doi:10.5028/jatm.2012.04025611

System Architecture-based Design Methodology for Monitoring the Ground-based Augmentation System: Category I – Integrity Risk

Paulo Elias*, Osamu Saotome
Instituto Tecnológico de Aeronáutica – São José dos Campos/SP – Brazil

Abstract: *This paper has described a method to accomplish the Ground-Based Augmentation System signal-in-space integrity risk monitoring for a ground station specified by ICAO, Annex 10, Vol. 1 and RTCA DO-245A, which is a mandatory requirement to meet the certification aspects for a Ground-Based Augmentation System station. The proposed methodology was based on the Risk Tree Analysis technique, which is an optional way to design and develop an engineering solution named as integrity risk monitor that assures the integrity risk requirement for standard system architecture. The achieved results concern the qualitative and quantitative aspects of solution, which are met through the system architecture and the system safety assessment process, in special by risk assessment concepts. Finally, the integrity risk monitor is an optional architectural solution (a practical way) that has demonstrated a satisfactory result to meet the certification basis of the Brazilian Aeronautical Authorities.*

Keywords: *Ground-Based Augmentation System, Risk, Integrity, Safety, System, Architecture.*

INTRODUCTION

In the last years, the Aeronautical Industry has worked in the development of a variety of assurance technologies to meet, or to exceed, the development assurance levels (DAL) of airborne systems, and it has reached them satisfactorily. It is important to mention that the DAL concept came from the Aeronautical Standards: Society of Automotive Engineers, Aerospace Recommended Practices (SAE ARP) 4754, from 1996, ARP 4754A, from 2010, and ARP 4761, from 1996; Radio Technical Commission for Aeronautics (RTCA DO-178B), from 1992, and DO-254, from 2000.

Once the certification aspects are met, the system safety and the DAL can be accomplished and demonstrated through analyses, tests, in-the-field services, and statistical data. However, in the ground systems segment, there is no useful body of knowledge (BOK), and there is still much work to solve the Engineering problems regarding the requirements to develop a safe design. In this context, the new generation of aeronautical navigation aids appears, mainly the ground-based augmentation system (GBAS) for Category I (CAT I) precision approach and landing procedures. The GBAS for CAT I is the current worldwide project under development, which is the newest concept of satellite navigation augmentation system to improve the accuracy, integrity, reliability, and availability of final approach and landing systems of the aircrafts. The GBAS ground subsystem is part of a GBAS total system, which is based on GNSS satellite signals pseudo range measurements and corrections.

Figure 1 has been used by the Federal Aviation Administration (FAA) to show a generic GBAS installation, which provides an overview of the operational concept of the automatic approach and landing (Category I).

Since 1999, the FAA has worked in the U.S. GBAS Program together with the Honeywell Company, initially called local area augmentation system (LAAS), which represents the ground facility that provides ground services portion of the GBAS total system. The GBAS system (or GBAS total system) is comprised of two subsystems: GBAS avionics system, and GBAS ground system (or ground facility as shown in Fig. 1).

The Brazilian Government has started the Brazilian GBAS Program, leaded by the Department for the Airspace Control (DECEA), and the Brazilian Company

Received: 04/12/11 Accepted: 26/03/12

*author for correspondence: pelias2011@bol.com.br
Pç. Mal. Eduardo Gomes, 50. CEP: 12.228-901
São José dos Campos/SP – Brazil

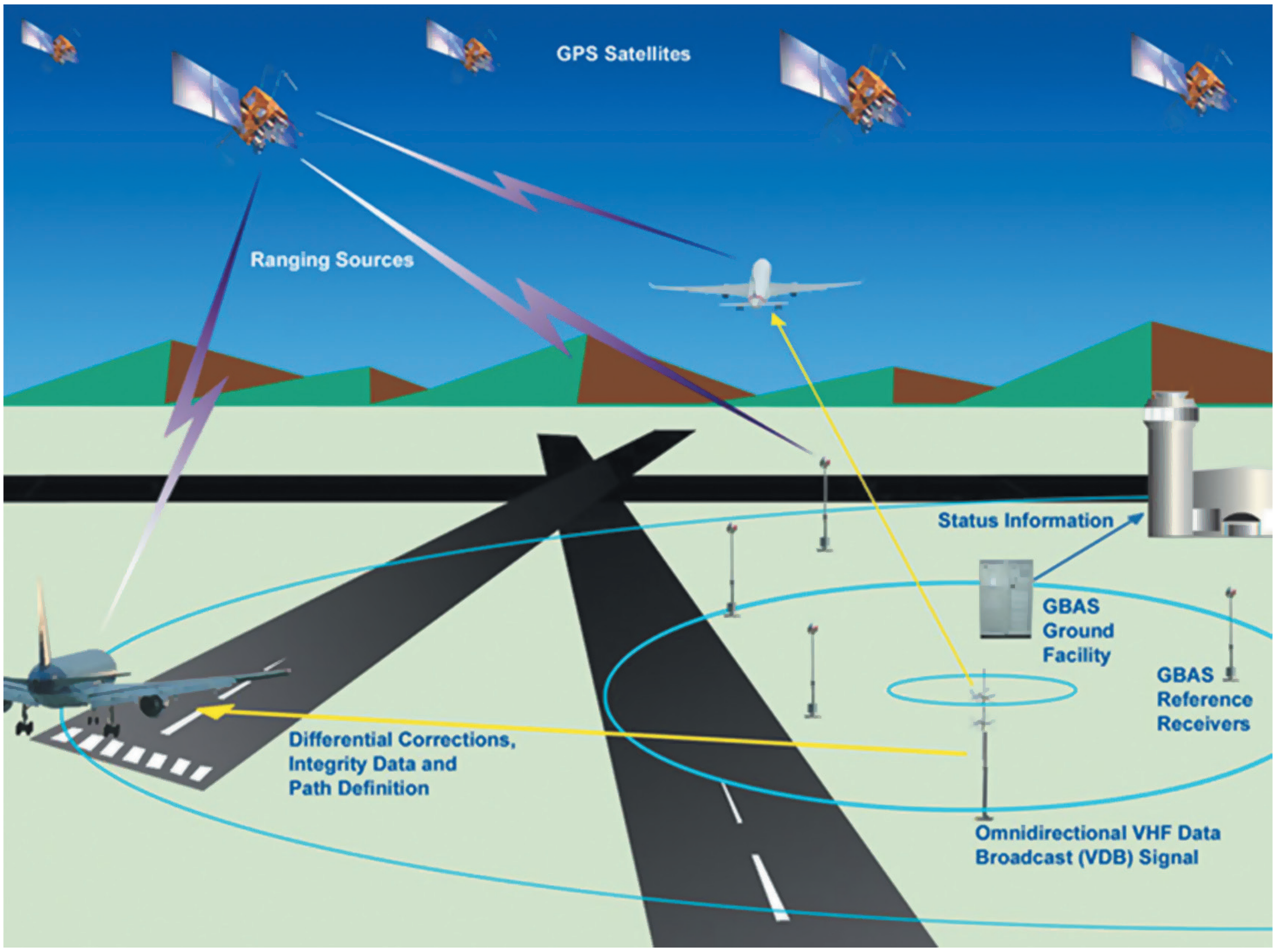

GPS Satellites
Ranging Sources
Status Information
GBAS Ground Facility
GBAS Reference Receivers
Differential Corrections, Integrity Data and Path Definition
Omnidirectional VHF Data Broadcast (VDB) Signal

Figure 1. GBAS system operation overview. Source: FAA, 2010.

IACIT *Soluções Tecnológicas Ltda*. has been working in the CAT I ground-based augmentation subsystem design and development since 2008.

