. of 7th ESA Workshop on Satellite Navigation Technologies (NAVITEC 2014)*, Noordwijk, The Netherlands.
[RD03]	CEN/CENELEC, *Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) - Part 1: Definitions and system engineering procedures for the establishment and assessment of performances*, DRAFT prEN 16803-1, October 2014.
[RD04]	Kovach, K., "Continuity: The Hardest GNSS Requirement of All," in *Proc. of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998)*, Nashville, TN, September 1998, pp. 2003-2020.
[RD05]	W. Y. Ochieng, K. Sauer, D. Walsh, G. Brodin, S. Griffin, and M. Denney, "GPS Integrity and Potential Impact on Aviation Safety," *The Journal of Navigation*, n. 56, pp. 51-65, 2003. Doi:10.1017/S0373463302002096.
[RD06]	S. Gleason and D. Gebre-Egziabher, *GNSS Applications and Methods*, Artech House, 2009. ISBN: 978-1596933293.
[RD07]	R. Conley et al., "Performance of Stand-Alone GPS," Chapter 7 in *Understanding GPS: Principles and Applications*, Second Edition, edited by E. Kaplan and C. Hegarty, Artech House, 2006. ISBN: 978-1-58053-895-4
[RD08]	GMV, "Integrity," Navipedia website, 2011. Available at: http://www.navipedia.net/index.php/Integrity
[RD09]	*Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment.* Washington, DC, RTCA SC-159, WG-2, DO-229D, Dec. 13, 2006. http://www.rtca.org
[RD10]	*Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment.* Washington, DC, RTCA SC-159, WG-4, DO-253C, Dec. 16, 2008. http://www.rtca.org
[RD11]	S. Pullen, "Providing Integrity for Satellite Navigation: Lessons Learned (Thus Far) from the Financial Collapse of 2008-2009," in *Proc. of ION GNSS 2009*, Savannah, GA, Sept. 22-25, 2009, pp. 1305-1316. Available at: http://waas.stanford.edu/papers/Pullen_IONGNSS_2009.pdf
[RD12]	A. Martineau, "Performance of Receiver Autonomous Integrity Monitoring (RAIM) for Vertically Guided Approaches," Ph.D. thesis, Université de Toulouse, November 14, 2008. Available at: http://ethesis.inp-toulouse.fr/archive/00000984/01/martineau.pdf
[RD13]	GSA, GNSS Market Report, Issue 4, March 2015. Available at: http://www.gsa.europa.eu/market/market-report

[RD14]	D. Salós, A. Martineau, C. Macabiau, D. Kubrak, and B. Bonhoure, "Groundwork for GNSS Integrity Monitoring in Urban Road Applications. The Road User Charging Case," in *Proc. of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, Portland, OR, September 2010, pp. 1130-1144.
[RD15]	International Organization for Standardization (ISO), *Electronic fee collection - Charging performance - Part 1: Metrics*, ISO/TS 17444-1, First Edition, 2012.
[RD16]	R.B. Langley, "The Integrity of GPS," *GPS World*, Vol. 10, No. 3, March 1999, pp. 60–63.
[RD17]	W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, *Fault tree Handbook*, U.S. Government Printing Office, 1981.
[RD18]	S. Pullen, T. Walter, and P. Enge, "Integrity for Non-Aviation Users: Moving Away from Specific Risk," *GPS World*, July 2011, pp. 28-36.
[RD19]	Oehler, Veit, Luongo, Francesco, Boyero, Juan-Pablo, Stalford, Roland, Trautenberg, Hans L., Hahn, Jörg, Amarillo, F., Crisci, M., Schlarmann, B., Flamand, J.F., "The Galileo Integrity Concept," in *Proc. of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2004)*, Long Beach, CA, September 2004, pp. 604-615.
[RD20]	J. Rife, B. Pervan, "Overbounding Revisited: Discrete Error-Distribution Modeling for Safety-Critical GPS Navigation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 2, pp. 1537-1551, April 2012. Doi: 10.1109/TAES.2012.6178077.