When assessing the hazards that threaten the correct operation of the GBAS (both the avionics and the ground facility), one can consider that the worst and most unpredictable risk is the ionosphere bubbles. This phenomenon is more frequent and more severe in the equatorial region, where the ionospheric interference on the Global Navigation Satellite Systems (GNSS) is more likely than in the USA region. Besides that, the ionospheric interference is a common cause of errors in the GBAS, especially on the GNSS receivers (both the avionics and the ground receivers). However, this hazard is detectable and possible to be handled by specific algorithms embedded on the ground-based augmentation computer subsystems. The focus of this paper is not to design such algorithm, but to propose a ground-based augmentation subsystem architecture, which could implement those algorithms and operate in a safely way in the presence of hazards, in special the ionospheric bubbles. When the ground-based augmentation subsystem achieves this operational condition, the system has sufficient integrity to be exposed to such hazards.

The integrity requirement for a CAT I GBAS, specified by the International Civil Aviation Organization (ICAO, 2008) is as in Eq. 1:

$$Integrity = 1-2\times10^{-7}/approach \qquad (1)$$

The real problem is to understand and to meet the integrity requirement, and then to propose a system architecture that could be certifiable and adopted by the Aeronautical Industry.

From this issue and considering the integrity value required for the system operation, this paper has presented a methodology to better understand and solve the problem. It has demonstrated that the proposed CAT I ground-based augmentation subsystem architecture meets the minimum aspects of the GBAS safety, mainly the integrity requirement of the ground station Category I GBAS, which was specified by ICAO, Annex 10, Vol. 1, 6th edition, Section 3.6.7.1.2.1.1 (2008); this was performed by applying an engineering architectural solution based on risk assessment considerations and on good practices. A risk assessment technique is presented and it is known as risk tree analysis (RTA) as ICAO, Annex 10, Vol. 1, Attachment A, ATT-A1 (2008). Some definitions are important to clarify the rationale and to facilitate the understanding of results, for example, meaning of integrity, misleading information, and integrity risk defined upon the sections of this paper.

The GBAS is composed of two subsystems: ground-based augmentation airborne subsystem (GBAS-ASS), and ground-based augmentation subsystem (GBAS-GSS).

Table 1 shows the top-level integrity requirement for the CAT I precision approach GBAS specified from ICAO.

The lower values given are the minimum availabilities for which a system is considered to be practical, but they are not adequate to replace non-GNSS navigation aids. For en route navigation, the higher values given are adequate for GNSS to be the only navigation aid provided in an area. For approach and departure, the higher values given are based upon the availability requirements at airports with a large amount of traffic, assuming that operations to or from multiple runways are affected but reversionary operational procedures ensure the safety of the operation (see ICAO, Annex 10, Vol. 1, 6th edition, Attachment D, 3.5 (2008).

Table 2 specifies the alert limits for accomplishment of the GBAS integrity levels.

Based on the top-level integrity requirement for the CAT I GBAS, it is important to define which is the portion of this value to be assigned to the ground station CAT I GBAS (ground subsystem). According to ICAO, the required integrity is (1-1.5E-07)/approach, as shown in Fig. 2.

Table 1. GBAS signal-in-space performance requirements (ICAO, Annex 10, Vol. 1, 6th ed., Table 3.7.2.4-1 (2008)).

Typical operation	95% horizontal accuracy (Notes 1 and 3)	95% vertical accuracy (Notes 1 and 3)	Integrity (Note 2)	Time-to alert (Note 3)	Continuity (Note 4)	Availability (Note 5)
En route	3.7 km (2.0 NM)	N/A	1-1E – 7/h	5 min	1-1E – 4/h to 1-1E – 8/h	0.99 to 0.99999
En route, Terminal	0.74 km (0.4 NM)	N/A	1-1E – 7/h	15 s	1-1E – 4/h to 1-1E – 8/h	0.99 to 0.99999
Initial, Intermediate, and Non-precision approaches (NPA), Departure	220 m (720 ft)	N/A	1-1E – 7/h	10s	1-1E – 4/h to 1-1E – 8/h	0.99 to 0.99999
Approach operations with vertical guidance (APV-I)	16.0 m (52 ft)	20 m (66 ft)	1-2E – 7 in any approach	10 s	1-8E – 6 per 15 s	0.99 to 0.99999
Approach operations with vertical guidance (APV-II)	16.0 m (52 ft)	8.0 m (26 ft)	1-2E – 7 in any approach	6 s	1-8E – 6 per 15 s	0.99 to 0.99999
Category I precision approach	16 m (52 ft)	6.0 to 4.0 m (20 to 13 ft) (Note 6)	1-2E – 7 in any approach	6 s	1-8E – 6 per 15 s	0.99 to 0.99999

Notes: 1. the 95th percentile values for GNSS position errors are those required for the intended operation at the lowest height above threshold (HAT), if applicable. Detailed requirements are specified in Appendix B and guidance material is given in Attachment D, 3.2. 2. the definition of the integrity requirement includes an alert limit against which the requirement can be assessed. These alert limits are: a range of vertical limits for category I precision approach relates to the range of vertical accuracy requirements. 3. the accuracy and time-to-alert (TTA) requirements include the nominal performance of a fault-free receiver. 4. ranges of values are given for the continuity requirement for en route, terminal, initial approach, NPA and departure operations, as this requirement is dependent upon several factors including the intended operation, traffic density, and complexity of airspace and availability of alternative navigation aids. The lower value given is the minimum requirement for areas with low-traffic density and airspace complexity. The higher value given is appropriate for areas with high-traffic density and airspace complexity (see Attachment D, 3.4.2). Continuity requirements for APV and category I operations apply to the average risk (over time) of loss of service, normalized to a 15-second exposure time (see ICAO, Annex 10, Vol. 1, 6th ed, Attachment D, 3.4.3, 2008). 5. a range of values is given for the availability requirements as they are dependent upon the operational need, which is based upon several factors including the frequency of operations, weather environments, size and duration of the outages, availability of alternate navigation aids, radar coverage, traffic density, and reversionary operational procedures.

Table 2. Horizontal alert limit (HAL) and vertical alert limit (VAL) of the GBAS.

Typical operation	Horizontal alert limit	Vertical alert limit
En route (oceanic/ continental low density)	7.4 km (4 NM)	N/A
En route (continental)	3.7 km (2 NM)	N/A
En route, Terminal	1.85 km (1 NM)	N/A
NPA	556 m (0.3 NM)	N/A
APV-I	40 m (130 ft)	50 m (164 ft)
APV-II	40.0 m (130 ft)	20.0 m (66 ft)
Category I precision approach	40.0 m (130 ft)	15.0 to 10.0 m (50 to 33 ft)

THE METHODOLOGY APPROACH

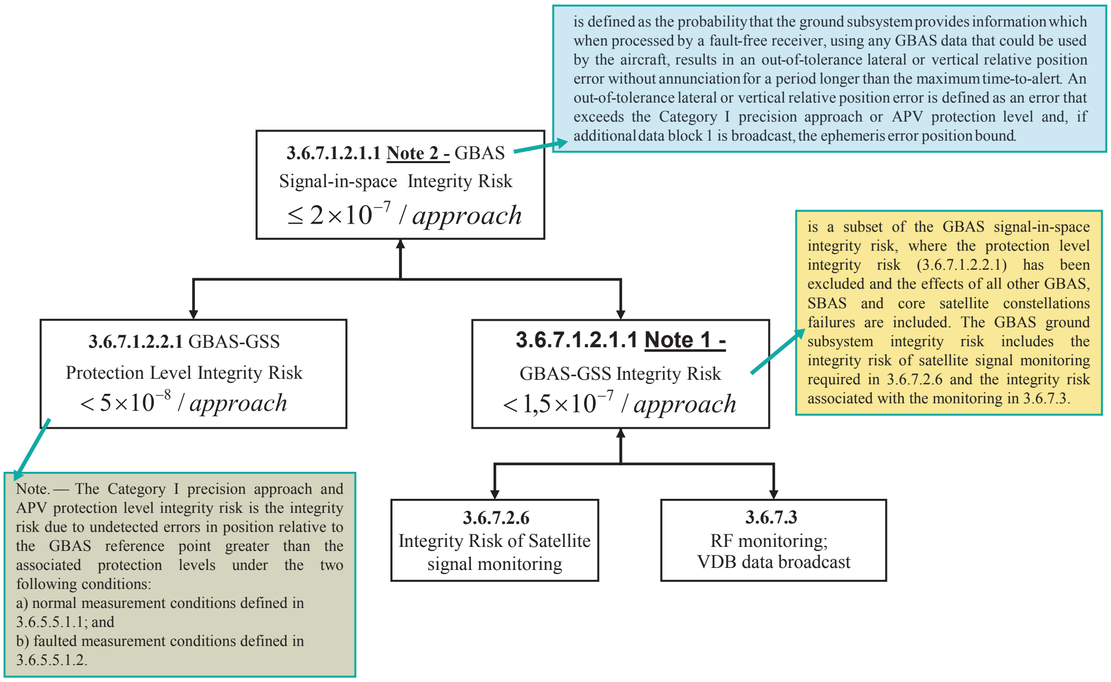
Integrity allocation methodology

The integrity allocation methodology considered for this paper was the same issued in (RTCA, DO-245A, 2004) and is illustrated in Fig. 2.

Integrity, considered a system attribute, is defined (RTCA, DO-245A, 2004) as a measure of trust that can be placed in the correctness of the information supplied by the total system. Integrity includes the ability of the system to provide timely warnings to the users (alerts) when the system should not be used for the intended operation. The maximum TTA of a CAT I GBAS is three seconds (ICAO, Annex 10, Vol. 1, 6th edition, Section 3.6.7.1.2.1.1, 2008.

An implicit assumption is that a Navigation System Error (NSE) greater than the alert limit bound for greater than the TTA is a condition that is hazardous for a CAT I approach. This paper refers to this condition as misleading information (MI). All MI hypotheses are accounted for, but two are given special attention. The H0 hypothesis refers to normal measurement conditions (i.e., no faults) in all reference receivers (RR) and in all ranging sources. The H1 hypothesis represents a fault associated with any, and only one, reference receiver. Under the H1 hypothesis, a fault includes any erroneous measurement(s) that is(are) not immediately detected by the ground system, such that the broadcast data are affected and there is an induced position error in the airborne subsystem.

The integrity allocated to the signal-in-space (SIS) is further allocated into two basic categories: integrity resulting from the NSE being bounded by the protection levels under H0 and H1 hypothesis; and integrity resulting from all other conditions not covered by H0 and H1.


3.6.7.1.2.1.1 Note 2 - GBAS
Signal-in-space Integrity Risk
$\leq 2\times10^{-7}$ / *approach*
3.6.7.1.2.2.1 GBAS-GSS
Protection Level Integrity Risk
$< 5\times10^{-8}$ / *approach*
3.6.7.1.2.1.1 Note 1 -
GBAS-GSS Integrity Risk
$< 1{,}5\times10^{-7}$ / *approach*
3.6.7.2.6
Integrity Risk of Satellite signal monitoring
3.6.7.3
RF monitoring;
VDB data broadcast

is defined as the probability that the ground subsystem provides information which when processed by a fault-free receiver, using any GBAS data that could be used by the aircraft, results in an out-of-tolerance lateral or vertical relative position error without annunciation for a period longer than the maximum time-to-alert. An out-of-tolerance lateral or vertical relative position error is defined as an error that exceeds the Category I precision approach or APV protection level and, if additional data block 1 is broadcast, the ephemeris error position bound.

is a subset of the GBAS signal-in-space integrity risk, where the protection level integrity risk (3.6.7.1.2.2.1) has been excluded and the effects of all other GBAS, SBAS and core satellite constellations failures are included. The GBAS ground subsystem integrity risk includes the integrity risk of satellite signal monitoring required in 3.6.7.2.6 and the integrity risk associated with the monitoring in 3.6.7.3.

Note.— The Category I precision approach and APV protection level integrity risk is the integrity risk due to undetected errors in position relative to the GBAS reference point greater than the associated protection levels under the two following conditions:
a) normal measurement conditions defined in 3.6.5.5.1.1; and
b) faulted measurement conditions defined in 3.6.5.5.1.2.

Figure 2. ICAO, Annex 10, Category I ground-based augmentation subsystem integrity apportionment.

The total integrity requirement on the probability of MI is allocated to the categories illustrated in Fig. 3, according to ICAO (2008).

Figure 3 groups the H0 and H1 hypotheses, which are directly addressed through the Protection Level calculations, into one allocation and groups all other cases into the other branch (cases not covered by H0 and H1). The cases not covered by H0 and H1 include the following:

- failures in the ground subsystem;
- erroneous broadcast of critical data due to failure in ground subsystem processors (e.g., corrections, B-values, sigma terms, and so on);
- undetected failures of measurements from more than one reference receiver (e.g., correlation between reference receivers (RR) measurements becomes unacceptably high and is not accounted for in broadcast terms);
- VHF data broadcasting (VDB) channel message failure or cyclic redundancy checks (CRC) fails;
- undetected failures in the ranging sources;
- GNSS constellation failure;
- failure to detect changes in atmospheric and environmental conditions;
- tropospheric parameters (e.g., refractivity, scale height, etc.);
- ionospheric variance estimation;
- environmental conditions (e.g., failure of ground monitor to detect change in environment that affects broadcast the parameter "sigma_pr_gnd".

The integrity risk associated with cases not covered by H0 and H1 will be assured to be acceptably small through design, analysis, and monitoring, and the use of ephemeris error position bound. For example, the integrity of the broadcast data is protected via CRC, in order that the probability of MI due to the VDB is acceptably small.

Rationale for integrity exposure time

The exposure times for the various service levels are based on the time associated with the operation (RTCA, DO-245A, 2004). Generically, it represents the time during which the