[RD21]	J. Lee, S. Pullen, and P. Enge, "Sigma-mean monitoring for the local area augmentation of GPS," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 42, no. 2, pp. 625-635, April 2006.
[RD22]	J. Lee, S. Pullen, and P. Enge, "Sigma Overbounding using a Position Domain Method for the Local Area Augmentaion of GPS," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 45, no. 4, pp. 1262-1274, October 2009.
[RD23]	Stanford GPS Lab website, "WAAS Precision Approach Metrics: Accuracy, Integrity, Continuity and Availability," 1999. Available at: http://waas.stanford.edu/metrics.html
[RD24]	S. Pullen, "Augmented GNSS: Fundamentals and Keys to Integrity and Continuity," Tutorial Presentation, ION GNSS 2011. Available at: http://www-leland.stanford.edu/~spullen/ION_GNSS_2011_Tutorial_-_Aug-GNSS_final_(Pullen,_09-16-11).pdf
[RD25]	P. Enge, "Local area augmentation of GPS for the precision approach of aircraft," in Proc. of the IEEE, vol. 87, no. 1, pp. 111-132, Jan 1999.
[RD26]	J. Farrell, T. Givargis, "Differential GPS reference station algorithm-design and analysis," in *IEEE Transactions on Control Systems Technology*, vol. 8, no. 3, pp. 519-531, May 2000.
[RD27]	B. Roturier, E. Chatre and J. Ventura-Traveset, "The SBAS Integrity Concept Standardised by ICAO. Application to EGNOS", ION GNSS 2001, May 2001.
[RD28]	C. Shively, and R. Braff, "An overbound concept for pseudorange error from the LAAS ground facility," in *Proc. of IAIN World Congress/ION 56th Annual Meeting*, San Diego, CA, June 26-28, 2000, pp. 661-671.

[RD29]	B. Pervan and I. Sayim, "Sigma inflation for the local area augmentation of GPS," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 37, n. 4, October 2001, pp. 1301-1311.
[RD30]	D. Salós, C. Macabiau, A. Martineau, B. Bonhoure, and D. Kubrak, "Nominal GNSS pseudorange measurement model for vehicular urban applications," in *Proc. of IEEE/ION Position Location and Navigation Symposium (PLANS 2010)*, pp. 806-815, 4-6 May 2010. Doi: 10.1109/PLANS.2010.5507319
[RD31]	J. Cosmen-Schortmann, and M. Martínez-Olagüe, M. Toledo-López, and M. Azaola-Saenz, "Integrity in Urban and Road Environments and its Use in Liability Critical Applications," in *Proc. of the Position Location and Navigation Symposium (PLANS 2008)*, Monterey, California, May 6–8, 2008.
[RD32]	F. M. Schubert, J. Wendel, F. Soualle, M. Mink, S. Carcanague, R. Ioannides, P. Crosta, and M. Crisci, "Integrity of Navigation for Land Users: Study Concept and Simulator Architecture," in *Proc. of 7th ESA Workshop on Satellite Navigation Technologies (NAVITEC 2014),* Noorwijk, The Netherlands, 3-5 December 2014.
[RD33]	C. D. Salós Andrés, "Integrity monitoring applied to the reception of GNSS signals in urban environments", *Ph. D. Thesis,* Institut National Polytechnique de Toulouse, July 2012.
[RD34]	D. Salós, A. Martineau, C. Macabiau, B. Bonhoure, and D. Kubrak, "Receiver Autonomous Integrity Monitoring of GNSS Signals for Electronic Toll Collection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 94-103, February 2014. Doi: 10.1109/TITS.2013.2273829
[RD35]	S. Pullen, T. Walter, and P. Enge, "SBAS and GBAS Integrity for Non-Aviation Users: Moving Away from "Specific Risk"," in *Proc. of the 2011 International Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2011, pp. 533-545.