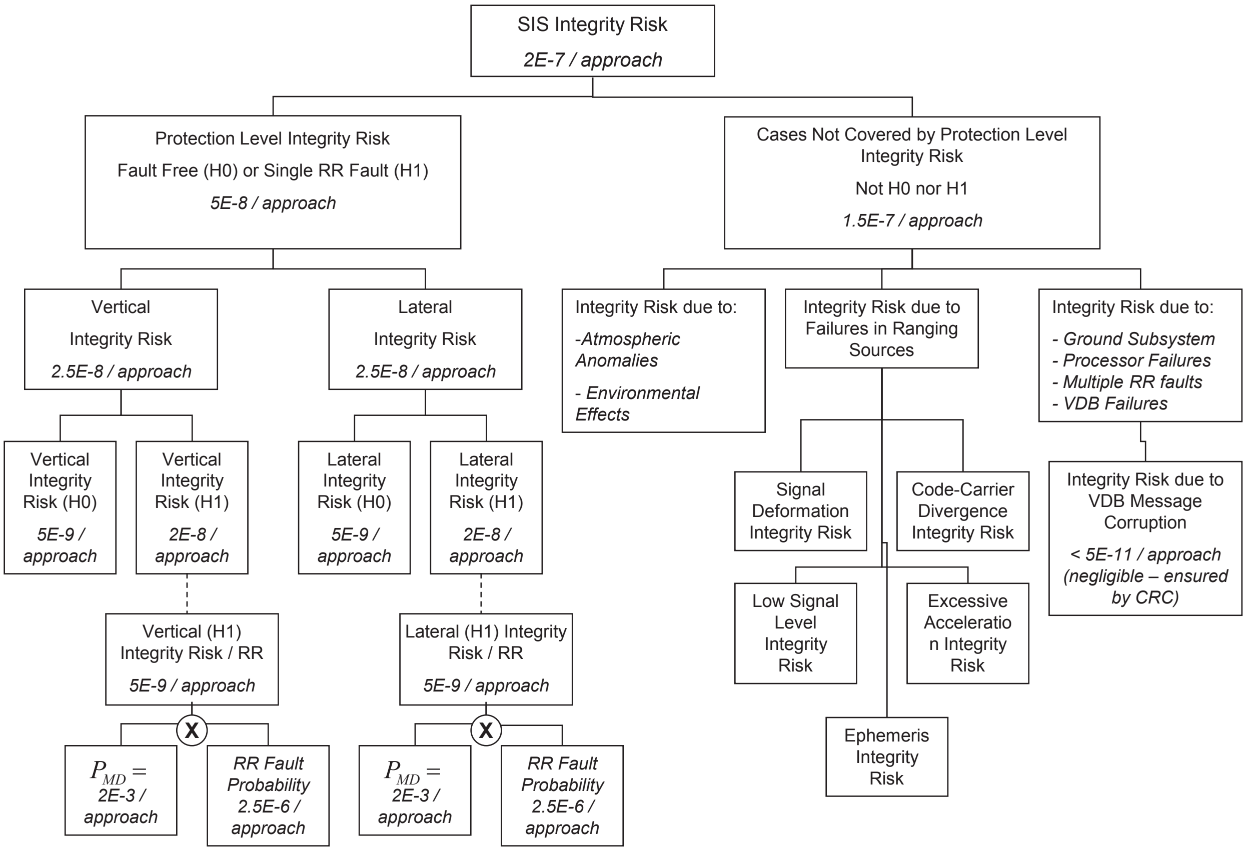


Figure 3. Integrity risk allocation tree (RTCA, 2004).

loss of integrity, and potentially resulting MI, exposes the aircraft to a hazard. Final approach begins at its fix, which is nominally located at 5 NM and in an altitude of 1,600 feet. The lowest CAT I decision height (DH) is at 200 feet. The time between the final approach fix and this CAT I DH is nominally 150 seconds, based on an aircraft approach speed of 110 knots.

Therefore, the exposure time for CAT I operations is defined to be 150 seconds. The hazard severity for MI during the phase of a precision approach from the final approach fix to the CAT I DH is classified as hazardous/severe-major, which is consistent with the SIS integrity requirement. This hazard severity through 200 ft is applicable for approach operations independent of the weather minima (CAT I, II, or III). CAT I, II, and III approaches are shown in Fig. 4.

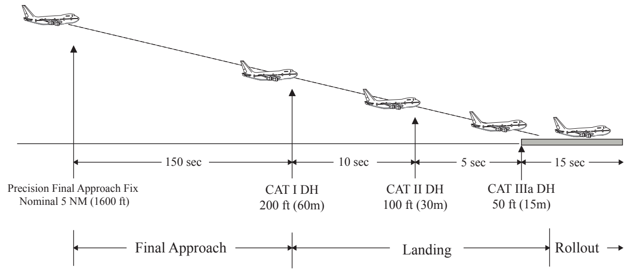


Figure 4. Approach and landing operations and associated time intervals.

Once the CAT I most severe failure condition is classified as hazardous event, considering the worst case evaluation of the identified hazard events by applying the functional hazard assessment (FHA) technique from SAE ARP 4761, Appendix A (1996), it is suggested that the required function DAL (FDAL) to accomplish the system certification is B, according to SAE ARP 4754A (2010), for the GBAS primary functions implemented on the ground subsystem to provide its functionalities. It is important to reinforce that the FDAL B required is related to the essentials functions of the system, which are identified during the conceptual phase of the system design and development.

Performing the FHA of the GBAS-GSS CAT I is out of the scope of this paper, so the most severe failure condition classified as "hazardous" is an assumption that must be evaluated and validated for each specific system design.

The required FDAL is based on the most severe failure condition classified during the FHA process. Table 3 presents the equivalent DAL (or FDAL) for each functional failure severity classification.

Table 3. Development assurance level assignment.

Failure condition classification	System development assurance level
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No safety effect	E

The DAL letters are equivalent to software integrity level letters in DO-178B (1992) and HW integrity level numbers in DO-254 (2000).

The Aeronautical standards follow the safety objectives stated by Advisory Circular/Advisory Material Joint (AC/AMJ) 25.1309 (2002) as shown in Table 4.

Integrity risk computations with ground-based augmentation system

The issue then is how to apply this approach to computing integrity for GBAS (RTCA, DO-245A, 2004). Since GBAS architectures typically are not the same as the conventional navigation systems, which consist of a transmitter and an independent monitor, the equation for calculating risk can be represented more generically as in Eq. 2:

$$Risk = 1-Integrity = P_{SIS}P_{md} \qquad (2)$$

where:

P_{SIS}= probability of a hazardous signal-in-space condition;

P_{md}= probability of a missed detection of the SIS condition.

GBAS integrity risk is actually comprised of risk from three kinds of conditions: fault free (H_0) rare normal; single reference receiver fault (H_1); and non-H_0 and non-H_1, the latter of which is also referred to as H_2. It is noted that the H_0 case is not a "failure" because there is no fault, and is rather a "rare normal" condition. The total integrity risk is the sum of these three contributors, as shown in Eq. 3. "Integrity Allocation Methodology" shows the risk allocation tree for the CAT I GBAS.

$$Risk(Total) = Risk(H_0)+Risk(H_2) \qquad (3)$$

Each of these risk types is explained and broken down in more details in the following sections. The relationship

Table 4. Failure conditions severity classification versus probability objectives.

Failure conditions severity	No safety effect	Minor	Major	Hazardous	Catastrophic
Effect on airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on flight crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Effect on occupants (excluding flight crew)	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Allowable qualitative probability	No probability requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Allowable quantitative probability (avg. probability per flight hour)	No probability requirement	$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$

between the computed risk and time is described along with a proposed methodology for handling time.

Fault free integrity risk (H_0)

Equation 4 presents the fault free integrity risk:

$$Risk(H_0) = P_{ffmd} \tag{4}$$

where:
P_{ffmd} = probability of H_0 fault free missed detection (dependent on K_{ffmd}).

The computed risk for H_0 is valid for each independent sample. This is true even though the protection level is computed by the receiver with each Type 1 message received (twice per second). The time between independent samples is dependent upon the correlation between GPS updates, GBAS corrections, and the processing of the corrections by the ground and airborne equipment (smoothing time, and so on). The effective time between independent samples depends on the absolute probability level and the duration of the event whose probability is to be characterized. The time between independent samples is approximately ten seconds for CAT I (RTCA, DO-245A, 2004). Therefore, there is a number of independent events during the period of an approach. This has to be taken into account when determining K_{ffmd}.

Single reference receiver fault integrity risk (H_1)

Equation 5 presents the single reference receiver fault integrity risk:

$$Risk(H_1) = P_{RR\text{ - }Fault} P_{H1\text{-}md} \tag{5}$$

where:
$P_{RR\text{ - }Faultd}$ = probability of a fault associated with one reference receiver;
$P_{H1\text{-}md}$ = probability of H_1 faulted missed detection (dependent on K_{md}).

The H_1 fault associated with one reference receiver includes hardware faults in the receiver and erroneous measurements induced by the environment (e.g., multipath).

H_2 integrity risk

The H_2 integrity risk is comprised of three primary elements (RTCA, DO-245A, 2004): ranging source faults; ground subsystem faults, and atmospheric anomalies (e.g., ionospheric effects), as in Eq. 6 and 7.

$$\begin{aligned}&Risk(H_2) = Risk(Ranging\ \_Sourse\_Fault)+\\&Risk(Ground\_Subsystem\_Fault)+\\&Risk(Atmospheric\_Anomaly) \qquad (6)\\&Risk(Ranging\ \_Sourse\_Fault)=P_{PS—Fault}P_{RS\_md}\\&Risk(Ranging\ \_Sourse\_Fault)=\lambda_{RS—Fault}T_{RSIS}P_{RS\_md}\end{aligned}$$

where:

$P_{PS—Fault}$ = probability of hazardous ranging source failure;
$\lambda_{RS—Fault}$= hazardous failure rate of ranging source;
P_{RS_md}= probability of missed detection of ranging source failure;
T_{RSIS}= time between independent samples of ranging source signals.

$$\begin{aligned}&Risk(Ground\_Subsystem\_Fault)=P_{Corr\_Fault}P_{Corr\_Mon\_md} \qquad (7)\\&Risk(Ranging\ \_Sourse\_Fault)=\lambda_{Corr\_Fault}T_{Corr\_Mon\_Ver}P_{Corr\_Mon\_md}\end{aligned}$$

where:

P_{Corr_Fault}= probability of hazardous corrections function failure;
λ_{Corr_Fault}= hazardous failure rate of corrections function;
$P_{Corr\_Mon\_md}$= probability of missed detection of corrections function failure;
$T_{Corr\_Mon\_Ver}$= time between verification of corrections monitor.

The value of $T_{Corr\_Mon\_Ver}$ depends upon the ground subsystem architecture. In an architecture based on redundancy where each set of corrections is verified by a voting scheme, $T_{Corr\_Mon\_Ver}$ would be 0.5 second. This does not take into account failures that could not be detected by the voting scheme (Eq. 8).

$$\begin{aligned}&Risk(Atmospheric\_Anomaly) = P_{AA}P_{AA\_md} \qquad (8)\\&Risk(Atmospheric\_Anomaly) = \lambda_{AA}T_{AAIS\_md}\end{aligned}$$

where:

P_{AA}= probability of atmospheric anomaly;
λ_{AA}= rate of hazardous atmospheric anomalies;
P_{AA_md}= probability of missed detection of atmospheric anomaly;
T_{AAIS}= time between independent samples of ranging source signals.

The value of T_{AAIS} depends upon the atmospheric anomaly and the types of measurements used for its detection.

Methodology for designing the integrity risk monitor (subsystem level)

The first step is to define the system architecture to be monitored (e.g., CAT I ground-based augmentation station presented in RTCA/DO-245A (2004), as seen in Fig. 5.

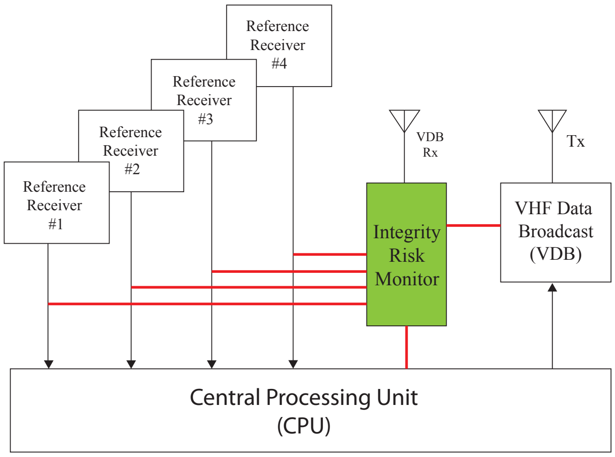


Figure 5. Ground-based augmentation subsystem block diagram with IRM.

The IRM architecture shown in Fig. 5 is a generic concept that may be applied to the GBAS systems composed by four RR, in which these four RR are identical and only one GPS L1 C/A signal receiving capability.

Currently, it is possible to implement an algorithm into RR for monitoring the GPS signal quality, which is known as signal quality monitor (SQM) (ICAO, 2006). The ICAO, Annex 10, Attachment D, Section 8.0 (2006) treats in details the SQM requirements and design aspects. The constraint of SQM is that it is only to GPS L1 signals and there is not any other reference or standard for guiding the implementation of it into the dual-frequency GNSS receivers for GBAS applications.

The second step is to define the integrity risk tree of the GBAS to be monitored (qualitative approach).

The integrity risk tree is the second step for constructing the IRM structure, and then an algorithm may be architected (it will be embedded on the IRM). For a system hierarchical purpose, the IRM is a GBAS Subsystem Unit.

The GBAS Integrity Risk Allocation (RTCA, DO-245A, 2004) is presented in Fig. 3, which is a preliminary assessment of the identified risks associated with the CAT I GBAS operations.

In accordance to DO-245A (RTCA, DO-245A, 2004), the integrity risk tree is a top-down approach, which is also known as risk budget allocation. This approach is very useful to the analysis of maximum risk levels acceptable for each item of the system. Risk levels are determined by a risk assessment process that can give a preliminary result to the risk analyst, regarding the effort necessary to implement the system architecture modifications and improvements. It is not only a technical issue, but it is also a management issue since it will usually demand for increasing the cost and the schedule of the system project, so the boundary of the analysis is not limited only by engineering efforts.

Table 5 is an example of the risk matrix to evaluate the risk level of each hazard (or threat) identified during the hazard analysis performed before the system architecture preliminary design.

Table 5. Risk assessment matrix example (DOD, 2000).

	Severity			
	Catastrophic	Critical	Marginal	Minor
Likelihood	(1)	(2)	(3)	(4)
Frequent (A)	1A	2A	3A	4A
Probable (B)	1B	2B	3B	4B
Occasional (C)	1C	2C	3C	4C
Remote (D)	1D	2D	3D	4D
Improbable (E)	1E	2E	3E	4E

Once the risk assessment standard is established, the analysis may be conducted so that each item of the risk tree assumes a level of risk in relation to the total one of the system. It is the risk analysis process and it must be conducted to create the risk matrix to be used for constructing the integrity risk algorithm to be embedded into the IRM.

The risk assessment process is performed by calculating the product of probability of occurrence (likelihood) and the severity of the consequences (impact) of each hazard (or threat) identified in the risk tree: risk = likelihood versus severity.

The result is a qualitative risk represented by a number (from one to four) and a letter (A to E). This pair is the representation of the risk level (e.g., 1A, 3C, 2B, etc.). Table 6 presents the risk assessment of identified hazards (from integrity risk tree).

Risk computations and exposure time

The exposure time associated with the operation also has to be taken into account in risk computations. In the case of instrument landing system (ILS) and microwave landing system (MLS), the computed risk is simply the one of loss of integrity over the time interval appropriate to the failure mode. For most cases, this is the monitor verification time, which can be a long interval (weeks) for manually performed checks.

The risk grows (usually exponentially) over time, and the time chosen to initiate the monitor verification action is such

Table 6. Hazards list and risk assessment (qualitative).

Protection level integrity risk fault free (H0) or single RR fault (H1)	Risk	Cases not Covered by protection level integrity risk (not H0 nor H1)	Risk
Vertical H1 Integrity Risk • RR Faults	Medium 3C	Atmospheric anomalies	2C
Vertical H1 Integrity Risk • RR Faults	High 2C	Environmental effects	Medium
Lateral Integrity Risk (H0)	Low	Integrity risk due to ground subsystem:	High
Lateral Integrity Risk (H1)	Medium	• Processor failures;	2C
		• Multiple RR faults;	2D
		• VDB failures;	2C
		• Message corruptions.	2B
Vertical Integrity Risk (H0)	Low	Integrity risk due to failures in ranging sources:	Medium
Vertical Integrity Risk (H1)	Medium	• Signal deformation integrity risk;	2D
		• Low signal level integrity risk;	3C
		• Code-carrier divergence integrity risk;	2D
		• Excessive acceleration integrity risk;	3C
		• Ephemeris integrity risk.	3C

that the maximum risk is never greater than the performance requirement. The maximum risk cannot be exceeded during a landing operation that could occur right at the end of the exposure time associated with the operation.