[RD36]	J. Cosmen Schortmann and M. Azaola Saenz, "Autonomous Integrity: An error isotropy-based approach for multiple fault conditions," *Inside GNSS*, pp. 28-36, January-February 2009.
[RD37]	E. Domínguez et al., "Characterization of GNSS Integrity Threats in Terrestrial Applications Using Real Signal Captures," in *Proc. of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, Tampa, Florida, September 2014, pp. 954-966.
[RD38]	G. Gargiulo, M. Leonardi, M. Zanzi, G. Varacalli, "GNSS Integrity and Protection Level Computation for Vehicular Applications", in *Proc. of 16th Ka and Broadband Communications Navigation and Earth Observation Conference*, pp. 569-574, 20-22 October 2010.
[RD39]	M. Caporale, "Need for GNSS Higher Integrity," *Presentation at ICG 9*, Prague, 10 November 2014.
[RD40]	International Organization for Standardization (ISO), Geneva, Switzerland, "Electronic Fee Collection—Charging Performance—Part 1: Metrics," *ISO/TS 17444-1*, First Edition, 2012.
[RD41]	GMV, "SBAS Fundamentals," Navipedia website, 2011. Available at: http://www.navipedia.net/index.php/SBAS_Fundamentals
[RD42]	ITU, "Propagation data required for the design of earth-space land mobile telecommunication systems", *Recommendation ITU-R P.681-7 (10/2009)*, P Series, Radiowave propagation, 2009.

[RD43]	A. Lehner, A. Steingass, "A Novel Channel Model for Land Mobile Satellite Navigation," in *Proc. of ION GNSS 18th International Technical Meeting of the Satellite Division*, 13-16 September 2005.
[RD44]	D. Margaria and E. Falletti, "A novel local integrity concept for GNSS receivers in urban vehicular contexts," in *Proc. of IEEE/ION Position Location and Navigation Symposium (PLANS 2014)*, Monterey, California, USA, pp. 413-425, 2014.
[RD45]	D. Margaria and E. Falletti, "The Local GNSS Integrity Concept: Feasibility and Experimental Validation in an Urban Vehicular Scenario," in *Proc. of 7th ESA Workshop on Satellite Navigation Technologies (NAVITEC 2014)*, ESTEC, Noordwijk, The Netherlands, 2014.
[RD46]	R. Toledo-Moreo, J. Santa, M. A. Zamora-Izquierdo, B. Ubeda, A. F. Gomez-Skarmeta, "A Study of Integrity Indicators in Outdoor Navigation Systems for Modern Road Vehicle Applications," in *Proc. of 2nd Workshop on Planning, Perception and Navigation for Intelligent Vehicles*, IROS 2008.
[RD47]	N. R. Velaga, M. A. Quddus, A. L. Bristow, and Y. Zheng, "Map-Aided Integrity Monitoring of a Land Vehicle Navigation System," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 13, No. 2, pp. 848-858, June 2012.
[RD48]	D. Margaria, E. Falletti, and T. Acarman, "The Need for GNSS Position Integrity and Authentication in ITS: Conceptual and Practical Limitations in Urban Contexts," in *Proc. of IEEE Intelligent Vehicles Symposium (IV'14)*, Dearborn, Michigan, USA, 2014.
[RD49]	S. Carcanague, "Low-cost GPS/GLONASS Precise Positioning Algorithm in Constrained Environment," Ph.D. thesis, Université de Toulouse, February 26, 2013. Available at: http://ethesis.inp-toulouse.fr/archive/00002296/01/carcanague.pdf
[RD50]	R. Orus and R. Prieto-Cerdeira, "The NeQuick G model," *Workshop on the Use of Global Navigation Satellite Systems for Scientific Applications*, Trieste, Italy, December 2, 2014.
[RD51]	International Civil Aviation Organization, *International Standards and Recommended Practices - Annex 10 to the Convention on International Civil Aviation – Aeronautical Telecommunications - Volume I, Radio Navigation Aids*, 6th Edition (with amendment 85), July 2006.

END OF DOCUMENT