Applying this to GBAS, for cases in which the time between independent samples is greater than the landing one, the computed risk should be the maximum that occurs within the time interval. It is different for a situation where the time interval of interest for several GBAS cases, the time interval is the time between independent samples, which is less than the landing period. The way this should be applied is computing the cumulative risk over the landing period. Figure 6 illustrates an example. In this example, there are five independent samples over the exposure time, $T_{ind\_samples}$ is the time between samples. Therefore, the risk allowed for each measurement must be maximum risk allowed divided by five.

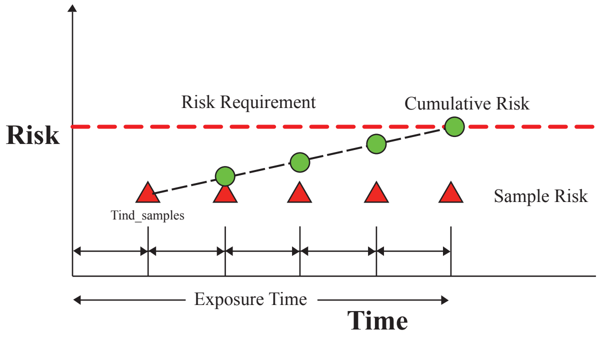


Figure 6. Integrity risk and sample intervals.

Another issue concerns how to account for failures that can remain undetected for periods longer than the exposure time. In that case, the risk computation must account for the total period of time that the failure can remain undetected.

Step 3 is to define the logic of risks and to determine the minimal cut sets of the integrity risk tree (qualitative approach).

The system items arrangement in a tree is a powerful graphical tool for visualization of the threats (or hazards) of the system and for providing an accurate evaluation of items dependencies and interrelationships among them. Over the last 50 years, this technique is used by safety and reliability specialists to model the system by a manner that any engineer or stakeholder may detect, at a glance, any hazardous situation that may affect the safety or integrity of the system under analysis.

Figure 7 represents the integrity risk tree of the ground-based augmentation subsystem under analysis. It is a preliminary evaluation of the root-causes that lead to a loss of integrity, which may occur during the aircraft operation and may threat its approach and landing (since the aircraft is equipped with a GBAS airborne subsystem).

The branch named as “Protection Levels Integrity Risk”, represented by “gate 032”, is the aircraft portion integrity risk, so it is not considered integrity risk calculation of ground-based augmentation subsystem. Therefore, it is represented with an undeveloped branch or event in accordance with the EUROCAE, ED-114 (2003), ICAO (2008) and RTCA, DO-245A (2004).

Step 4 is to allocate the SIS integrity risk budget to the system items of the integrity risk tree and to calculate the minimal cut sets (quantitative approach) (Fig. 8).

Preliminary results

Cut Sets for G029.

Top Event Probability = 2,90E-04.

By analyzing the preliminary results of cut sets probabilities (Table 7), it is very important to check if the top event probability (Gate 029) is within the limit established by the EUROCAE, ED-114 (2003), ICAO (2008) and RTCA, DO-245A (2004), which must be lower than 1.5E-07 per 15 seconds or per approach (average time of a CAT I precision approach is 150 seconds approximately). It means that the integrity level (or DAL) of the ground-based augmentation subsystem must be equivalent to Level B of the DO-178B (Software DAL) and DO-254 (Hardware DAL) to meet the safety requirements of AC/AMJ 25.1309 (2002) specified to “hazardous” failure conditions analyzed by the FHA process in the conceptual phase of the design. Therefore, as the preliminary result is out of tolerance, it is necessary to update the system architecture so that the integrity risk may be mitigated at below the limits; this process of risk mitigation (DOD, MIL-STD-882D, 2000) is also known as ALARP (as low as reasonably practicable) (ICAO, 2009).

Table 7. Cut sets probabilities.

Cut set	Probability of occurrence (Pf / hour)	Gate path
1	2.00E-04	G008
2	3.00E-05	G028
3	1.00E-05	G022
4	1.00E-05	G023
5	1.00E-05	G024
6	1.00E-05	G025
7	1.00E-05	G026
8	1.00E-05	G027

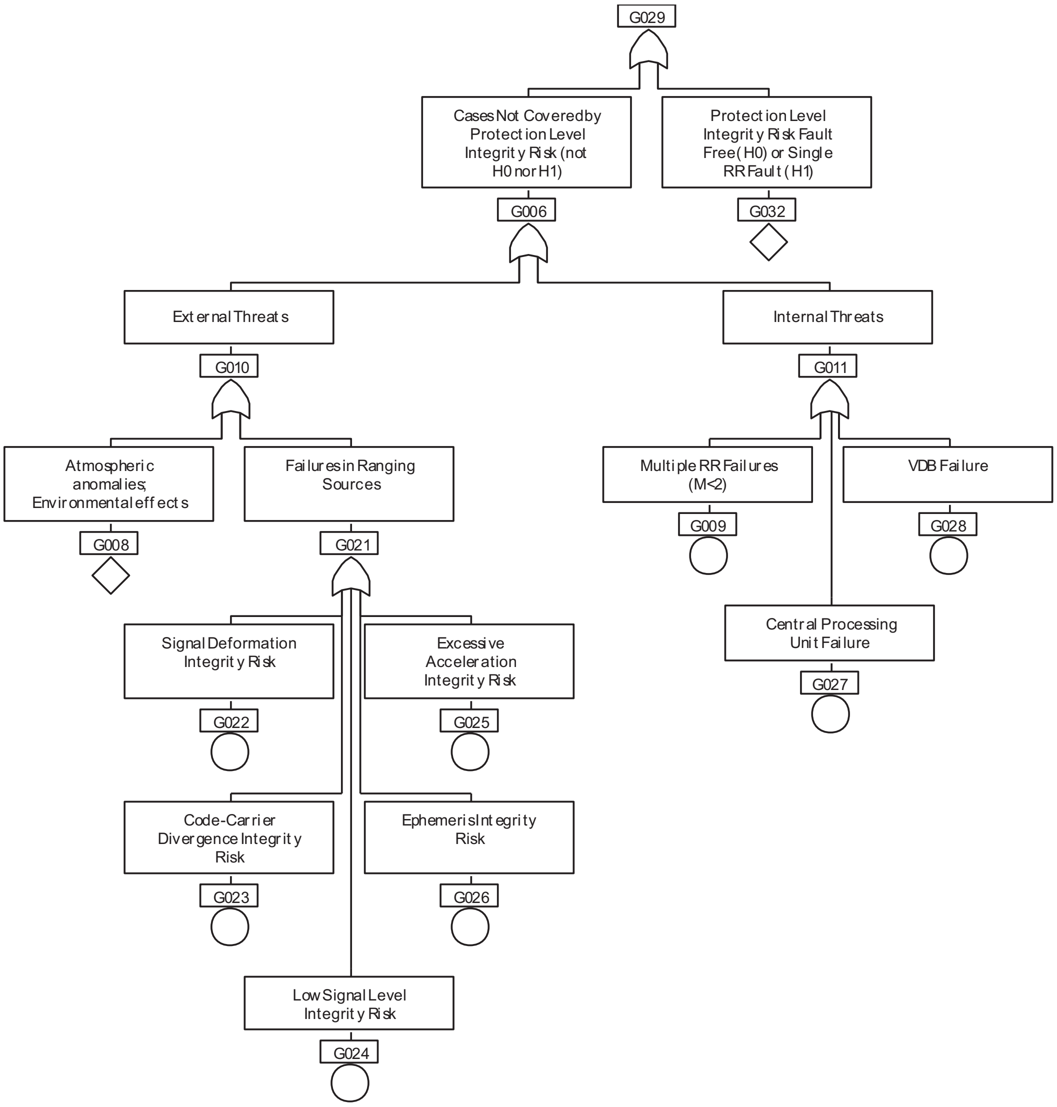

G029
Cases Not Covered by Protection Level Integrity Risk (not H0 nor H1)
Protection Level Integrity Risk Fault Free (H0) or Single RR Fault (H1)
G006
G032
External Threats
Internal Threats
G010
G011
Atmospheric anomalies; Environmental effects
Failures in Ranging Sources
Multiple RR Failures (M<2)
VDB Failure
G008
G021
G009
G028
Signal Deformation Integrity Risk
Excessive Acceleration Integrity Risk
Central Processing Unit Failure
G022
G025
G027
Code-Carrier Divergence Integrity Risk
Ephemeris Integrity Risk
G023
G026
Low Signal Level Integrity Risk
G024

Figure 7. Qualitative integrity risk tree.

The fifth step is to redefine the system architecture to get an acceptable level of SIS integrity risk (p<1.5E-7/approach), rearranging the system items of the integrity risk tree, inserting additional controls of system integrity (e.g., FDIR algorithm, built-in test equipment (BITE), health monitoring, warning devices, etc.) and recalculating the probability of the top event (Gate 029), as in Fig. 9. Each item added to the system architecture is a barrier to the undesired event occurrence, so the logical arrangement of these barriers is fundamental to improve the integrity and the safety levels of the system (qualitative and quantitative approaches).

The final result of the probable calculation of top event: cut sets for G029 cut set #1: 5,00E-08 G032. The top event probability is 5.00E-08.

Once the probability of the top event (Gate 029) is under limits of controls (reached result = 5.0E-08), the system integrity risk is within the acceptable limits of risk, then the system architecture may be considered acceptable and the safety assessment process (SAE ARP 4761, 1996) can be fed back and follow-on.

The final step, number 6, is to document the process and to provide feedback to the designers' team about the most appropriate system architecture that shall comply with the safety and integrity requirements.

CONCLUSIONS

The process of designing the integrity risk algorithm to be embedded on the IRM subsystem is not discussed in this paper because it is software engineering issue and can be treated

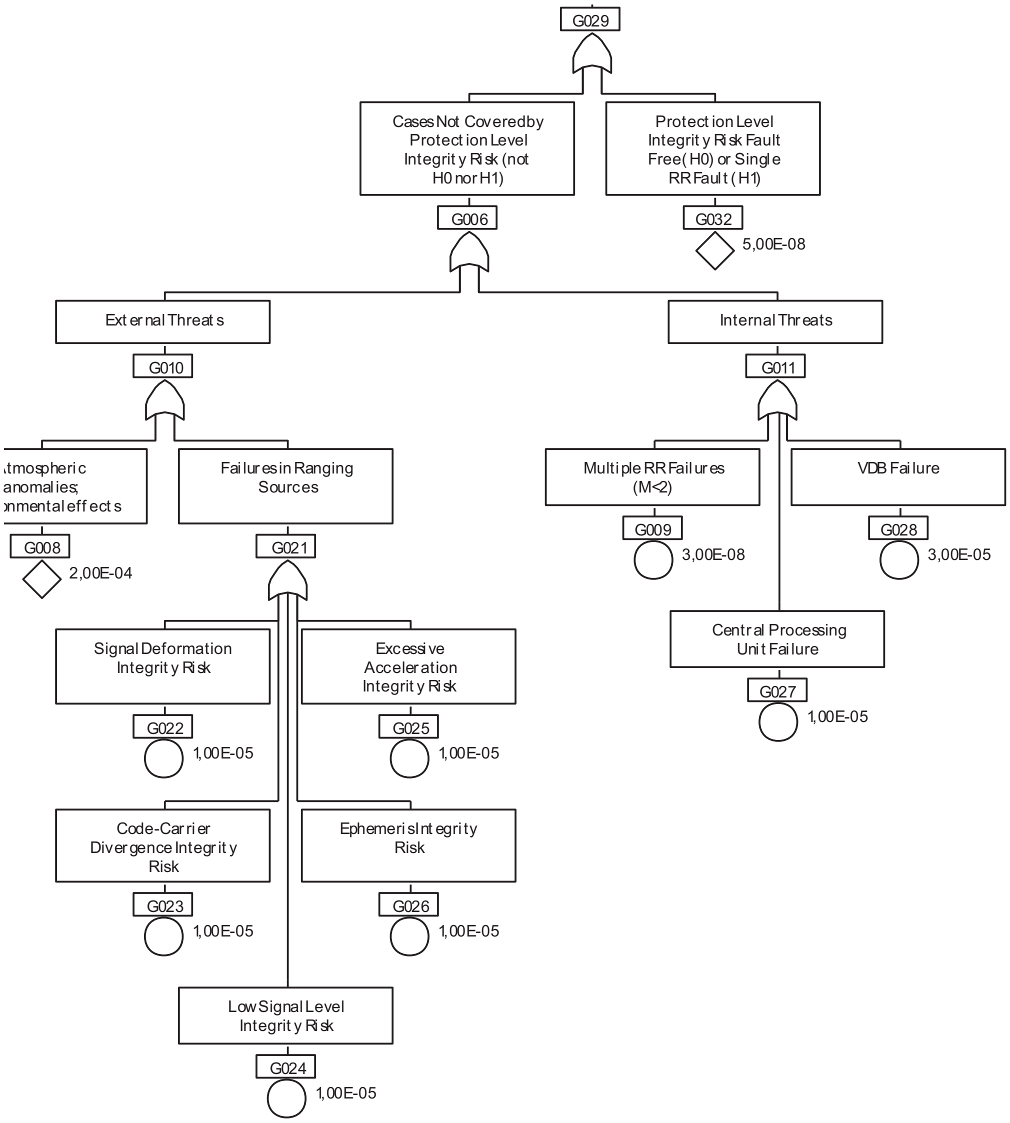

G029
Cases Not Covered by Protection Level Integrity Risk (not H0 nor H1)
Protection Level Integrity Risk Fault Free (H0) or Single RR Fault (H1)
G006
G032
5,00E-08
External Threats
Internal Threats
G010
G011
tmospheric anomalies; nmental effects
Failures in Ranging Sources
Multiple RR Failures (M<2)
VDB Failure
G008
2,00E-04
G021
G009
3,00E-08
G028
3,00E-05
Signal Deformation Integrity Risk
Excessive Acceleration Integrity Risk
Central Processing Unit Failure
G027
1,00E-05
G022
1,00E-05
G025
1,00E-05
Code-Carrier Divergence Integrity Risk
Ephemeris Integrity Risk
G023
1,00E-05
G026
1,00E-05
Low Signal Level Integrity Risk
G024
1,00E-05

Figure 8. Integrity risk tree with probabilities of events.

as a future work. The goal of this paper is not the algorithm design and development, it is the methodology of preparing the inputs for the algorithm design.

The RTCA (2004) and ICAO integrity risk requirement is met by using the RTA (ICAO, 2008) technique to identify, evaluate, display and calculate the risks associated with the system architecture, environment, and operation. This technique is based on the fault tree analysis (FTA) principles as a basic input, and it is possible to get a visual and mathematical approach of the system risks, allowing an accurate system risk modeling and assessment. The method shown is a way to lead the safety efforts to certification activities of the system and to contribute to safety specialists and risk managers by providing a new alternative for treating and solving the engineering problems which threaten the feasibility (or success) of the GBAS programs around the world.

The methodology presented also provides a dynamic approach to manage the system risk for it is a continuous variable whose values are cumulative in time (increase over time). Nowadays, the great difficulty to manage the system integrity risks is its dynamic characteristics over time, mainly within a system that aids satellite navigation of aircrafts. This is a very dynamic scenario, where the GBAS does not know if there is any aircraft using its services in any time, so the exposure time belongs the most important variable to be controlled by IRM.

Finally, the methodology presented has shown the importance of the IRM to automatically manage the risks of the system, and it belongs to a fundamental part of the ground-based augmentation subsystem (or ground station) and helps the safety engineers to assure the safe design and the operational safety of the total GBAS.

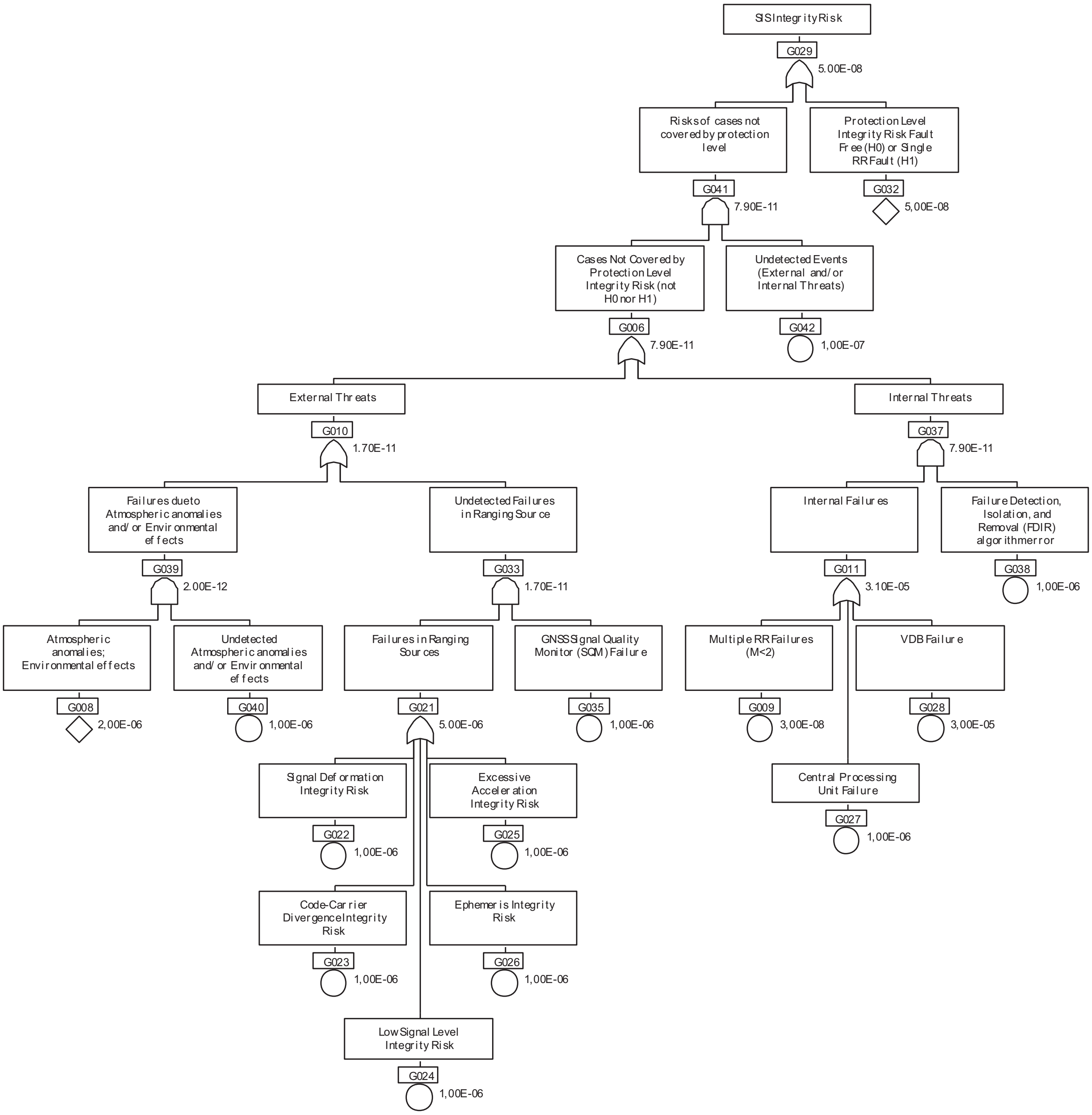

SIS Integrity Risk
G029
5.00E-08
Risks of cases not covered by protection level
G041
7.90E-11
Protection Level Integrity Risk Fault Free (H0) or Single RR Fault (H1)
G032
5,00E-08
Cases Not Covered by Protection Level Integrity Risk (not H0 nor H1)
G006
7.90E-11
Undetected Events (External and/or Internal Threats)
G042
1,00E-07
External Threats
G010
1.70E-11
Internal Threats
G037
7.90E-11
Failures due to Atmospheric anomalies and/or Environmental effects
G039
2.00E-12
Undetected Failures in Ranging Source
G033
1.70E-11
Internal Failures
G011
3.10E-05
Failure Detection, Isolation, and Removal (FDIR) algorithm error
G038
1,00E-06
Atmospheric anomalies; Environmental effects
G008
2,00E-06
Undetected Atmospheric anomalies and/or Environmental effects
G040
1,00E-06
Failures in Ranging Sources
G021
5.00E-06
GNSS Signal Quality Monitor (SQM) Failure
G035
1,00E-06
Multiple RR Failures (M<2)
G009
3,00E-08
VDB Failure
G028
3,00E-05
Signal Deformation Integrity Risk
G022
1,00E-06
Excessive Acceleration Integrity Risk
G025
1,00E-06
Central Processing Unit Failure
G027
1,00E-06
Code-Carrier Divergence Integrity Risk
G023
1,00E-06
Ephemeris Integrity Risk
G026
1,00E-06
Low Signal Level Integrity Risk
G024
1,00E-06

Figure 9. Final integrity risk tree.

REFERENCES

U.S. Federal Aviation Administration (FAA). Advisory Circular/ Advisory Material Joint – AC/AMJ 25.1309, 2002, "Arsenal revised (draft), System Design and Analysis", Washington, DC, USA.

U.S. Department of Defense, DOD, MIL-STD-882D, 2000, "Standard Practice for System Safety". Washington, DC, USA.

The European Organisation for Civil Aviation Equipment (EUROCAE), ED-114, 2003, "Minimal Operation Performance Specification (MOPS) for Global Navigation Satellite Ground-Based Augmentation System Ground Equipment to Support Category I Operations", Paris, France.

Federal Aviation Administration, 2010, “Navigation Services – Ground Based Augmentation System (GBAS)”, Retrieved in 2012 February 11, from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/laas/.

International Civil Aviation Organization, ICAO, 2009, “Doc 9859, Safety Management Manual (SMM)”, 2nd edition. Montreal, QC, Canada.

International Civil Aviation Organization, ICAO, 2008, “ANNEX 10 to the Convention on International Civil Aviation – Aeronautical Telecommunications” – Volume I – Radio Navigation Aids. 6th Ed., Amendments 1-81, July 2006, amendment 82, November 2007 and amendment 83, August 2008. Montreal, QC, Canada.

Radio Technical Commission for Aeronautics, RTCA, DO-245A, 2004, “Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS)”, Washington, DC, USA.

Radio Technical Commission for Aeronautics, RTCA, DO-254, 2000, “Design Assurance Guidance for Airborne Electronic Hardware”, Washington, DC, USA.

Radio Technical Commission for Aeronautics, RTCA, DO-178B, 1992, “Software Considerations in Airborne Systems and Equipment Certification”, Washington, DC, USA.

Society of Automotive Engineers, Aerospace Recommended Practice, SAE ARP 4754A, 2010, “Guidelines for Development of Civil Aircraft and Systems”, Warrendale, Pennsylvania, USA.

Society of Automotive Engineers, Aerospace Recommended Practice, SAE ARP 4761, 1996, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment”, Warrendale, Pennsylvania, USA.

Society of Automotive Engineers, Aerospace Recommended Practice, SAE ARP 4754, 1996, “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”, Warrendale, Pennsylvania, USA.